Question R.1

Information Systems Implementation

Section R: Information Systems

R.1 Describe your approach for implementing information systems in support of this RFP, including:

An MIS Organized for Implementation In Support of Managed Medicaid Programs

Louisiana Healthcare Connections (LHC) is joint venture between the Louisiana Partnership for Choice and Access (LPC&A - an organization of 19 Federal Qualified Health Centers (FQHC's) throughout Louisiana) and the Centene Corporation (Centene). Our 27 years of Medicaid health plan implementation and operations experience, and over 275 Information Technology (IT) professionals are focused solely on public sector programs. Nationwide, Centene's scalable MIS supports the goals of responsive, accountable, and coordinated care for almost 1.6 million Americans in our public sector full risk managed care plans in 11 states. We support health care administration and coordinated care through an MIS architecture and organization *engineered* for:

1. Integrated **application delivery**, reliability, availability, and interoperability *and*
2. **Flexible, low risk, implementation** in the service of public sector health plans such as the Coordinated Care Network (CCN).

Delivering CCN Functionality. We deliver item (**1**) above through an innovative Service Oriented Architecture (SOA) which allows us to offer "best of breed" managed Medicaid and CHIP administrative and clinical functionality; all delivered through an experienced MIS staff seamlessly organized around our local plan needs for MIS requirements definition, implementation, operation and support. We describe these aspects of our MIS throughout this Section; for example: see Question R.4 for details on our SOA; Question R.3 for the reliability aspects of our MIS; Questions R.2, R.6 and R.15 for more information on our open standards; and Question 12 for more on our MIS organization.

Ready and Organized to Implement. We deliver item (**2**) above through integrated MIS components with open, well documented industry standard application, data, and communications interfaces; allowing us to implement connectivity reliably and quickly with our state clients, their intermediaries (some of which we work with in multiple states), and providers. Our MIS components all feature configuration utilities that are *table driven* and *parameter based*, with very little need for custom software development and thus minimal implementation risk. As a result, our IT Implementation Team can focus our project efforts on detail analysis, precise definitions of business rules and LHC and DHH specific data edits, thorough integrated internal and external test plans with full scenario test cases, and thoroughly configured and tested data and online communication links with DHH, the DHH Fiscal Intermediary and Enrollment Broker, and our network providers and other Trading Partners.

We also enable item (**2**) through IT industry recognized *best practices* in Change Management, such as the Agile Software Development Life Cycle (SDLC) discipline for rapid, iterative deployment of implementations as well as system enhancements or changes; and for our approach to systematically driven Capacity Monitoring and Planning and Annual Systems Refresh Program - both processes leveraging our approach to quick, but thorough and auditable Change Management.

Finally, a key ingredient in our ability to deliver new health plan start/ups is our *organizational focus* on implementations. Our dedicated MIS implementation team is led by our Senior Director of IT Implementations, who reports directly to Centene's Chief Information Officer (CIO). Our team of implementation specialists is multi-disciplined to handle start-ups from proposal preparation (our implementation staff were directly involved with the preparation of this proposal) through business analysis, configuration design, testing, training, deployment, and smooth hand-off to ongoing operations staff. Every member of our dedicated implementation team has years of experience with 22 new health plan or program implementations over the last five years, and some of our key Lessons Learned can be seen in our response to Question R.6. For more on our Change Management processes, please see

Question R.8. And, of course, see the discussion below for more on our configuration, testing, and project planning approaches for LHC in Louisiana.

LHC's Partner In CCN Implementation: LPC&A. In the case of LHC's CCN implementation, we are ***particularly fortunate*** to work with our FQHC owner-partners that form LPC&A; and we are already leveraging the experiences and plans of these 19 statewide FQHC's. For example:

- Through LPC&A, LHC has a built-in network of FQHC **emergency planning contacts**, and LPC&A has been invaluable in helping us define Louisiana specific needs and nuances for emergency management planning. In addition, our work with LPC&A has already contributed to the customization and configuration of our LHC Business Continuity Plan (BCP). Please refer to Section M, Questions M.1 and M.2 for more information.
- LCP&A has been indispensable in helping us to define some important MIS configuration requirements for CCN implementation. For example, we have already been able to define many provider data collection specifics for our Provider Relationship Management (PRM) system - to allow for the capture, tracking, and management of emergency volunteer practitioners and facilities, and the "real time" emergency status of these providers and facilities during a declared disaster. PRM is Centene's enterprise provider data management platform - supporting key provider functions such as contracting, provider service and unified communications, and master data management for "all things provider related". Please see Questions R.4 and R.11 for more information on PRM.
- To help inform our implementation planning for administrative and clinical data integration with a critical portion of our provider network (FQHC's), we have used valuable input from LPC&A in our "tiered" plan for helping FQHC's - and all our network providers - on their path to increased meaningful use of Health Information Technology, online health records, (including Electronic Health Records (EHR: as defined by recent Federal rules and regulations), and the use of Health Information Exchanges (HIE), as HIE capabilities unfold in Louisiana. Please see Question R.15 for more information on our tiered approach to enabling the increased meaningful use of electronic health information.

• Capability and capacity assessment to determine if new or upgraded systems, enhanced systems functionality and/or additional systems capacity are required to meet contract requirements;

A Systematic Approach to Capacity Assessment and Planning - Aligned With Our Clients' Needs

Capacity is a Design Point of our MIS. Since Centene's inception, we have always based our MIS strategy on a simple operating tenet: that MIS capacity will *never* limit our ability to grow in any of the Public Sector healthcare markets we strive to serve, such as Louisiana's CCN program. We continue to adhere to this approach: from 2005 through 2010 we experienced an average growth rate of 19% per year in membership, with no negative impact on MIS service levels. It is against this backdrop of continual sizable growth that we have, as a matter of *strategic importance*, incorporated ***scalability*** in our MIS, and instituted systematic capability and capacity assessment processes throughout our IT planning activities.

We Have MIS Capacity to Grow in the Near Term. Scalability represents our MIS capacity to administer ever increasing membership with continually evolving MIS applications, while simultaneously improving both performance and reliability. In short, we engineer scalability and reliability in our MIS architecture through the careful deployment of proven technologies such as automated systems management, virtualization, storage area networks, server clustering, and hardware and software *redundancy* - including the use of redundantly sourced communication services from multiple vendors.

This means that, although we currently serve 1.6 million members, we have the MIS capacity to serve 2.25 million members - today - and still maintain a workable level of redundancy and performance. In addition, and not accounted for in this "2.25 million member scenario", is the fact that in 4Q 2011, we will bring our new datacenter installation online; more than *quadrupling* our existing physical MIS

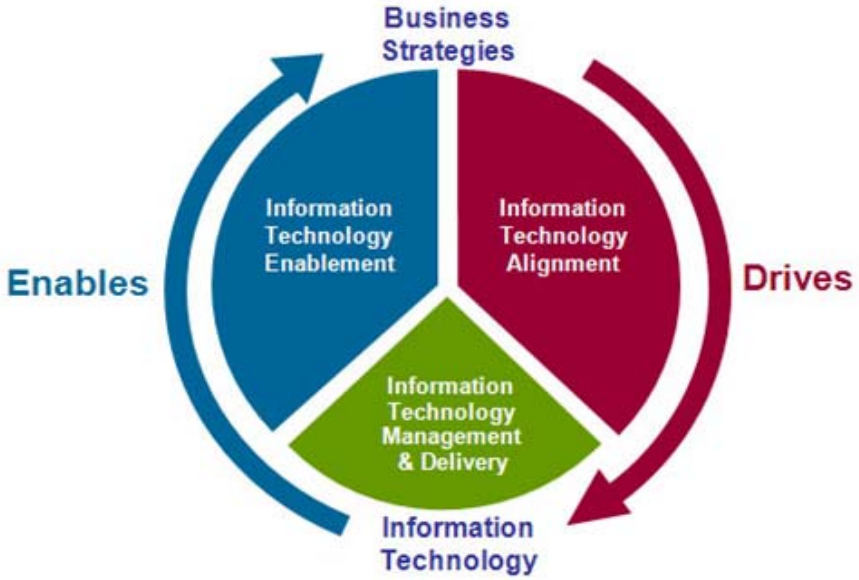
facilities. Please see Questions R.3 and R.7 for more information on the scalability aspects of our MIS, and our new datacenter installation.

We have reviewed all requirements in the RFP, including (and in particular) Sections 16 and 17, and the CCN-P Systems Planning Guide, as well as estimated membership ranges across all three GSA's (members in programs exactly like those we serve in 11 other states today) - and we have determined that we have the processing capability and capacity in place *today* to serve LHC and the CCN. Nonetheless, we can only make a statement like this because of the ongoing capability and capacity assessment processes we have in place - described immediately below.

Capability and Capacity Assessment: An Ongoing Process

There is one driving purpose in all of our Capability and Capacity Assessment processes: to support the business strategies and operational needs of our health plans, including LHC. See ***Figure R1-A: Alignment Drives Enablement***.

Figure R1-A: Alignment Drives Enablement.



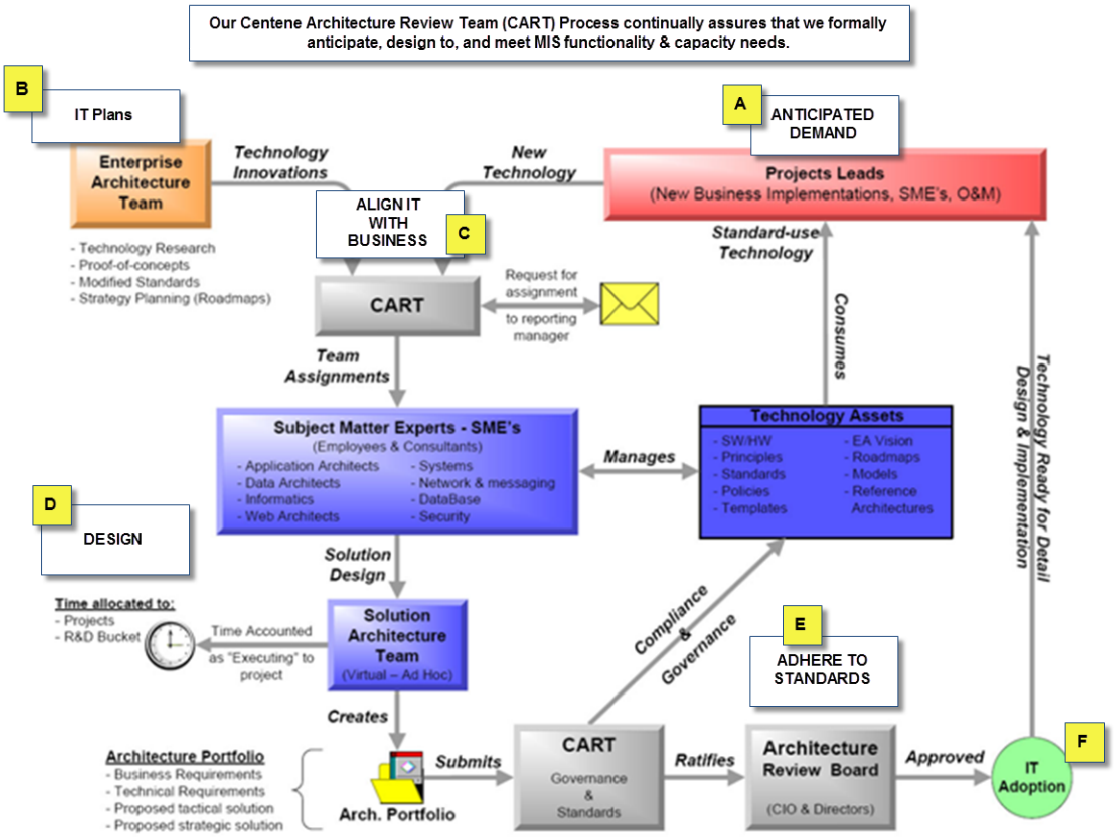
We actualize this alignment of IT capability and capacity with business need through **the Centene Architectural Review Team (CART)** process. CART is our ***IT Governance body*** and contains subject matter experts and management from each IT discipline. CART is responsible for the review of new, existing, and evolving architectures within the Centene environment to enforce strict adherence to accepted design principles, security best practices, and Centene's overall and business-aligned strategic technology direction. Please refer to ***Figure R.1-B: Centene Architectural Review Team (R.1-B)*** for the following discussion. R1-B is a graphical depiction of the overall process through which we continually surface, align, vet, specify, harmonize, and deploy IT capability and capacity upgrades to meet business requirements: both functional enhancements to our MIS ("capability") and processing power, storage, and bandwidth ("capacity"). In R1-B:

- Item A connotes the formal identification, documentation, and presentation to CART of new capability or capacity needs from either our health plans themselves, or one of our Centene corporate business units (e.g. claims operations) - *or the IT department through our regular and systematic monitoring of processing performance (see below)*. Please note: that not all MIS

changes need to go through the CART process - only MIS changes with an impact on our overall architecture (including capacity needs), are managed through CART. All software changes and implementation projects go through our Change Review Board (CRB - see Question R.8); and if the CRB determines the need for review, a specific Change Request or project is sent by the CRB to CART.

- Item **B** represents our strategic IT plan at any point, and in the CART process we ensure on an ongoing basis that our IT plan will support the capability or capacity need in **A** - or if additional capability or capacity is needed.
- Item **C** - represents the review by the CART team of planned enhancements. As a result of CART review, an appropriate design team is assembled - depending on the expertise required - to develop detail business and technical design specifications (item **D**) ; including capacity assessments of Central Processing Unit (CPU) power, online disk, data communications bandwidth, etc.
- After the design team in **D** completes and documents the design for the capability or capacity upgrade, the CART board ensures that our IT standards and compliance needs will be met; and following that, CART and the design team prepare a summary of the design and supporting business decision which is tabled with Centene's CIO and appropriate business directors and local health plan management (**E**). Note that, also in item **D**, CART may update our IT Strategic Plan (**B**) - depending on the nature of the approved project in **E** that is approved by our CIO and business stakeholders for deployment (**F**).
    - For example, if (in item **A**) our IT Architecture Team (see discussion below) determines that "organic" business volume growth (that is: growth in our transaction volume due to the membership growth in our existing health plans) will require extra server hardware, CART will update the Technology Refresh portion of our IT Strategic Plan (**B**) accordingly.

Figure R1-B: Centene Architectural Review Team.



In short, our CART process ensures an ongoing, but controlled and disciplined, approach to capability and capacity upgrade management.

Capacity Planning Expertise and Tools. Centene's Architecture Team (IAT) has implemented a thorough Capacity Management Architecture (CMA) and process to monitor and report on system metrics, such as CPU load, memory usage, disk I/O, network bandwidth, and transaction times, that are crucial to maintaining satisfactory performance and capacity service levels. Within our IAT, we have a dedicated ***Capacity Management Team (CMT)***, supported by other subject matter experts in systems design and performance, who focuses on constantly reviewing and monitoring the utilization and capacity of all our key production IT Systems; including:

- AMISYS Advance: our claims processing platform.
- TruCare: our platform for collaborative care coordination, case, and utilization management.
- Member and Provider Relationship Management (MRM and PRM): our enterprise member and provider: services, unified communications, and master data management systems, respectively.
- MDE Xpress Encounter Pro: our best of breed encounter submission and workflow system.
- Centelligence™: our enterprise data integration, informatics, desktop reporting and decision support system.
- EDIFECS: our HIPAA and HL7 compliance, interface, and communications system.

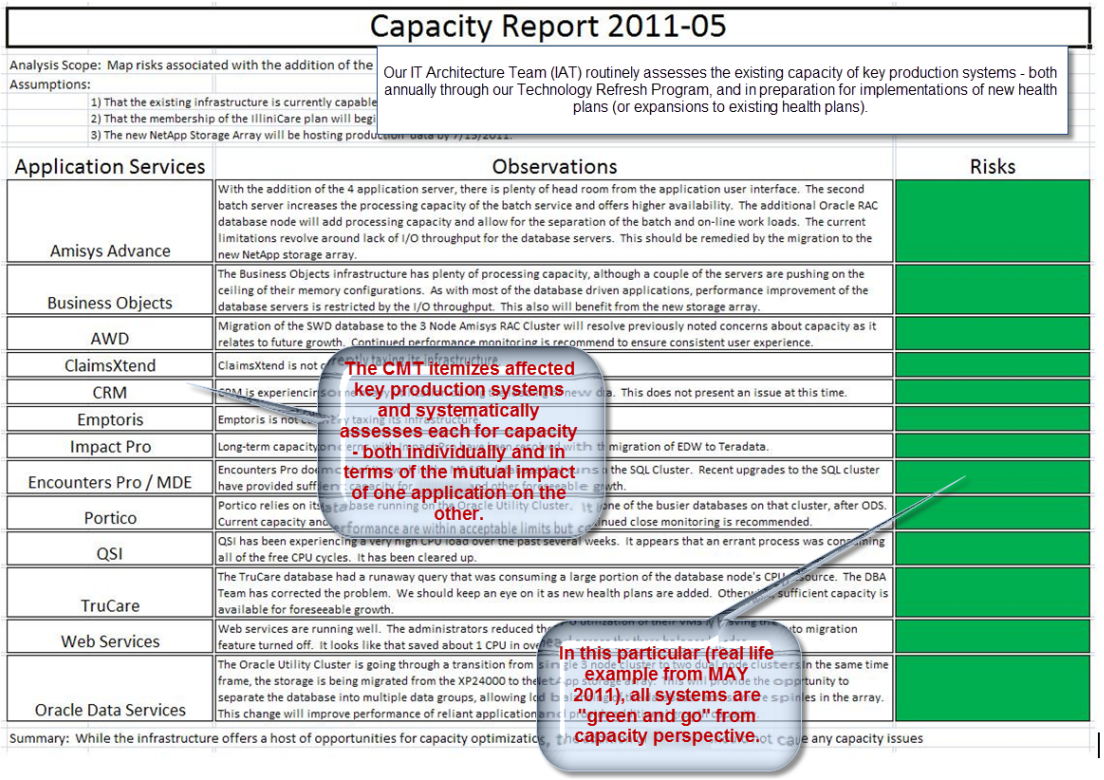
- Member and Provider Web Portals: our web-based secure portals for Member and Provider self-service and care engagement and coordination.
- Systems software: our underlying middleware and Relational Database Management Systems (RDBMS) and operating systems.

Each month, for our key production systems above, our Capacity Manager and his team compare the current utilization with our 12 month historical trend to determine if there are projected capacity deficiencies or foreseeable needs that cue us to plan in advance for additional capacity and obtain approval through the CART process above.

In addition, with every new business implementation, and well before extra capacity is needed, we use our ***CA Technologies Hyperformix (Hyperformix)*** performance simulation software to assess alternative upgrade strategies and the effect these alternative strategies will have on our existing and anticipated online and batch processing workload performance. Hyperformix is specifically designed to model complex architectures like ours: an MIS that make extensive use of virtualization, database and application server clustering, and the other "high availability" and fault tolerant aspects of our MIS componentry. Please see Question R.3 for more information on the availability aspects of our architecture.

As an example, real life, capacity assessment recently performed by our IAT in anticipation of a May, 2011 "go live" for a health plan in another state is shown below. See ***Figure R.1-C: Example Capacity Assessment Report.***

Figure R.1-C: Example Capacity Assessment Report.



Finally, on a continual basis, our Capacity Management Team analyzes batch, real time, and core end-user transactions volumes and trends to keep IT personnel aware of any growing negative trends.

The MIS performance "intelligence" provided by the processes and tools above equips Centene leadership with the information required to be proactive in ensuring that the available capacity and performance of essential systems always exceeds the capacity and performance that is required.

• Configuration of systems (e.g., business rules, valid values for critical data, data exchanges/interfaces) to accommodate contract requirements;

We use a best practices Agile Software Development Life Cycle (SDLC) process for required system changes or enhancements - including software configurations for our health plan start/ups or expansions; while maintaining auditable business controls. We implement system configuration changes as part of an integrated release management process. Each Centene application team (e.g. claims, reporting, care management) establishes and publishes a *release calendar*, with controlled releases typically every two to four weeks, a frequency which mitigates operational risk by reducing emergency changes. Although we will only need relatively minor configuration changes in our MIS to support LHC's CCN program, we will still employ our SDLC rigor prior to "going live". Our IT Implementation Team uses Atlassian's integrated Greenhopper and JIRA software tools to manage the Agile workflow of the project - including the user stories and iterations, prioritized work items, and all other Agile artifacts and techniques.

Our SDLC includes the following phases, all orchestrated by our IT Implementation Project Manager. It is the approach below, led by a dedicated IT Implementation Project Manager, and dedicated IT Implementation Team, with oversight from our Senior Director of IT Implementations, which we will use for LHC's CCN MIS implementation; as part of the **overall** LHC CCN Implementation Plan (see Section C, Questions C.2 and C.4):

1. **Requirements:** Our IT Implementation Project Manager facilitates several design sessions between IT and the business stakeholders on our overall health plan implementation team (e.g. the LHC Implementation Team), to ensure that we meet or exceed the contract requirements in each specific area (eligibility, claims, encounters, etc.). Our business analysts document specific configurations for the business rules, specific edit settings, benefit plan configurations, and file and data formats for inbound and outbound file exchanges. These are reviewed and signed off by all key business stakeholders.
2. **Input on Release:** During this phase, our Development Team creates technical specifications from requirements and testing scenarios. We hold daily meetings to check progress, ensure understanding of requirements, and identify barriers for management.
3. **Development/Unit Testing:** During unit testing, our Development Team works closely with business sponsors to keep the project on track, and our engineers perform Peer Review to ensure the new software code (code) meets Centene standards.
4. **Release Review/Deploy to Test**: The Release Team reviews the code to make sure it is ready to move to the test environment. The Release Team uses a checklist to ensure all requirements are taken into consideration before the code is released to integration testing.
5. **Integration Testing/UAT:** After numerous iterations in our Agile IT processes, we perform integration testing that includes our business stakeholders to ensure appropriate outcomes for business areas related to member, provider, authorization, claims and reporting (our Centelligence™ Enterprise Data Warehouse (EDW) and Centelligence™ Insight reporting system). During this phase, we complete regression testing to prevent unintended impact on current functionality. We use IBM Rational automated testing tools to assist in this process.
6. **Management Validation:** The Development Team Leads review each Agile user story or use case and approve or deny the change.
7. **Change Review Board:** The Change Review Board (consisting of project managers and architects from key areas) performs final release review, including risk and impact of the release. All relevant parties must agree on a release date.
8. **Move to Production:** Once the release has all been approved by all parties, the Release Team moves the release into the production env**ironment. We u**se Subversion and Serena ChangeMan for our

Unix and Windows environment library and software versioning control processes as software configurations move from unit test to production.

9. **Production Validation:** Here the Development Team reviews the release to validate that enhancements function as planned. Should issues be discovered, they implement the backout plan for this change. Otherwise, the release is closed.

• System setup for intake, processing and acceptance of one-time data feeds from the State and other sources, e.g., initial set of CCN enrollees, claims/service utilization history for the initial set of CCN enrollees, active/open service authorizations for the initial set CCN enrollees, etc.; and

Full Support for HIPAA or Proprietary Formats for One Time Feeds

Our MIS fully supports all HIPAA transaction and codeset standards. Where possible, we suggest HIPAA standards for use with the one-time data feeds for several reasons:

- As we note in one of our lessons learned (Question R.6) - it is easier for two parties exchanging data to understand the meaning, context and syntactical use of data within HIPAA transaction files than with proprietary formats.
- DHH and DHH intermediaries (the Fiscal Intermediary and Enrollment Broker: "FI" and "EB", respectively) will need to support multiple CCN's - as many as six in a GSA. The odds are greater that these potential six CCN's "all speak HIPAA" and using HIPAA formats will ease the normal issues and considerations that come to surface in implementations such as these.
- As a corollary to the above, (and as is the case with Centene and LHC), if all CCN's and DHH (and the FI and EB) use HIPAA formats for the one time feeds, this lowers implementation risk - since there will be no separate set/up configurations needed for "one time" authorization feeds (for example).

Nonetheless, Centene and LHC can and will support proprietary feeds of initial data if needed. Our EDIFECS EDI and TIBCO middleware software, combined with our COVIANT multi-protocol file transmission system allows us to *configure* (not develop) for the CCN program. Please see Question R.6 for more information on our ability to process HIPAA and non-HIPAA (proprietary) formats.

Based on our implementation experience, we would suggest the following plan for one time data feeds:

- Initial meeting(s) as early as possible for DHH, the FI, the EB and CCN's for GSA 1 to review each "one time" and ongoing data interface. We have several suggestions around these meetings - please see Question R.6 for details.
- Individual send/receive tests of the one time data feeds - merely to check format, parsing, and readability by all parties.
- Stage the one time data feeds in this order:
    - First data load of CCN membership (enrollment and eligibility) - we suggest in the HIPAA 834 format.
    - Prior claims (including prescription and dental claims) history - we suggest in HIPAA 837 format.
    - Outstanding service authorizations that span the "go live date" (e.g. 1/1/2012 for GSA 1) - we suggest in HIPAA 278 format.
- We have used the above "one time data feed" order in the past and have found it the best approach - because it allows us to link member to utilization history to open authorizations; and allows us to ensure data integrity at the master member level prior to receiving transition utilization and authorization information.
- After each of the three feeds, we will report back to DHH (or FI or EB, as appropriate) an acknowledgement of what we received, the record counts, and any issues. We can then work with DHH to decide if any issues are serious enough that they would need to be addressed prior to proceeding.

Initial CCN Enrollee. In terms of loading the initial "live" production set of initial CCN enrollees: we will not be loading this data until we have successfully tested eligibility data exchanges with the EB (see ***Attachment R1-A: LHC CCN MIS Implementation Plan***).

Once eligibility file load testing is complete, and when we get the initial set of CCN enrollees, we will load this data through our EDIFECS EDI HIPAA compliance system into our MRM system, and subject to RFP requirements in Section 12, this enrollment data will trigger our welcome calls and kit mailings; and the automated provisioning of secured Member Web portal accounts. Because most of our anticipated membership is less than 18 years of age (and we cannot provision a Member Portal account for someone less than 18 years old), we propose to use the "Responsible Person" segment in the HIPAA 834 file from the EB and work with the EB and DHH to consider the "Responsible Person" as being the Parent or Legal Guardian (PLG) of the member. We would then provision a Member Portal account for that validated PLG. This "PLG feature" of our Member Portal is a direct benefit of our role based access control approach to security. Please see Section K, Question K.5 for more information on PLG support, and R.16 for more information on our security controls.

Another process that will systematically occur with the initial load is the detection of members with special health care needs (if indicated on the inbound 834 from the EB). Our MRM uses this data to populate the special health care needs indicators in our master member records - available for a number of applications; including, for example, the presentation of this information on our online member roster within our secure web based Provider Portal.

Claims History. We will receive the claims history data through our Informatica ETL system, as we will do with ongoing pharmacy, dental, or other fee-for-service claims that DHH provides us for the duration of the program. When we receive this data we will validate it against the initial enrollment files (as described above) – so that we can identify any mismatches and work with the EB and/or the FI to verify if we are missing a member in the enrollment file or we are getting claims data that we should not be getting that perhaps some other CCN should be receiving. Once we validate the data, we will load it into our Centelligence™ informatics platform. Centelligence™ has direct access to our master member data files in MRM - and will link the claims records with the "already loaded" member information in MRM. Please see Question R.4 for more information on the interoperability of our MIS components.

The claims data will then be available to our Centelligence™ Insight reporting system, and our Centelligence Foresight™ predictive modeling application so that we can systematically identify care gaps and health risks the member may have.

Please note that we support HIPAA NCPDP formats for the import of prescription drug claims data – should that be the format that DHH uses. Again, we will accommodate any format that DHH chooses.

Active/Open Service Authorizations. We will work with DHH to finalize the service transition strategy per RFP (e.g. the length of outstanding service authorizations after 1/1/12), and use those finalized requirements to process the service authorizations data that we receive prior to go-live. We will load the service authorizations data into our EDIFECS EDI system which checks for HIPAA compliance, and reformats for processing in our TruCare clinical care and utilization management system. Like Centelligence™, TruCare has integrated access to the member data in MRM - and TruCare will systematically link the open authorizations data to the member records in MRM. TruCare will also publish these authorizations to Amisys, ensuring that the claims for these services are properly adjudicated and paid. Finally, TruCare also makes the open authorizations data available to Centelligence™, and our Medical Management Team will use Centelligence™ Insight to determine if and when any interventions should be made for members based on the open authorizations and any potential care gaps and health risks identified by Centelligence™ Foresight (see above).

• Internal and joint (CCN and DHH) testing of one-time and ongoing exchanges of eligibility/enrollment, provider network, claims/encounters and other data.

Step #1: Analysis and Finalization

Data Files, Codesets, and Reference Data. Our first step in testing of data exchanges (one time and ongoing) will be for our assigned business analysts (see above discussion) to obtain, review, and validate with DHH and/or the FI and/or the EB - the finalized, required formats for eligibility/enrollment, encounters, claims history, and other files and reference data we need to send and receive (e.g. the Claims Summary Report mentioned in Section 17.5.5 of the RFP), and other codesets we need to employ (such as those DHH will publish at the url: www.lamedicaid.com: the list of Louisiana Medicaid provider types, specialty, and sub-specialty codes). DHH has already supplied specifications for the Provider Directory/Network Provider and Subcontractor Registry (CCN-P Systems Companion Guide, Appendix G) - but we will document focused questions on this interface format (and all interface formats) - in order to "lock down" fully our understanding of the meaning of all data element fields in all data interfaces; including the intended use and context of all fields; as well as their conditional or situational use. We will offer our documented questions (and working assumptions) to DHH prior to meeting with DHH and/or the FI and/or the EB (all at DHH's direction).

We will also request, per question #628 in DHH's document: CCN PREPAID RFP QUESTIONS AND ANSWERS, dated 5/23/11, the ongoing receipt of the HIPAA 835 for use in the encounter acknowledgement process. Wherever possible, Centene uses HIPAA transactions for business data exchanges; because we have found this leads to less implementation risk, less chance of misunderstanding between Trading Partners in the intended usage of data, and quicker ability to introduce changes on a go-forward basis.

From a HIPAA transaction format perspective, it is our working assumption that all testing will be done using HIPAA 5010 (Errata Version) formats (for HIPAA 834 and 837 exchanges). We also noted - in question #277 in DHH's document: CCN PREPAID RFP QUESTIONS AND ANSWERS, dated 5/23/11, that CCN's will use the FI's website for a number of data downloads and entry of information (such as TPL information, and possible download of HIPAA 820 premium notices). We will include documented questions, and (where possible) our working assumptions on the use of the FI's website (including security provisions and any interface capabilities or limitations) - which we will bring to our first data interface meeting with DHH, the FI, and EB.

Test Data. During this step, we will also finalize with DHH, the FI, and EB the source and use of test data for external testing. We recommend strongly, wherever possible, that test data be "linked" for "end to end" scenario testing. We have learned from prior implementations, that it is important to avoid viewing individual data interfaces as "silos" of isolated data exchanges. We have found that it is not enough to test individual exchanges (e.g. receipt of eligibility data, transmission of test encounter data) with our state clients and Trading Partners without progressing through an entire cycle of information processing that spans all the core functions served by enrollment, eligibility, provider, claims, and encounter data in holistic "end to end" scenarios. This approach not only allows us (and our Trading Partners) to validate each data exchange, it also allows us to simulate the scenario throughout our member and provider inquiry services applications, our reporting applications, and our web portal application "experience". "End to end" scenario testing such as this is, in our judgment, the most practical way to uncover implementation nuances and challenges that might not otherwise surface.

Data Communications Set/up For Test and Production. Even while we are working on the above analysis, our EDI team will set/up "base" HIPAA 5010 translation maps in our EDIFECS system (for subsequent customization per DHH specifications above), and our data communications specialists will provision test and production secured FTP directories for subsequent use by the FI and EB. Conversely, through our IT Implementation Project Manager, our data communication specialists will contact appropriate personnel at DHH, the FI or the EB; to obtain secure FTP accounts for test and production use. Our data communications team will also finalize (per DHH, the FI and EB) the requisite communications protocol and secured file exchange controls (e.g. PGP, digital certificate exchanges) for test and production use. We will implement the required data exchange protocols in our COVIANT file

exchange management system (see Questions R.2, R.6, and R.7 for more information on our COVIANT system).

Step Two: EDIFECS and TIBCO Configuration and Internal Testing

Once we have finalized formats with DHH, the FI, and the EB, we will configure our EDIFECS EDI and integrated TIBCO middleware (see Question R.6 for more information) with the appropriate translation configurations, working off of the "base maps" set/up in Step One above. Our EDI configuration specialists will perform unit testing of the LHC mappings in our EDIFECS development environment, and then we will perform internal testing on each map in our integration test environment: testing the feed of inbound data (e.g. 834 enrollment/eligibility) and load into our integrated test environment Member Relationship Management (MRM) system; and from there, to our AMISYS Advance claims system, Centelligence data integration engine and TruCare clinical care and utilization management system - again: all in our integrated test environment. We will be doing the converse as well: producing test encounters through our AMISYS Advance claims system, through Centelligence's EDW, through our MDE Xpress Encounter Pro encounter workflow system and finally output from our EDIFECS EDI system as a HIPAA 837 transaction file.

We prefer to use DHH supplied test data for this and all internal tests; but if no test data is available from DHH (or the FI or EB), we can use our own test data from prior implementations.

Step Three: External Testing

We propose to do "end to end cycle" transaction testing with DHH, the FI and EB - with sign-off from all parties for each "step" in the cycle. For example, we would propose this order for the key data exchanges:

1. Testing of LHC transmission of Provider Directory/Network Provider and Subcontractor Registry to FI with acknowledgement back from FI.
2. Testing of LHC receipt of HIPAA 834 from EB and issuance of 997 or 999 Functional Acknowledgement (FA) from LHC to EB. Ensure effective communication of PCP assignment referencing directory from Step 1.
3. Testing of LHC transmission of member demographic changes in HIPAA 834 to EB, and receipt of 997 or 999 FA from EB.
4. Testing of LHC receipt of claims history (medical and pharmacy) data from DHH and/or FI. We were not certain of the format of these files based on the RFP and subsequent Questions and Answers, but we can (and do) support HIPAA 837 and HIPAA NCPDP formats for inbound medical and pharmacy claims today; and also proprietary formats.
5. Testing of LHC transmission of HIPAA 837 encounters to FI, with receipt of 997 or 999 FA back from FI to LHC.
6. Testing of transmission from FI of HIPAA 835 (encounter processing results); and other (non HIPAA) encounter processing files (repairable encounters, etc.)

Concomitant with above, we will also be doing testing of claims submission from our key providers: our network of FQHC's (including the FQHC's that form LPC&A) and other large volume providers. All of our network providers will also have online access (via our secure web based Provider Portal) to our EDIFECS Ramp Manager online EDI on-boarding system, to allow interactive testing and certification for the submission of HIPAA 5010 electronic claims to us. Please see R.13 for more information on our EDIFECS Ramp Manager facility.

Provide a Louisiana Medicaid CCN-Program-specific work plan that captures:

• Key activities and timeframes and

• Projected resource requirements from your organization for implementing information systems in support of this contract.

The work plan should cover activities from contract award to the start date of operations.

MIS Work Plan - Integrated With Overall LHC CCN Implementation Plan

Please refer to ***Attachment R1-A: LHC CCN MIS Implementation Plan*** (MIS Workplan) for our Microsoft Project based workplan. Our MIS Workplan was developed with the active input and oversight of our Senior Director of IT Implementations, who reports directly to Centene's Chief Information Officer (CIO), and we formulated our MIS Workplan in coordination with our overall LHC CCN Implementation Team (which is our standard approach for new health plan implementations such as LHC's). In fact, our MIS Workplan is integrated with the overall LHC CCN Implementation Plan (please see Section C, Questions C.2 and C.4), including the inclusion of estimated hours per workplan activity area.

Please see ***Figure R.1-D: MIS Workplan Snapshot*** below for a brief highlight of the contents of our MIS Workplan.

Figure R.1-D: MIS Workplan.

Summary Highlight of MIS Workplan (See ***Attachment R1-A: LHC CCN MIS Implementation Plan*** for the complete MIS Workplan.

	Task Name	Duration	Start	Finish	Predecessors	Group By Summary	Resource Names	Work Effort
1	Pre Implementation Readiness and Activities	224 days	Fri 6/24/11	Tue 5/1/12		No		
14	Implementation	209 days	Wed 7/20/11	Fri 5/4/12		No		
15	Program Management	19 days	Wed 7/27/11	Mon 8/22/11				1320
22	Infrastructure	53 days	Tue 7/26/11	Wed 10/5/11				1872
61	Software Configuration/ Iterations/Sprints	209 days	Wed 7/20/11	Fri 5/4/12		No	IT Imp Lead	
299	Software Integration Testing	30 days	Tue 10/25/11	Mon 12/5/11	5SS+40 days	No	IT Imp Lead	480
305	Readiness Review	57 days	Wed 9/14/11	Wed 11/30/11		No	IT Imp Lead	
313	Transition Phase	[illegible]	[illegible]	[illegible]	[illegible]	No	[illegible]	
314	GSA B - Enrollment testing	20 days	Fri 3/2/12	Tue 3/4/12	12FF	No	[illegible]	
315	GSA C - Enrollment testing	20 days	Wed 4/4/12	Tue 5/1/12	13FF	No	[illegible]	

Our MIS Workplan extends to the "go live" of GSA C.

Exhibited here (for convenience) is a "second level" roll-up of activity areas. Attachment R1-A lists all sub-activity areas and detail tasks.

Work Effort by Activity Areas is listed in HOURS.

Describe your historical data process including but not limited to:
• Number of years retained;
• How the data is stored; and
• How accessible is it.

Historical Data Process

Number of Years Retained

Transactional Data. All transactional data in our key production systems are stored ***online indefinitely*** (exceeding DHH requirements, although we will archive LHC transactional data after six years if DHH desires - otherwise we keep the data online for at least 7 years, or longer if there is a valid business

reason). We only purge data to offline storage if explicitly asked by our state clients, or if the age of the data exceeds what would be useful for trend analysis (never less than 7 years, and in practice, not less than 10 years). Of course, and in ALL cases, we backup all transactional data in our systems every 24 hours, and we store this data with a secured off-site HIPAA compliant storage vendor, Recall. By "transactional data" we mean all the key production transaction data we collect or generate; process; manage; use and report on; that is:

- Membership and eligibility related information (demographics, historical eligibility spans, TPL/COB information, etc.)
- Service authorizations
- Claims data (including imported processed claims data - e.g. pharmacy claims data from DHH), Health risk assessments and lab test results
- Provider data (demographics, specialties, contract information, etc.)
- Encounter submissions and associated files
- Reference and other data (codesets, etc.)

Paper and Fax Data. We scan paper claims and associated documentation, and member and provider paper correspondence, immediately upon receipt using our MACESS FormWorks and EXP software. We store the paper originals off-site indefinitely through our HIPAA compliant off-site storage vendor, Recall; and we store images online indefinitely. All other paper documentation (for example, a contract or legal document) is scanned using our Zasio Versatile Enterprise™ system and available as images indefinitely. Our Provider Network Management staff scan, index, and store provider contracts in the Emptoris provider contracting module of our Provider Relationship Management (PRM) system and these documents are available online indefinitely. Faxes are received by us via our RightFax enterprise, secure fax receipt and workflow system, and (depending on the nature of the fax) are indexed and stored in our MACESS EXP system (we rarely print faxes - they are received and handled electronically). Please see Question 7, 16.13.1 (Document Retention Periods and Retrieval Requirements) for more information.

How Data Is Stored

Transactional Data. All of our key production transactional data is stored in our integrated Relational Database Management System (RDBMS) software. We use industry standard RDBMS software from Oracle, Microsoft (SQL/Server) and Teradata (Extreme Data Appliance). Please see Question R.4 for more information on our Master Data Management (MDM) approach to data storage to ensure integrity and interoperability of the data we manage.

Paper and Fax Data. In the case of scanned paper and fax data, as mentioned above, this "data" is indexed and housed in our MACESS EXP, Zasio, or Emptoris (for provider contracts) systems. Please see Question 7, 16.6 (Other Electronic Data Exchange) for more information.

How Data Is Accessed

Transactional Data. Data is accessed online by internal and external users through our implementation of Role Based Access Controls (RBAC) to ensure confidentiality and compliance with the HIPAA Minimum Necessary rules. Our RBAC implementation controls:

- What data can be accessed and viewed by which user
- What data can be updated by which user

In general, all of our data access is via SQL compliant queries (e.g. direct SQL queries, or via stored procedures with compiled SQL, or via published Structured Object Access Protocol (SOAP) published web services for consuming applications.

Below is a quick summary of the online applications and how they make data accessible to appropriate users and information consuming applications: (Note, as mentioned above, data for all these applications is housed in RDBMS structures):

- AMISYS Advance: online access to submitted claims and processed claims data for our staff of claim processing.
- TruCare: our platform for collaborative care coordination, case, and utilization management, accessed by our Case Managers and Integrated Care Teams. Other information accessible from TruCare includes our TruCare Service Plan - accessible by appropriately authorized providers and members via our secured Provider and Member Portal.
- Member and Provider Relationship Management (MRM and PRM): our enterprise member and provider: services, unified communications, and master data management systems, respectively - with access to "all things member" and "all things provider" - predominantly for the use of our Member and Provider Services Representatives.
- MDE Xpress Encounter Pro: our best of breed encounter submission and workflow system, with access to all encounters and encounter processing related information, including status of encounter records with respect to receipt and acceptance by DHH's FI. Encounter Pro is predominantly used by our Encounter Business Operations (EBO) unit and LHC encounter reporting staff.
- Centelligence™: our enterprise data integration, informatics, desktop reporting and decision support system. Centelligence™ enables internal and external users to access appropriate information from our key production systems. Please see Questions R.4 and R.10 for more information. Note that we will provide secure access to authorized DHH users to Centelligence™ for online access to LHC program data for the decision support, reporting and other business intelligence uses by DHH. Please see Question R.10 for more information.
- Member and Provider Web Portals: our web-based secure portals for Member and Provider self-service and care engagement and coordination. Working with Centelligence and appropriate systems (e.g. TruCare for viewing of the TruCare Service Plan), our Portals allow authorized and appropriate access to data in our systems.

Paper and Fax Data. Depending on the image, we index by Internal Control Number (e.g. "Claim Number") for claims; as well as (if applicable) member and provider ID number - so that these images can be retrieved by appropriate business applications. For example: our Member Services Representatives (MSR's) can retrieve scanned documents through the member search screen in our online MemberConnect member services application. Please see Question 7, 16.6 (Other Electronic Data Exchange) for more information.

Data Archiving

Although we will keep all LHC data online indefinitely (if DHH wishes - see above discussion), we do archive data and documents in compliance with our state clients' policies and in line with our own retention procedures. Please see Question R.7, 16.13 (Records Retention) for more information.

Question R.2

Ensuring Integrity, Validity, and Completeness of Information Provided to DHH and the Enrollment Broker

R.2 Describe your processes, including procedural and systems-based internal controls, for ensuring the integrity, validity and completeness of all information you provide to DHH and the Enrollment Broker. In your description, address separately the encounter data-specific requirements in, Encounter Data Section of the RFP as well as how you will reconcile encounter data to payments according to your payment cycle, including but not limited to reconciliation of gross and net amounts and handing of payment adjustments, denials and pend processes. Additionally, describe how you will accommodate DHH-initiated data integrity, validity and provide independent completeness audits.

National Experience Providing Data To Public Sector State Clients.

Louisiana Healthcare Connections' (LHC) parent company, Centene Corporation (Centene), has over 27 years experience receiving, processing, reporting, and securely transmitting membership, provider, encounter, and other reporting data to our state clients and their agents, including their Fiscal Intermediaries (FI) and Enrollment Brokers. Today we receive, transmit and supply quality and timely data to 11 state Medicaid agency clients (as well as CMS for Medicare) on schedules ranging from daily to annually, depending on the specific information and data product required by our clients. We also provide secure online access to our desktop reporting and decision support tools for our state clients who require that functionality, such as DHH.

An Engineered Approach to Supplying Accurate and Complete Information.

We ensure the integrity, validity and completeness of the information we send to our state clients through ***four general architectural components*** that make up our integrated Management Information System (MIS). These four categorical components essentially trace the "flow" of data through our health plan (LHC) and to our state client (DHH and DHH's FI and Enrollment Broker):

- Our "**external facing**" application interfaces include all the capabilities and controls we deploy to support data entered or viewed ***online*** by providers using our secure Provider Portal; members using our Member Portal; and LHC staff using any of our internal business applications (claims, clinical management, etc.). We also have the capability to expose many of our portal capabilities through web services for partners that would prefer to use their native applications. Please see K.5 for more information on our Member Portal; R.11 and R.15 for more background on our Provider Portal; and R.11 for information on our internal business applications.
- Our **data and file communications** protocols, controls and supporting systems allow us to *send and receive* formatted data (including HIPAA and HL7 transactions, and state proprietary formats) with integrity, confidentiality, reliability, and assured delivery. Please see R.6 for more information on our ability to send and receive production data with DHH and DHH intermediaries using our EDIFECS EDI processing system and ancillary proprietary capabilities.
- Once we receive or collect inbound data, the **Service Oriented Architecture** (SOA) design of our interoperable application components, along with our **Master Data Management** (MDM) approach to data storage - persistence, quality assurance and distribution - ensures that our data is represented and stored accurately, completely and uniquely (e.g. no data discrepancies or duplicates). Please see R.4 for more information on the data interoperability of the application components that comprise our MIS.
- Our **Centelligence™** data integration engine, and reporting, informatics and decision support system leverages the SOA services in our architecture, as well as the near real time Change Data Capture (CDC) capabilities of our Informatica middleware - to *integrate* and *consolidate* data, and to create the information products we supply to our state clients. Once a report or data extract is ready for a state client, Centelligence™ then uses the services of our data and file communications subsystems (above) for reliable transmission to our state clients or their intermediaries.

Audit logging and tracking tools are a common aspect of *all* of the above capabilities. We use audit tracking mechanisms at both the application level (for example, date/time, user ID, and record level update audit tracking in our AMISYS Advance claims system and other business applications); and at the

relational database management system (RDBMS) level - through the native audit logging and journaling functions in our Oracle, Microsoft SQL/Server, and Teradata Extreme Data Appliance software.

We are experienced in ensuring that auditors have the access to the systems, documentation, control artifacts and data they need to do their tests, and we will be ready to accommodate any DHH initiated audit activities. Please refer to R.15 for more information.

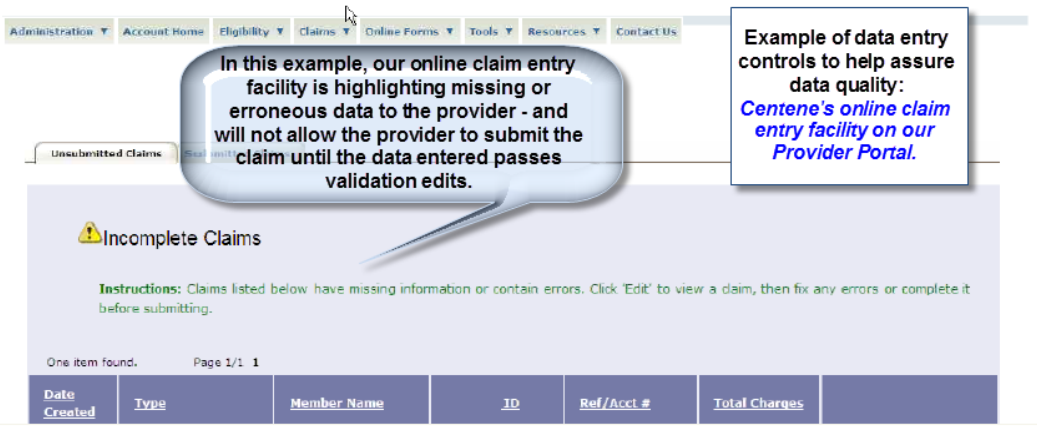
External Facing Applications Help to Enforce Data Quality on the Front End. Much of the data that users enter into our MIS will eventually be reported by us to DHH either directly or indirectly (e.g. used for aggregation into summary reports, and/or used in the computation of statistics for DHH). Thus it is critical for our externally facing applications, such as the online interfaces to our internal applications, and our Member and Provider Web Portals, to facilitate the entry of "clean data" by users who are authorized to enter that data.

There are two general sets of controls we use to ensure that data entered into our MIS has quality and integrity:

- Secure access controls to ensure that only authorized users are entering data appropriate to their "role"; and
- Data entry field level edits

Access Controls. We use network level security, Oracle's Virtual Private Database (VPD), Microsoft Active Directory Application Mode (ADAM), Teradata's Enterprise Security Model, IBM Tivoli Directory Server (TDS), and application level authentication, along with Role Based Access Control (RBAC) to control what applications a user may have access to; what information they can view; and *what data they can view, edit or update*. Please refer to R.16 for more information on our access controls and methods.

Data Entry Field Level Edits. All of our applications - including those on the web, enforce an appropriate degree of field level edits - ranging from simple alphanumeric formats (e.g. HIPAA standard lengths for name fields), to more sophisticated edits (NPI check digit validation), to (wherever possible) the use of drop down lists to prompt valid field data choices, to situational field logical checks (e.g. if user enters a value in one field, this drives the mandatory entry of data in another field). Figure R.2-A below is an example of how our applications help users enter syntactically valid data. This particular example is from our HIPAA Direct Data Entry (DDE) compliant online claim submission application - available to our network providers on our secure web based Provider Portal.



Protected Health Information has been removed from this exhibit.

The Role of SOA and MDM in Internal Applications

Once validated, "clean" data is received in our MIS (via online entry or batch processes, such as EDI claims receipt), the data is available to our business applications via our SOA approach to application interoperability. We also ensure data integrity through a Master Data Management (MDM) approach to data stewardship. Thus, for the core and central information components in our operations:

- Our Member Relationship Management (MRM) system is the "system of record" for ***member related*** data, and employs a "master member index" to link together all member specific information and history (including, for example, links to clinical records in our TruCare clinical case and utilization management system, and claim records in our AMISYS Advance claims processing system).
- Similarly, our Provider Relationship Management (PRM) system is the "system of record" for provider related data. Specifically, the Portico provider data management subsystem of our PRM is the central repository of key provider identifier, demographic, affiliation, specialty, and other pertinent data used by all business applications for the appropriate job at hand (e.g. claims payment by AMISYS Advance, service authorization in TruCare).
- Our AMISYS Advance system is the MDM component for claims; and MDE Xpress Encounter Pro is our "system of record" for encounters data.

The combination of our SOA and MDM application architecture allows us to enforce specific data integrity controls within the appropriate system of record (MRM for member data, PRM for provider data, AMISYS Advance for claims data, etc.), while allowing each application to interface with each other via our message oriented middleware architecture supporting service calls, automated Extract / Load / Transport (ETL) processes, database interfaces such as Open Database Connect (ODBC), and Change Data Capture (CDC) processes - whichever interface is appropriate for the specific situation.

Thus, for example, TruCare issues service authorization information to AMISYS Advance via an SOA service, so that AMISYS Advance can adjudicate claims when they arrive, against those service authorizations.

In summary: Once data is received into our MIS, it is not logically duplicated, and only the system of record can alter that data - an approach that assures the highest possible level of integrity for downstream reporting and information support.

Please refer to R.4 for more information on the interoperability of our software components, and our approach to MDM.

Centelligence™: Where Data Comes Together to Meet DHH Information and Reporting Needs.

Centelligence™ is our integrated data warehousing, decision support and healthcare informatics solution. Our Centelligence™ enterprise platform integrates data from multiple sources, including our internal business applications, to produce actionable information, including the data extracts and reports that our state clients require.

At the heart of Centelligence™ is our Enterprise Data Warehouse (EDW). EDW integrates medical, behavioral, and pharmacy claims and lab test results, member and provider demographics, clinical care information, and Health Risk Assessments (HRA's) into a centralized, relational database repository. Centelligence™ capitalizes on our SOA architecture, employing our Informatica ETL and near real time Change Data Capture (CDC) middleware, along with TIBCO's Java Messaging Service (JMS) software, and open database interfaces protocols (such as ODBC) - all employed to connect with our operational, transactional RDBMS systems, including:

- Our EDIFECS EDI processing system
- TruCare clinical care and utilization management platform
- MRM master member data management system. Among other data, MRM sends member demographic information updates to EDW. These are updates that the member self-reports to us, e.g. when a member calls our Member Service Representatives (MSR's). Through EDW, we will send

these updates to the Enrollment Broker, at DHH's direction, and in the format dictated by DHH. We can supply this information in HIPAA 834 or proprietary format. We can schedule these transmissions on a daily, weekly, or other schedule to suit DHH needs.

- PRM master provider data management system. Similar to MRM, PRM sends provider demographic and other updates to EDW, and from EDW we will send provider registry data as stipulated in the RFP and in Appendix G of the CCN-P Systems Companion Guide
- AMISYS Advance claims processing application
- MDE Xpress Encounter Pro system for encounter data production and associated workflow. From EDW, we will transmit encounter data to DHH's FI in HIPAA 837 compliant format through our EDIFECS EDI system to insure both data integrity and HIPAA compliance for the outbound encounter data.

EDW is essentially the high performance data "junction" in our MIS - the system where operational, transactional data is integrated and consolidated - and available for a variety of informatics and reporting applications, including the information we will supply to DHH and DHH's FI and Enrollment Broker. Please refer to R.10 for more information on our Centelligence™ reporting capabilities.

All of the interfaces in and out of EDW have their own mechanisms and audit trails to assure data integrity and process transparency (e.g. for data message integrity), but, in addition, we assure continuous data quality in EDW *itself* through a number of ongoing controls. As an operating principle, EDW presumes that inbound data is inappropriate for loading until quality validations are complete and data errors are within tolerance range. For example, EDW can reject data through automated validation and notification processes at the file level when the number of record errors in the file exceed tolerances. In these situations EDW tags individual data records with a full set of identifiers noting all issues with the data record, in the event the number of errors are within a pre-set tolerance but where the individual data issues may be of interest to applications or systems using EDW's data. EDW performs quality checks horizontally, vertically, referentially and temporally (trending) to ensure both content quality and *prevent* data duplication, and data over- or under-representation.

During 2010, we implemented a *significant* upgrade to our EDW with the incorporation of the Teradata® Extreme Data Appliance. This major capital investment significantly improves our ability to handle **truly large amounts of data** (hundred of Terabytes of information) in much shorter timeframes (hundreds of times faster than a traditional DBMS), resulting in more timely data sharing and reporting.

Data Exchange Controls to Ensure Transmission Integrity

Once information is prepared by EDW and ready for transmission, our COVIANT Diplomat Transaction Manager (COVIANT) handles our automated, scheduled file exchanges (transmission and receipt) with our state clients and/or their FI's, Enrollment Brokers or other authorized Trading Partners. We support all standard industry data communication protocols such as Secure FTP–SFTP (SSH), FTPS (TLS/SSL), PGP encryption over the internet or via a Virtual Private Network (VPN). COVIANT protects our file exchanges with access control, authentication, and secure configuration features for total data integrity protection during transmission. From an internal data networking perspective, our network backbone is highly redundant through a mesh design that provides multiple paths to and from each point, allowing maximum network *availability* to our state clients and, for example, enabling us to meet DHH transmission schedules.

In addition, our EDIFECS and TIBCO software suite, in conjunction with Coviant – supports a wide range of *file transmission acknowledgement* protocols, including proprietary formats as well as ANSI standard 997, 999, TA1, 831, and 824 formats. We encourage the use of acknowledgements for both file transmission and receipts - as a further control for assured delivery, data integrity, and record balancing. We also encourage the use of Public Key Infrastructure (PKI) security implementations not only for encryption but for sender authentication purposes - ensuring not only that the file was transmitted un-tampered, but that the receiver can validate *who the sender was* as well.

Encounter-Based Controls and Edits

Our end-to-end encounter processing cycle, from provider claim submission through encounter record acceptance by our state clients, leverages the same data quality controls and techniques described above. There are, of course, pertinent distinctions and details that we would like to review below.

Controls to Validate Claims Data: Critical for Successful Encounter Processing. *Claims data* submitted from our providers is a major "ingredient" to the information we ultimately supply to our state clients; most prominently in the form of *encounter data submissions*. Thus, no discussion on encounter data quality is complete without an understanding of the data integrity controls in our claim submission process.

Ensuring Quality in EDI Submissions. Today, more than 85% of claims submitted to us are submitted as HIPAA EDI transactions, and we have a long standing and large investment in processes and controls to ensure the systematic and "up front" validation of HIPAA claims. We validate all electronically submitted claims data, including the HIPAA 837 Professional (837P) and 837 Institutional (837I) claims transactions, using EDIFECS XEngine (XEngine) software. XEngine supports HIPAA compliance standards as defined by the Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP), and allows us to configure edits and testing scenarios, for our specific business rules. XEngine validates data against X12 syntax and rules for data structure; tests to ensure conditional rules requiring secondary fields are completed accurately and completely; and ensures all data is in compliance with our HIPAA Companion Guides (we will review LHC's HIPAA Companion Guides with DHH and/or DHH's FI during implementation activities). These upfront edits not only ensure that transactions are compliant with Federal mandates and DHH rules, but also allow us to recognize and immediately communicate to providers and Trading Partners (e.g. clearinghouses) any problematic claim submissions in the earliest stage of the process, through our transmission of ANSI TA1 and ANSI 997 Functional Acknowledgements (FA), and the ANSI 999 FA for HIPAA 5010 transactions, which we will support beginning 1/1/2012.

We have recently offered providers the option of submitting HIPAA EDI claims to us *directly* (in lieu of submission via a clearinghouse), and we are enhancing our EDI support for directly submitting providers or other Trading Partners (e.g. billing agents) with our introduction of EDIFECS Ramp Manager in the second half of 2011. Ramp Manager validates against our transaction rules and provides immediate feedback on any errors that the provider or other Trading Partner can then correct. Our overall objectives with Ramp Manager are: i) to further assist providers in their efforts to capitalize on the speed and efficiencies offered through EDI processes; and ii) for Centene and LHC to obtain the highest quality data possible for health plan operations and submission to DHH.

We currently validate EDI claims submitted to us to SNIP Level 4 (Situational Compliance) and are beginning to test Level 5 (Codeset Compliance), and have the capability of enforcing up to a HIPAA Level 7 leveraging EDIFECS XEngine and Ramp Manager tools, and 2011 we will increase the number of front end EDI validation edits we make to include code set and code combinations. We will work closely with DHH as we define the timeline and key milestones as we move to Level 5 (or higher), and we will support this transition through our provider education programs. In our experience, it is critical to increase compliance levels *smoothly* and in *synch* with the EDI capabilities in the provider community - balancing the need for providers to file claims and have them accepted by LHC swiftly with the need to collect "clean data" for subsequent state reporting.

Ensuring Data Quality From Paper Claims. Approximately 90 percent of all paper claims we receive can be indexed and converted into machine readable data through the use of Optical Character Recognition (OCR). We use MACESS EXP Form Works Optical Character Recognition (OCR) software to greatly enhance the accuracy of machine readable data from the paper and fax claims we receive from providers. We encourage, train, and support our provider to move to electronic claims submission; or to use standard "OCR friendly" red ink paper claim forms with typed or clearly written data if a provider must use paper.

Once we have captured the claims data into machine readable form, that "paper claim" data is ***treated identically*** to EDI claims we receive, or claims that our providers enter directly via our Provider Portal using our DDE online claim entry application.

Identical Validation and Edits for Electronic and Paper Claims. All claims data we receive (paper or electronic) is loaded into pre-adjudication tables managed by our *TIBCO BusinessWorks*™ (BusinessWorks) for validation of member and provider fields. For example, BusinessWorks compares the member data we have on file in our Member Relationship Management (MRM: our enterprise master data management system for "all data member related") with member information on the submitted claim on the claim. If a claim transaction is rejected for any of the specific reasons configured in BusinessWorks, a notification is automatically provided to the EDI Trading Partner or provider outlining the reason for the claim rejection. The types of edits performed in BusinessWorks include (among a number of other data quality checks):

- Member Validation– confirms presence of member record in our systems.
- Provider Validation - confirms presence of provider record in our systems.
- Validate Dates of Service – confirms that the claim date of service is valid and does not contain a future date.
- Diagnosis Code Validation/ICD9 tables – confirms the presence and accuracy of ICD9 codes.

Adjudication in AMISYS Advance. Claims data that passes all HIPAA compliance, codeset edits, and data validation is then systematically loaded into our AMISYS Advance claims processing system for adjudication, including application of health plan rules (covered services), verification of member eligibility for the dates of service on the claim, matching (if applicable) of claim to service authorizations, application of appropriate fee schedule based on the provider information on the claim, edit checks for third party liability, and several other automated edits and processes, until the claim is finalized to a paid or denied status. Please see Section Q, Question Q.1 for more information for details on our claims adjudication process, including our real time automated process to handle any claim pends.

Encounter Record Preparation. Once AMISYS Advance adjudicates claims to a finalized status, our MDE Xpress Encounter Pro (Encounter Pro) encounter workflow system will extract, prepare and submit the data as encounters to DHH, via EDW and EDIFECS (for application of HIPAA compliance rules of our outbound HIPAA 837 encounter data). MDE (the creator and supplier of Xpress Encounter Pro) has a proven track record within the Medicaid industry of providing "best of breed" submission and correction functionality to meet encounter submission guidelines as required by all our state partners. We will configure Encounter Pro to submit encounter data that complies with all DHH standards for electronic file submission, standard HIPAA file format (specifically including ANSI X12N HIPAA 837 provider-to-payer-to-payer COB transaction format), file size, submission frequency, and submission method as required by DHH. Our encounters capture the same line item detail regardless of the claim type, disposition (e.g., paid or denied), third party liability indicators or capitation arrangements. We include all rendered services, original and adjusted claims, application of retroactive fee or member changes, etc., in a *single* encounter file as appropriate for the claim type, and we can include encounters we receive from OptiCare Managed Vision® (OptiCare), LHCs affiliated vision benefits subsidiary and subcontractor, for submission to DHH's FI. We also adhere to NCQA, AMA coding, UB-04 editor, NCCI, and DHH standards regarding the definition and treatment of certain data elements captured on claims, use of standard codes (including CPT Category I and II , HCPCS Level II and ICD-9-CM), counting methods, units, etc.

Centene will retain all data elements in our claims history necessary for creating encounters in compliance with DHH and the Fiscal Intermediary requirements.

Specific functionality provided by Encounter Pro includes, but is not limited to:

- Support of DHH-specific business rules to “scrub” data prior to submission

- Automation of LHC defined actions, in conformance with DHH guidelines, to correct *repairable* encounters
- Linkage to our base claim database, outbound encounters, and inbound acceptance reports to facilitate comprehensive encounter reconciliation efforts - from provider submission, through claims processing, to encounter production
- Automated prioritization of encounter correction activities
- Extensive operational and executive reporting to identify encounter trends, monitor acceptance rates, and proactively correct issues, through integration with our Centelligence™ Insight desktop reporting system
- Automated extract and delivery mechanisms to minimize bottlenecks and the need for manual intervention - assuring process consistency.

As mentioned above, Encounter Pro includes a module which provides a 'pre-submission scrub' mechanism to customize and apply edits to as a final check for encounter accuracy prior to submission to the state. We will configure Encounter Pro to recognize conditions that will cause an encounter to deny at DHH and hold the encounter record and corresponding claim for review. This will allow us to work with providers to correct any issues and/or reprocess the claim for a valid encounter submission to DHH.

Once processed, the encounter data is batched into appropriate HIPAA standard 837 files and will be submitted in accordance with DHH timeliness requirements via our secure, auditable, COVIANT file transfer system (see discussion above). Encounter response files are also processed by our Encounter Pro application, updating the encounter history and identifying encounters that must be re-processed. Encounter Pro provides an online management tool and extended reporting for encounter submission and response analysis. For example, if errors are reported in the DHH response file, Encounter Pro provides a platform by which each error can be researched by our Encounter Business Operations (EBO - our Centene nationwide encounter processing center of excellence) and LHC encounter staff. Once we determine the solution to the error, we re-process the claim in AMISYS Advance and the encounter is then resubmitted through Encounter Pro.

Encounter Reconciliation. Each month, LHC will balance paid claims and encounters to ensure submitted encounter batches are complete. Using our Centelligence™ Insight reporting platform (see response to Question R.10 for information on Centelligence™ Insight) we will compare total claims payment amounts to the total payment amounts processed within Encounter Pro on a monthly basis**.** These totals are then compared to the total paid amounts contained in that month's encounter submission. Using this process, we account for every paid dollar and we verify that all finalized claims have been processed as encounters and is inclusive of all payment adjustments, settlements, pends and denials. Similarly, we ensure the reconciliation of other key claim statistics including claim count, service line count, total gross charges, as well as procedure and diagnosis codes. We pay special attention to ensure the accurate and complete submission of encounters from our capitated providers to ensure we capture the full and complete encounter history for our members.

Centelligence™'s EDW houses both paid claims data from AMISYS Advance (and this paid claims data is immediately updated in EDW after every pay cycle); and EDW houses encounter data from Encounter Pro (with the most recent encounters processed), greatly accommodating flexible reporting support for encounter reconciliation. To compare encounter data to our financial lag, we utilize monthly lag data and compare "claim-to-encounter" and "claim dollar - to - encounter dollar" amounts: including billed charges ("gross"), allowed amounts and paid amounts; all possible because these dollar amounts are present on both the processed claims data - and encounter records - in Centelligence™. If any gap or difference is identified, EBO specialists conduct a focused analysis to identify the root cause and resolve the discrepancy.

For additional detail on our encounter data management process, and our EBO, please see R.5.

Audits to Ensure Systems and Data Integrity

Centene currently undergoes several routine audits to ensure the integrity, validity and completeness of all data we process and store. Our audits include all aspects of system processing such as financial and claims controls, network and physical security, application security and regulatory compliance.

We ensure HIPAA compliance through systematic monitoring, internal, and external audits. Centene's Compliance Department uses Compliance 360 software which incorporates updated databases of federal, State, HIPAA, and accreditation agency regulations. Centene's Internal Audit Department regularly evaluates our operations and systems to ensure risks have been identified, impact assessments are conducted, and adequate mitigation controls are deployed to minimize risk per HIPAA Risk Assessment requirements. Please see R.15 for more information on how we comply with Federal mandates.

Our IT Security Department conducts monthly penetration tests on our systems to attempt Denial of Service attacks, phishing, spoofing and social engineering. We use these tests to identify and correct potential risks. In 2010, Centene engaged Ernst & Young to review Centene's IT risk profile to ensure that we had identified appropriate risks, their potential severity, likelihood of occurring, and impact. Ernst & Young had no material findings in that audit. Our HIPAA IT risk profile is used in Centene's Enterprise Risk Management (ERM) process, which includes an ongoing review and assessment of Centene's risk environment with senior management.

Centene health plans routinely undergo audits conducted by State agencies to evaluate the accuracy and completeness of our data (including encounter data). Centene takes pride in successfully meeting all State expectations regarding the exchange and maintenance of our data and will be committed to meeting all DHH data integrity requirements. Given appropriate notice, we will accommodate all DHH-initiated data integrity and validity audits by providing any necessary materials or documentation as requested or providing DHH with on-site access to systems and resources necessary to conduct the audit. We look forward to working with DHH on establishing audit requirements and protocols.

Finally, in order for LHC to ensure that we have developed and continually maintain effective information systems controls we utilize both internal audit (Ernst & Young) and external audit (KPMG) professionals to conduct a SAS 70 Type II audit. Statement on Auditing Standards No.70 (SAS 70) is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) in 1992. It is used to report on the "processing of transactions by service organizations", which can be done by completing either a Type I or a Type II audit. A SAS 70 Type I is known as "reporting on controls placed in operation", while a SAS 70 Type II is known as "reporting on controls placed in operation" and "tests of operating effectiveness". Centene participates in the Type II audit the 4th quarter of each year. This ensures that we maintain the highest quality while enforcing the lowest risk to our production systems. In addition to the above formal audit, we utilize our own Internal Audit department to review our controls each quarter to validate both the quality of the control as well as the activities related to our controls.

Question R.3
Ensuring Availability of Systems

R.3 Describe in detail how your organization will ensure that the availability of its systems will, at a minimum, be equal to the standards set forth in the RFP. At a minimum your description should encompass: information and telecommunications systems architecture; business continuity/disaster recovery strategies; availability and/or recovery time objectives by major system; monitoring tools and resources; continuous testing of all applicable system functions, and periodic and ad-hoc testing of your business continuity/disaster recovery plan.

Identify the timing of implementation of the mix of technologies and management strategies (policies and procedures) described in your response to previous paragraph, or indicate whether these technologies and management strategies are already in place.

Elaborate, if applicable, on how you have successfully implemented the aforementioned mix of technologies and management strategies with other clients.

Centene Corporation (Centene) will manage the Management Information System (MIS) on behalf of Louisiana Healthcare Connections (LHC). Centene engineers the hardware, software, communications, and processes in our MIS to ensure that our applications are available for our internal staff, providers, members, and state partners, such as DHH, with the least possible disruption. We maintain and continually enhance the availability of our MIS related capabilities through the design of redundancy we factor into the hardware, software, and networking components of our MIS architecture. All of the MIS infrastructure technologies, MIS service management strategies, Incident Management, Business Continuity and Disaster Recovery policies, procedures, and processes supporting our MIS offering to DHH are *in place today*, serving nearly 1.6 million members in full-risk managed care programs in Centene's 11 affiliated health plans across the United States.

Recently, we have successfully implemented and operate these solutions for our plans in Illinois and Mississippi, and these are the same solutions that support all our operations in 11 plans across the United States. We also design and test hurricane-specific disaster responses in our markets that face the threat of hurricanes, including Texas, Mississippi, Georgia, and Florida. As described below, we will extend these exercises to include LHC.

By Q4 2011, Centene will also complete construction of our new, fully-functional, Tier 3, 19,000 square foot datacenter, with capacity for over 165 IT racks; 6,000 square feet of datacenter floor; and fully redundant environmental, power, and network connectivity systems. This new datacenter will provide us with full redundant capability, with our current datacenter serving as our failover operation, reducing our recovery capability from hours to minutes in most cases. For large-scale MIS events, *Centene targets to restore all centralized MIS operations within **12 hours** of the declared disaster* as defined below. This is well before DHH's requirement of 72 hours. Please see our discussion below for more information about our recovery time objectives and new state-of-the art datacenter. Further, our telecommunications architecture is engineered so that *mission critical phone communications* remain available at all local sites.

We have protocols in place to help manage an emergency either localized at the LHC office, Centene datacenter, corporate offices, or if the event is regional. LHC plan management will be responsible for notifying DHH of any event that affects our ability to serve our members and providers and the state, and will do so within the timeframes required by DHH. We will also provide DHH will contact information for all our key personnel both at LHC local offices and Centene Corporate so that DHH is able to reach out to LHC in the event of a large scale emergency. Please see below for more information on our Business Continuity and Disaster Recovery notification and activation procedures.

Hardware Architecture Engineered for Availability

Our MIS architecture is based on these principle design points:

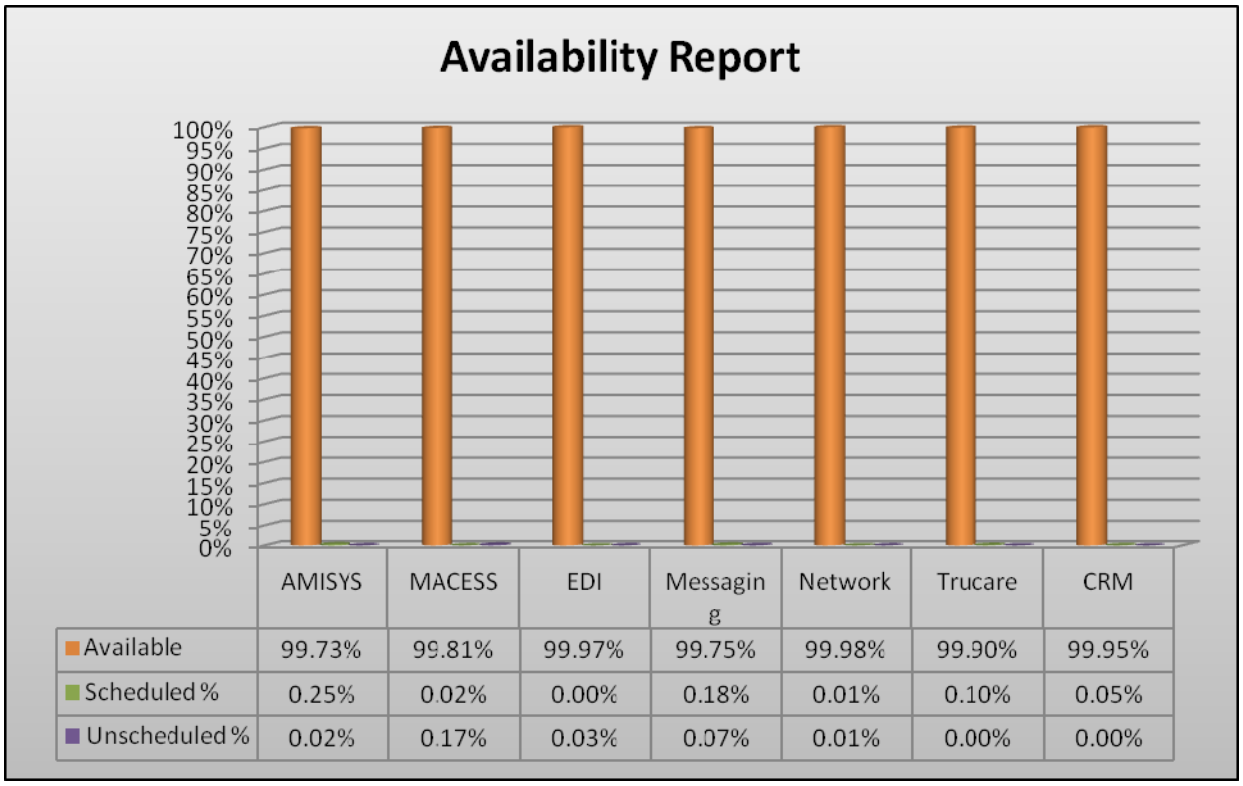
- ***High Availability*** is achieved through effective risk mitigation strategies and by maintaining extensive redundancy in our entire computing infrastructure and network features. For example, our

use of Virtualization provides an optimal solution to deploy and manage applications while also maximizing application availability and integrity.

- ***Utilizing Industry Standard and Best In Class*** operating systems (e.g. Windows, Linux, HP-UX), virtualization platforms (e.g. VMWare VSphere, Citrix XenServer and XenApp), application software (e.g. Amisys Advance, Microsoft CRM, TruCare, etc), and hardware components from hardware leaders, such as Cisco, Hewlett-Packard, NetApp, EMC, Wyse, and Avaya. Our use of *Blade Servers*, *Virtualization*, *Clustering*, *Storage Area Network*, and *hardware redundancy* affords us the availability and performance to power the three broad tiers of our systems architecture, which are presentation, application, and data storage.
- ***Scalability and Flexibility*** to maintain agility in our MIS, allowing for quick changes based on business imperatives. From a *hardware* perspective, we realize these principles through a "computing utility" approach, which is the ability to expand the ***capacity*** of our operations without affecting the availability of current business operations and deliver computing power and reliable data storage any time, to any application and in any amount.
- ***Monitoring and Service*** to achieve and maintain high availability; monitoring our environment to anticipate problems; service our members, providers, government customers and plan staff; and address situations before there are issues.

Our rigid adherence to the above principles leads to solid performance results as illustrated in the Availability graph below for the preceding 12 months of service, which serves as a testimony to our successful implementation of the integrated technologies and management strategies we have implemented in 11 states.

System Availability Report June 1, 2010 Through June 1 2011.



	AMISYS	MACESS	EDI	Messaging	Network	Trucare	CRM
Available	99.73%	99.81%	99.97%	99.75%	99.98%	99.90%	99.95%
Scheduled %	0.25%	0.02%	0.00%	0.18%	0.01%	0.10%	0.05%
Unscheduled %	0.02%	0.17%	0.03%	0.07%	0.01%	0.00%	0.00%

Our Server Architecture - Delivering the Right Processing Power. We use proven, industry standard hardware components for our core processing applications and to deliver the necessary computing power to our local plans. These are realized in each layer of our architecture described below in the following

categories: *Database Layer, Business System Layer, Presentation Layer, Network Layer and Telecommunications Layer*.

Database Layer. All core LHC data (claims, member, provider, etc.) will be stored on our fully redundant Storage Area Network (SAN), which supports access to 2 highly available NetApp SAN Storage Arrays configured with over 200 TBs of shared storage *(Reference Figure R.3-A: Data Storage Architecture).* Our Centelligence™ family of reporting and decision support applications is powered by our Teradata® Extreme Data Appliance.

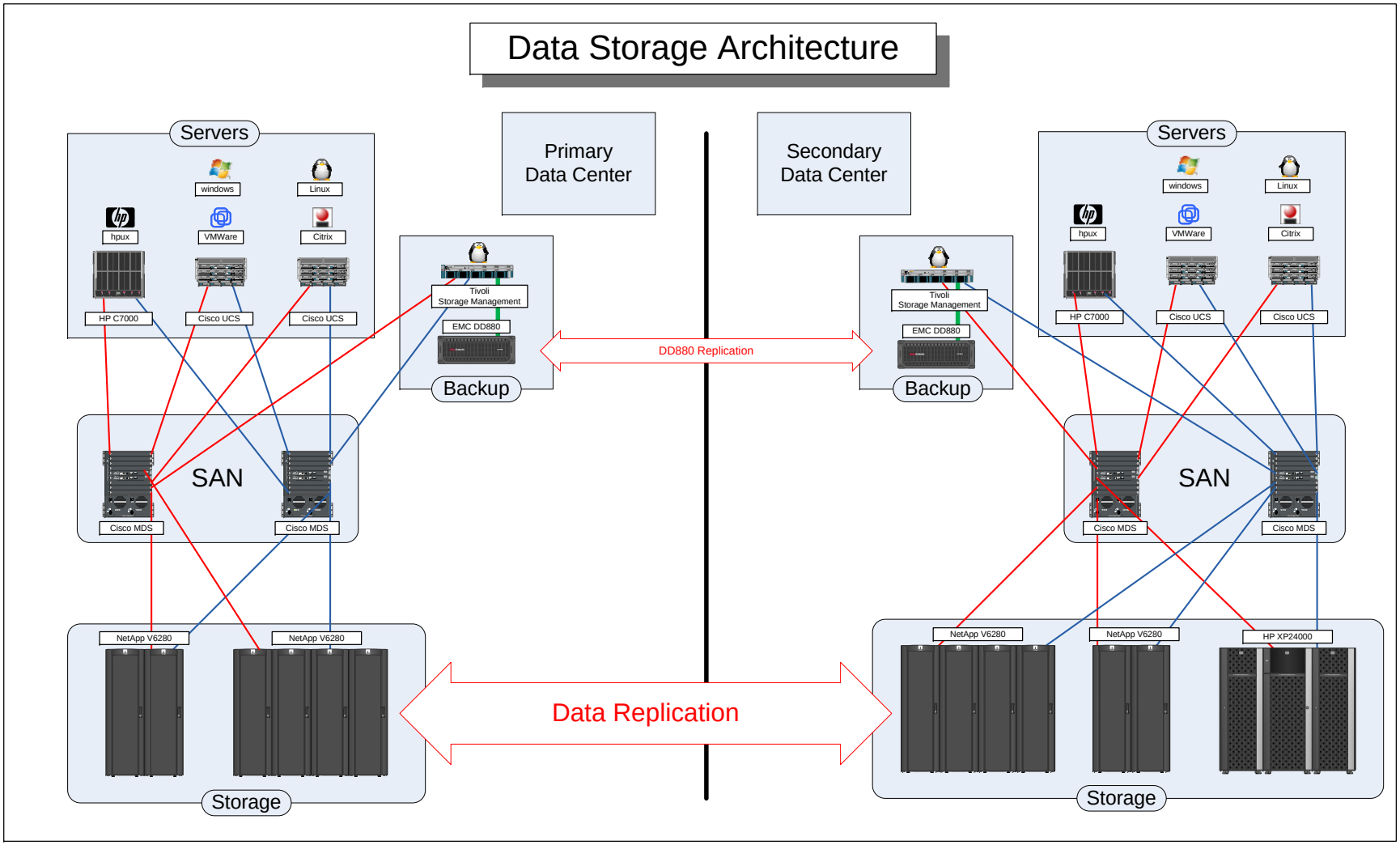
Protecting DHH Data Records - Systems Backup/Recovery. Starting in Q3 of 2011, all Tier 1 and 2 data will be continuously replicated from our primary corporate datacenter to our secondary datacenter for the purposes of high-speed disaster recovery. However, for routine data recovery, system backups are performed on all Centene servers using an Enterprise class backup software package from IBM, called Tivoli Storage Manager (TSM). All database transactions are logged and written to high-speed media several times per day. All data is written to a tapeless environment using a pair of backup storage devices (EMC DD880). One device serves as the primary device and the second device is replicated to the secondary datacenter facility. Daily backups are retained for 30 to 60 days following the original backup. In addition, a backup archive is generated and maintained once per month, according to HIPAA regulations, using traditional tape backup. These tapes are sent offsite to a secure, climate controlled, fireproof facility. Access to offsite tape media is limited to key Centene employees and is strictly enforced by our Tape Management vendor. Centene's Enterprise backup strategy enables us to provide business continuity and a robust backup capability with virtually no chance of data loss. Our new dual datacenter, described below, will be available in Q4 of 2011 to support replicated data on a near real-time basis for our tier 1 databases and applications. This will provide additional recovery points that create more depth of recovery and a more agile recovery environment.

While the necessity of a good backup solution is obvious, the whole intent of the backup strategy is to manage a recovery scenario in the most efficient way possible. This includes file recovery, database recovery, or even a full data center recovery due to an unexpected disaster. A summary of the key features available with our backup solutions include:

- Automated, operator-less backups and restores
- Fast online backups to high-speed media backup storage device (EMC DD880) and monthly tapes
- Fast single file, database or full system recovery
- Robust Tape Management facility to manage the location and protection of all tape media
- Complete catalog containing a history of all backup data at its location on media
- Replicated backup storage device and automated tape copies for offsite storage and Disaster Recovery needs.

When our local health plan offices have need for a local server, a full Windows Server system backup is performed on a nightly basis. This allows for the ability to recover local files in the event of a server failure. A standard generational back-up tape rotation is used with a 5-week cycle, monthly tapes are held for 18 months and yearly tapes are held indefinitely. Tapes are rotated offsite daily to a secure, climate-controlled, fireproof facility. For security reasons, recovery of the tapes is limited to select Centene personnel. In the event of an emergency, the backup tapes can be recovered from the secure backup facility in one hour.

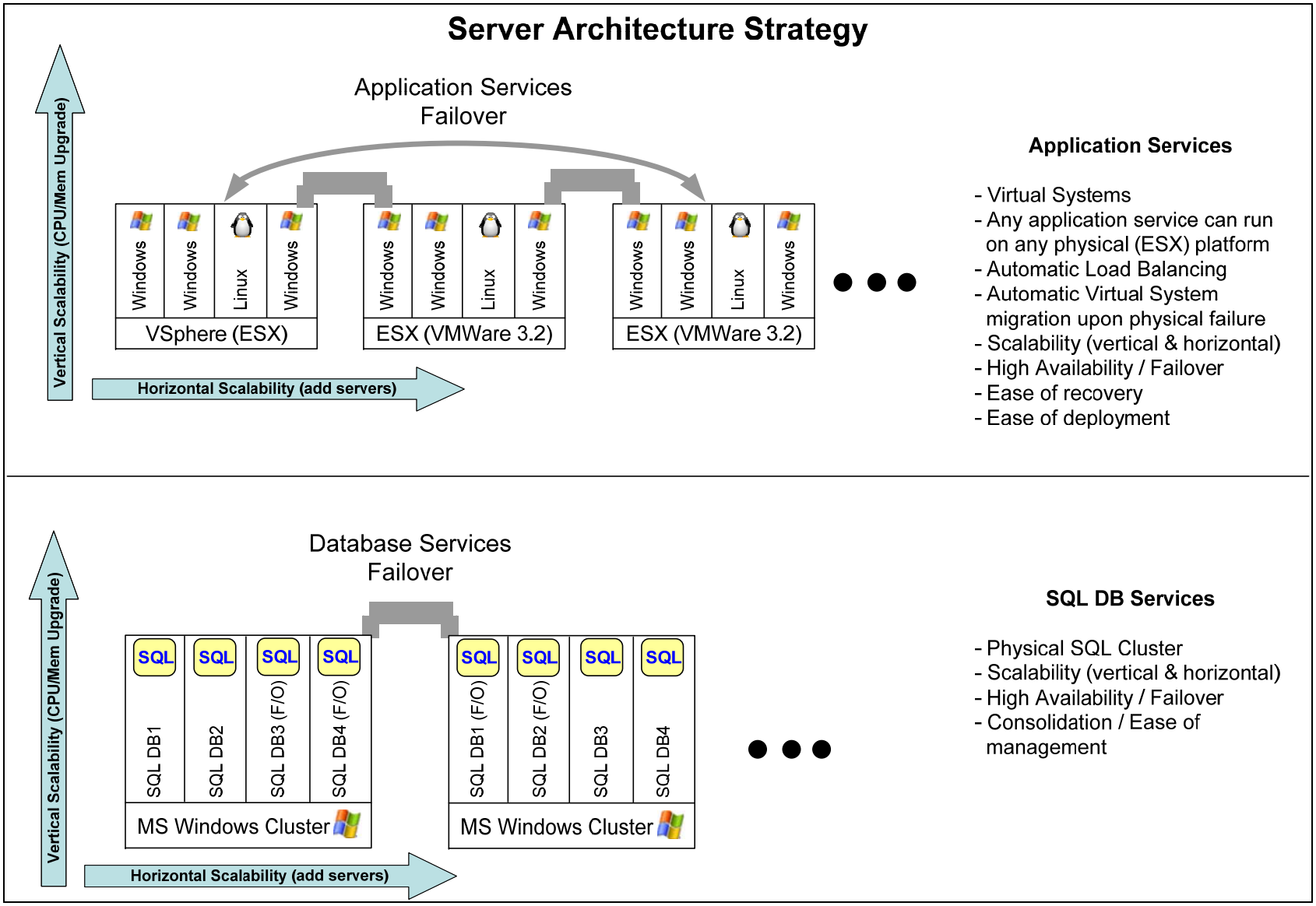
Figure R.3-A: Data Storage Architecture



Business System Layer - Engineering Performance and Availability in Servers and Storage. Five HP 9000 servers running HP/UX Unix power AMISYS Advance, our core eligibility and claims processing system. Three *application* servers operate as a cluster using Veritas technology and are configured to provide a scalable, redundant computing array for our claims platform. Three *database* servers use Oracle 10g Real Application Clustering (RAC) for high availability and are configured to provide a fully redundant, scalable architecture for our claims data. Two batch servers, capable of backing each other up, are configured to run all claims management jobs. Each of these clustered solutions are designed to grow in capacity either vertically (adding more CPU's and Memory) or horizontally (adding additional nodes) to meet our processing needs. For our Clinical Applications (such as our TruCare clinical system), we use rack mounted Windows/Intel ("WinTel") blade servers operating in a virtual environment, using EMC's VMware VSphere virtualization software technology.

Our multi-tiered hardware platform delivers highly available application services using Clustering, Server Virtualization, and Blade Servers. Clustering technologies, including Oracle RAC, VMware, Windows Server 2008r2, and Citrix, allow us to deliver presentation, application, database, and networking services across a group of server nodes configured so that any one of the nodes can provide appropriate end-user access. *In the event that one of the nodes is lost, the surviving nodes pick up the workload, usually averting an outage*. With the use of VMware's Server Virtualization Infrastructure and High Availability Services, we deliver a fully redundant server farm capable of running a number of different application services. Virtualization, as pictured below (*Reference Figure R.3-B: Windows Server Architecture Reinforces Availability*), reduces our power consumption and air conditioning needs, and optimizes the amount of CPU performance and data storage that we can house in our building space. Virtualization also provides high availability for our applications, and streamlines application deployment and migrations. The servers are automatically load balanced to provide the best performance. If one of the physical nodes were to fail, be taken out of service for maintenance, or experience higher than expected utilization, the application service automatically moves to another node in the server farm without any interruption to the application service (i.e. no impact to the user). Because our MIS is architected for horizontal and vertical growth, we do not anticipate any changes in our current infrastructure footprint or design. Through our existing vendor relationships, we will easily be able to grow horizontally adding the necessary servers into vacant positions within our existing environment and vertically upgrading the Central Processing Unit to service DHH and our LHC member population.

Figure R.3-B: Windows Server Architecture Reinforces Availability.



Presentation Layer (User Desktop). We deploy virtual desktop and remote application support using Citrix XenDesktop, XenServer, and XenApp products. Essentially, a virtual desktop separates the workstation computer hardware from the operating system and client applications that are utilized by the end-user. Our corporate datacenter in St. Louis, Missouri, will centrally run and maintain All LHC programs, applications, processes, and data. Our high-speed network, described above, will connect LHC virtual desktops to our centralized IT resources. We configure, provision, and use a standardized desktop environment for all Centene and health plan staff with operating systems that include Desktop Windows Server 2003, SP2 with Citrix XenApp 4.5 for thin clients, and Windows XP, SP3 for desktops and laptops. We use IBM WebSphere technology web and portal platforms operating on Red Hat Enterprise Linux. WebSphere Portal Server (WPS) is used to integrate our electronic business applications across multiple computing platforms, using Java-based Web technologies. Centene was selected as a finalist in the 2010 Citrix Innovation Award for our rapid deployment of virtual desktops.

Centene's preferred approach to desktop workstation hardware demonstrates our commitment to utilizing industry leading technology solutions to provide superior performance to the end user while maintaining the highest levels of information security and availability. Please see our response to R.7 for a table which correlates RFP Workstation Hardware and Software requirements with Centene and LHC deployments.

Our virtual desktop approach, also known as a "thin client," allows our standardized PCs to present an engaging, intuitive, and responsive interface to the user, while the enterprise servers house our high transaction, critical business applications and data in a safe and reliable computing environment, which is the kind of large scale, environmentally secure infrastructure that only an enterprise scale installation can deliver. We have moved to the "thin client" approach for reasons list below, based on experience learned from setting up field offices across our affiliate plans in 11 states.

- Data Integrity. Because Protected Health Information (PHI) and LHC's core applications and operational data will be housed in our central datacenter, LHC will benefit from all the infrastructure support of our corporate datacenter including our data integrity controls, back-up capabilities, audit trails, help desk support, described in detail below.
- Business Continuity. With centralized data, our local plan's information is safe in the event of any local site disabling events, and further, operations can continue from any other location throughout our enterprise.
- Confidentiality. VDI and thin client hardware support more secure operations. The theft risk of the thin client, virtual workstations is reduced because they do not have any operating hardware or system software stored locally on the machine. Further, Protected Health Information (PHI) is better protected because it is not stored on the virtual desktop; it is only accessed through the virtual desktop. Our encrypted laptop drives also contribute to data confidentiality and secure operations.
- Centralized application control. Changes to our core business applications can be developed and systematically deployed by our MIS staff across our network from a central location, which allows for easy, quick, noncomplex, and non-risky business and technical changes and upgrades, including specific changes for a particular health plan such as LHC. We are also able to more effectively and efficiently deliver rapid upgrades and patch deployments because these are done centrally in our data center with no need to push upgrades and patches to end-user equipment, which lends for a less error prone, labor intensive process. The bottom line: we can respond more quickly and in an operationally non-disruptive manner to business requirements from DHH or LHC.
- Protection from viruses**.** Although we have enterprise wide anti-virus software for any of our PC based applications (predominantly Microsoft Office applications) by having our core transactional data and applications centrally housed, we eliminate the exposure to any Windows virus or malware impacting operational data, such as member, provider, claims, care management, and other business critical information.
- Efficient workstations. Employees are able to access their virtual desktop on any capable device, such as a traditional personal computer, or thin client hardware, which will be the case for LHC office

workstations. Thin client hardware far exceeds traditional workstation computers typically using 1/10th the power of traditional workstation computers, which will significantly reduce the environmental impact related to delivering advanced computing technology to LHC. The process for logging into a virtual desktop system is the same familiar process as logging into a local workstation. Once authenticated to the virtual desktop, LHC staff will be presented a full Windows desktop that appears to operate as a local desktop. Our high-speed WAN described above ensures the response and performance of applications present to our staff as if they were running locally.

- Superior User Experience. Users of our thin client systems enjoy a performance advantage that is a key benefit to the thin client architecture. Thin clients, with the virtualized desktops and applications that they present, process applications requests utilizing the CPU, memory, I/O, and disk resources of the enterprise class server machines that host the virtualization software. The performance capabilities of this server class hardware are significantly greater than the commodity hardware that is used to build traditional desktop and laptop machines.

Network Layer - An Open Standards, Secure and Highly Available Network Infrastructure. Today, local Centene health plan field offices connect to our core applications via Centene's Wide Area Network (WAN), a secure, high-performance, fault-tolerant network architecture designed for continuous availability, stability, interoperability, and growth through a mesh design that provides multiple paths to and from each point. If one path is down, or not performing optimally, the request is rerouted through another branch. Please refer to *Figure R.3-C: Centene Wide Area Network.* Centene Corporation's Wide Area Network (WAN) defines the communications infrastructure required for demanding, performance-driven applications. Within this framework, Centene is able to provide a secure access medium for mission-critical applications including data, voice, and video.

Data and voice services are provided via a Dedicated OC-12 (622Mbps) SONET Ring Service (DSRS). Carrier diversity (which is sourcing data and voice communications services from different vendors) is established by using dual SONET ring service from two independent, inter-exchange carriers. Each SONET connection consists of a resilient ring topology that connects the corporate office to the service provider's telecommunications infrastructure. Additional physical link protection is provided by establishing geographic diversity through physical separation of fiber routes.

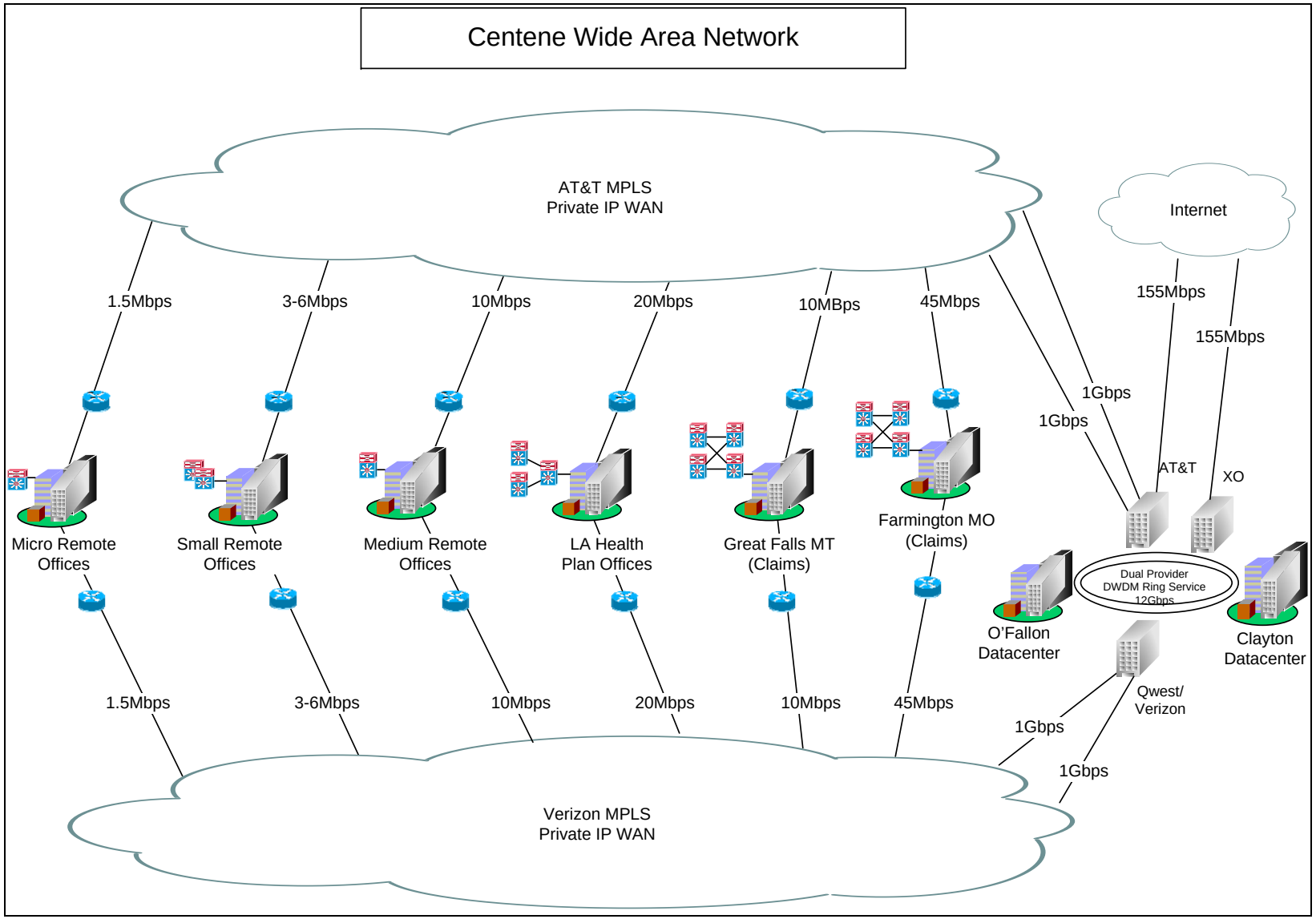
The primary WAN infrastructure consists of a high-speed, virtual full-mesh, Private IP Multiprotocol Layer Switching (MPLS) network. The MPLS core provides connectivity for all corporate, health plan, and specialty companies. The corporate campus is linked to this MPLS infrastructure via an OC-3 (155Mbps) circuit transported within the OC-12 SONET service. Our local field offices and other remote sites connect to the MPLS infrastructure using the primary MPLS router with aggregated T1s bonded via Multilink PPP (MLPPP). Remote office connections range in bandwidth from 1.5Mbps for small offices to 10Mbps for large regional offices such as LHC.

Redundant WAN connectivity is established through a **secondary** MPLS Service Provider providing carrier-diversity. The redundant circuits are equal in bandwidth capacity to the primary network. Local field offices and other remote sites connect to the **secondary** MPLS infrastructure using the secondary MPLS router with DS3 circuits or aggregated DS1s bonded via Multilink PPP (MLPPP). Remote office connections range in bandwidth from 1.5Mbps for small offices to 45Mbps for large regional offices. The Corporate **secondary** link is equivalent to the primary, an OC-3 (155Mbps) circuit transported within the OC-12 SONET ring. A 200Mbps connection is provided for the dedicated business-continuity and disaster recovery site.

Resiliency is built into Centene's network through redundancy. A primary and secondary WAN infrastructure exists to compensate for fluctuations in network capacity and/or stability. Independent locations ensure that high-utilization in one location will not impact system performance in another. In the event that an office loses its direct connection with corporate headquarters, alternate route paths are available for redirecting traffic through backup connections on the secondary network. In addition, all network equipment used for primary and secondary service delivery is designed for high-availability

using redundant component configurations. In the event of a complete systems failure or environmental catastrophe that would prevent normal operations, the Business Continuity Plan (BCP) will provide direction for sustaining operations during the disaster, to guard against catastrophic loss of information and to ensure a prompt return to normal operations. Please see our BCP description below as well as M.1 and M.2 for more information on our comprehensive Business Continuity Program.

Figure R.3-C: Centene Wide Area Network.



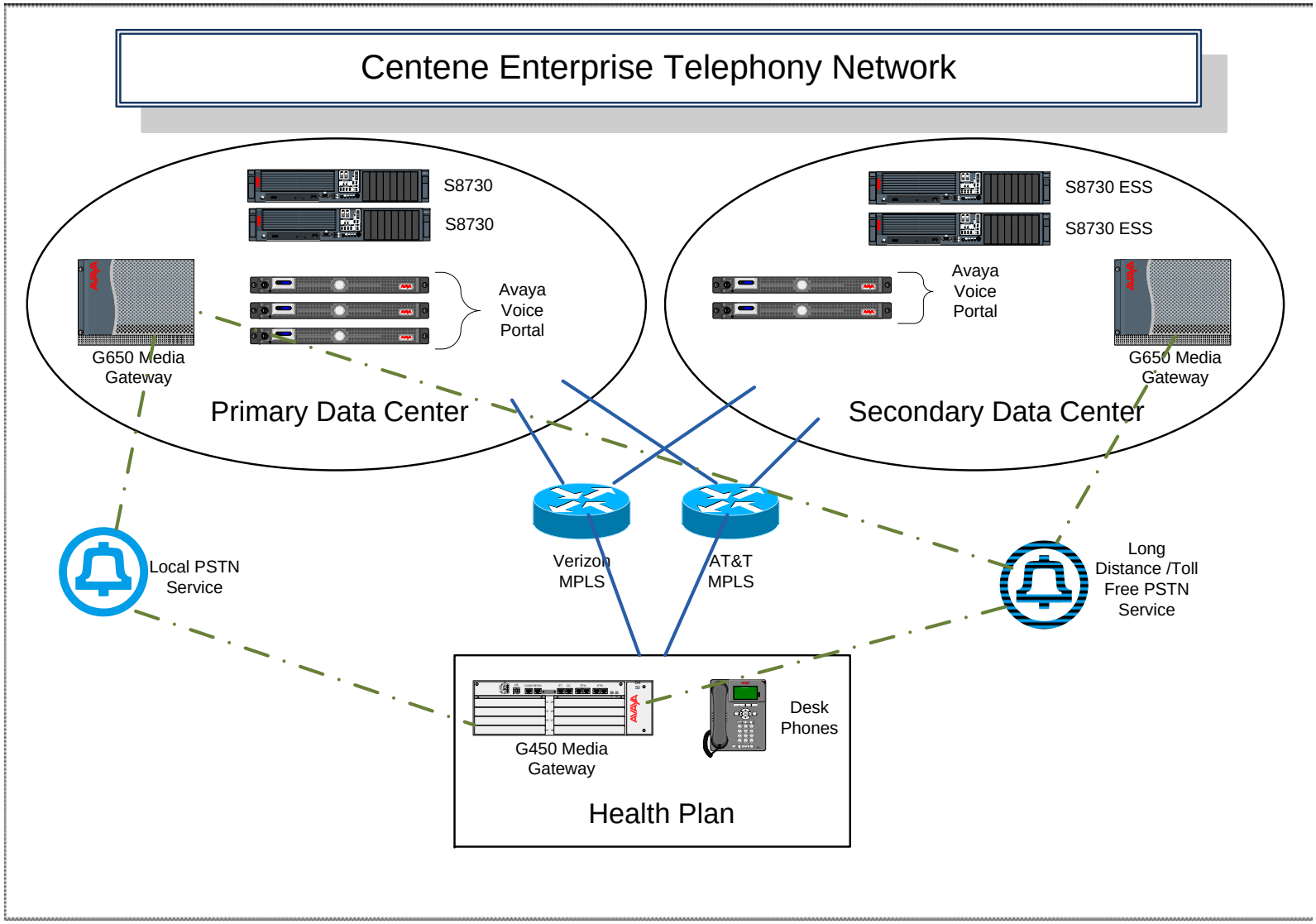
Local Area Network. We have a standard Local Area Network configuration using 100 Mbps T100 Network Interface Cards and Cat5 dual port wiring to each work area.

Secure, High Capacity Internet Connectivity. Today, Centene provides field offices and all field office users with Internet access through Centene's OC-3 circuit. The 155Mbps Internet service is transported and terminated on a Cisco access router, which is connected to redundant corporate firewalls (Cisco 6500s with Firewall Switch Modules). The Cisco 6500 Internet Access switches are connected to the internal network using Gigabit Ethernet over fiber. Centene's Internet infrastructure defines trusted and un-trusted segments. Intrusion Detection Systems (IDS) are located in strategic locations within the trusted and un-trusted segments to assist in the detection of security violation attempts, including unauthorized access attempts, denial-of-service attacks, or other malicious attempts to disrupt normal business activities. In addition to the trusted and un-trusted zones, established De-Militarized Zones (DMZs) provide semi-trusted segments for Web Servers, Domain Name System (DNS) Servers, and Secure Access Gateways. We provide remote access to Centene Corporation's network through a Virtual Private Network (VPN) using Cisco's VPN 3000 Concentrator and also through encrypted web access sessions using Citrix Secure Gateways.

Telecommunications Layer - Architecture Designed for 24 by 7 by 365 Operation. Centene's telecommunications hardware is the Avaya IP Telephony platform with Dual S8730 Media Servers in an enterprise data center. These servers are capable of failing over to a redundant pair of Avaya S8730 Enterprise Survivable Servers (ESS). ESS servers are active, redundant systems, installed at our Secondary Datacenter for back up and disaster recovery. One or more Avaya G450 Media Gateways provide local connectivity at remote offices for analog, digital, and IP endpoints. The G450 Media Gateway also provides ISDN-PRI trunk modules for local access to the Public Switched Telephone Network (PSTN) and has a Local Survivable Processor (LSP), which can process calls in the event that connectivity is lost to the Enterprise network. Avaya Communication Manager (CM) delivers world-class call routing and feature rich applications. Automatic call distribution (ACD) and advanced vectoring technology will support LHC. Avaya CM provides the ability to support remote IP agents, allowing maximum flexibility for distributing call agent workload as well as supporting disaster contingencies. Our managed private IP Multiprotocol Layer Switching (MPLS) backbone is deployed in a fully meshed topology with vendor diversity, connecting our field offices and specialty company telephone systems using Voice Over IP (VOIP) technology, and providing multiple routing paths for high volume and emergency conditions. The voice network consists of dedicated local Primary Rate Interfaces (PRIs) and analog lines provided by the Local Exchange Carriers (LECs) and long distance PRIs that carry outbound toll and incoming toll free calls provided by Verizon Business. Call center prompts on the toll-free numbers for member, provider, and medical management services will be designed using the Avaya Voice Portal IVR platform. See *Figure R.3-D: Enterprise Telephony Network.*

Continuity of Call Center Services to Providers, Members and DHH. In the event of a natural disaster or pandemic, all business functions that rely on our telecommunications system have *top priority*, specifically our member and provider call centers. We have engineered several levels of *redundancy* in our phone system hardware, software, and networking, with automated rerouting of inbound calls to other Centene call centers in the event of a communications failure for any one of our call centers. If an emergency event were to disable any of our offices, including LHC offices, our Business Continuity Plans (BCP) call for phone lines to be transferred to NurseWise, our after hours call center, to ensure continuity of service. NurseWise staffing needs at the call center are reviewed at the time of the emergency and, if needed, additional staff are called in to address any increase in call volumes. In 2010 and through Q2 of 2011, we addressed all incidents that threatened our telephone-based functions without any material impact on operations. This includes severe winter weather that took down telephone lines and transformers in the Southeastern and Eastern regions; rolling power outages that impacted our Texas locations: potential tornados and flooding affecting our offices in Mississippi; and several other less dramatic events.

Figure R.3-D: Enterprise Telephony Network.



System Monitoring - Tools and Resources; Continuous Testing of All Applicable System Functions. Centene maintains a centralized approach to managing system capacity, availability, and performance.

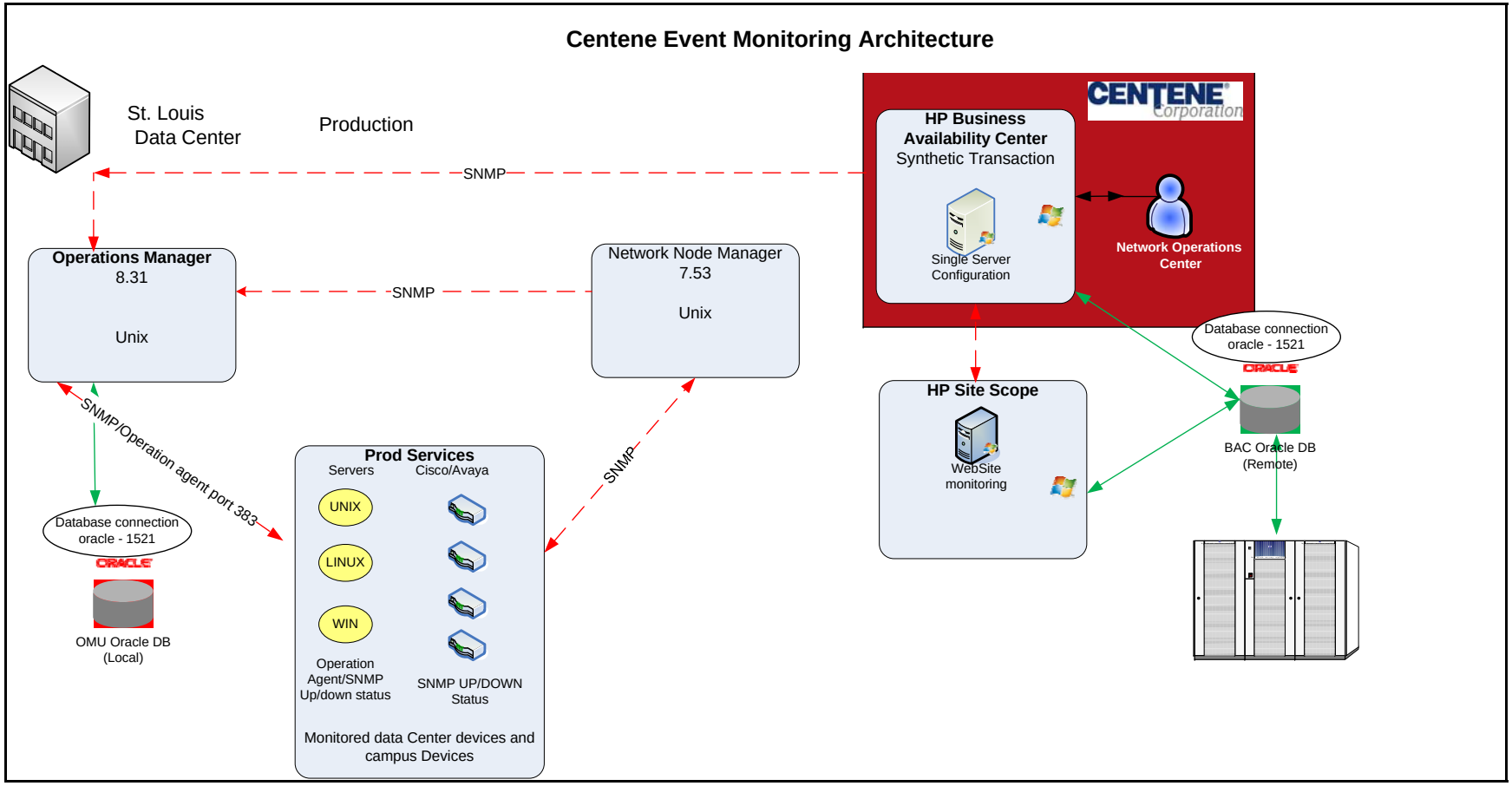
Our Network Operations Center (NOC) located in St. Louis, Missouri, monitors all production systems and remote offices 24/7/365 for service availability, system performance, and capacity utilization. Centene's NOC staff are dedicated to monitoring business critical applications, employing an Information Technology Infrastructure Library (ITIL)-based Incident Management Process enabled by industry-leading incident management and system monitoring tools, such as Hewlett-Packards OpenView Operations®, Solarwinds, Cascade, and Fluke's Visual Performance Monitor. Reference Figure R.3-E Centene Event Monitoring Architecture below.

Connectivity between the management systems and monitored nodes provides fault-tolerance. The HP Business Availability Center (BAC) and CA Wily Introscope provide applications and service level monitoring. Strategically placed HP BAC probes emulate client access to business-critical applications; ; provide metrics that assist in the prediction, isolation, and diagnosis of application events; and provide data that aid in capacity planning, performance measurement, and service level reporting activities. Introscope runs on our web application servers and enables visibility into complex transactions for our end-to-end application performance monitoring. For example, we use it today to monitor adherence to our performance service level agreements with our state partners, such as LHC.

Fluke Visual Probes, located at each remote office, monitor network performance and utilization of the connections to our corporate datacenters. If we experience a system or network service failure, *a notice is automatically sent to our central monitoring station and is reviewed by our Network Operations Center (NOC)*.

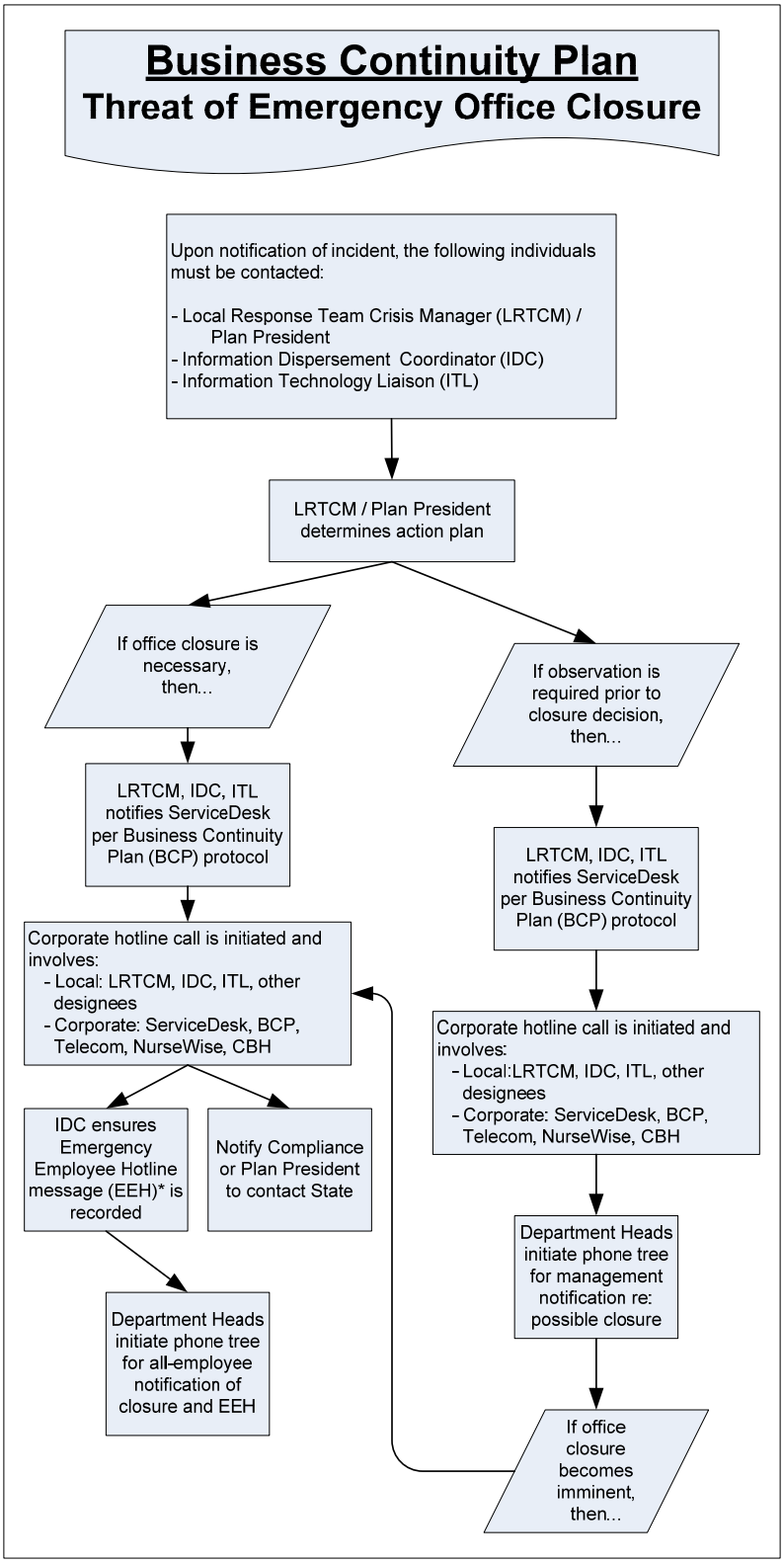
Based on the issue, when appropriate, the NOC will alert the Centene Service Desk who is responsible for initiating a virtual Emergency Management Team call line. All on-call staff and our Business Continuity Team participate in these calls, along with the Local Response Team lead. Our CMT has well defined protocol for managing the CMT call line, allowing them to quickly assess the issue, engage the appropriate staff, ensure notification to the state on a timely basis, and provide communication to all appropriate parties. Status updates for all Emergency Management Team calls are provided to senior management on a periodic basis until the issue is resolved. Our Information Technology staff can access all of Centene's systems remotely using Citrix. Staff can quickly and securely resolve issues any time and from any place with access to an Internet connection, cellular network, or telephone line.

Figure R.3-E Centene Event Monitoring Architecture.



Supporting LHC's Internal Front Line Users. Our Service Desk also allows us to continuously monitor the availability and responsiveness of our MIS. Centene will support local LHC staff in Louisiana and authorized users of LHC systems, including DHH's enrollment broker and fiscal intermediary, with a fully staffed technical Service Desk located at Centene's headquarters in St. Louis, Missouri. The Service Desk will be available to LHC front line users 24/7 through a dedicated toll-free number, or internally through a 5-digit extension. The Service Desk is staffed by a minimum of 2 agents from 6:00 AM to 7:00 PM CST, Monday through Friday, with on-call staff available after hours and on weekends. Should DHH require support on holidays and weekends, the Service Desk will be manned upon request. As front line support, the Service Desk is also at the center of emergency management and coordinates with our Network Operations Center (NOC) as described above, and key emergency management staff whenever there are issues affecting business operations. A core team of systems support analysts, engineers and management are on standby 24/7 to respond to any emergency call initiated by the Service Desk. The Service Desk is also the focal point for all emergency alerts, across all of our health plans. For example, during inclement weather that forces office closure, we instruct our plans to notify the Service Desk, who initiates a virtual Emergency Management Team call line to ensure the efficient and safe closure of the office, including the transfer of phone lines to NurseWise and the safe power down of all computer equipment, and ensure notification to the state within the required timeframe. For DHH, we will include that notification must occur within 60 minutes of an event, within or outside LHC's span of control. *Reference Figure R.3-F Office Closure Procedures below*. This flowchart and procedures list are specifically designed for each Local Response Team Management Business Continuity Plan.

Figure R.3-F- Office Closure Procedures



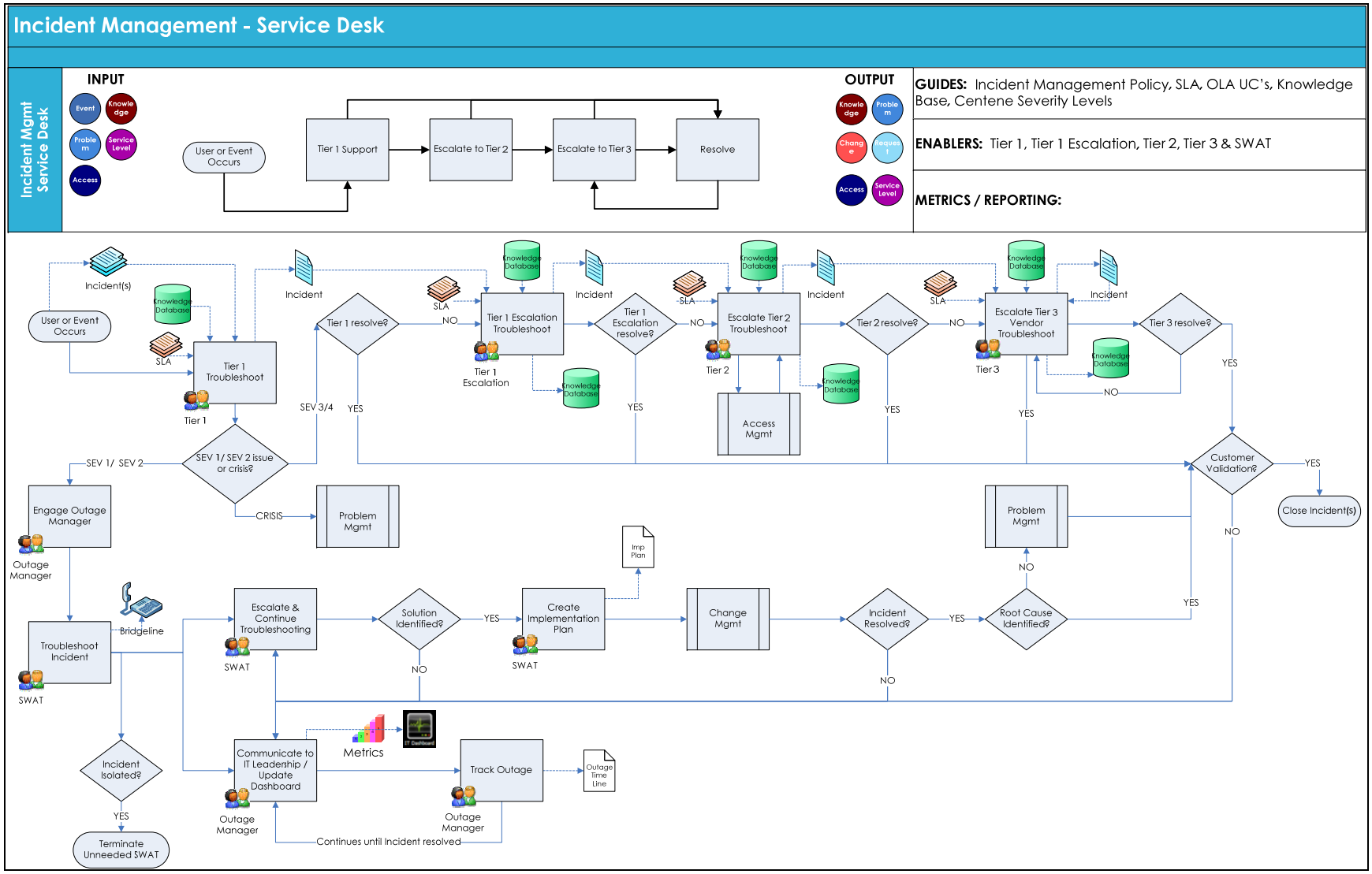
Incident Management. Our Service Desk uses ServiceNow (on-demand IT Service Management tool) as an integrated incident support management solution to submit, monitor and manage calls and change requests from front line users through to completion. Service Desk staff document all calls and requests into ServiceNow where a unique ticket number is assigned. ServiceNow then issues a notification email to the Centene or LHC user who contacted the Service Desk. This email contains the ticket number and a summary of the user's issue or request. Once the user receives an email with a ServiceNow ticket number, they can log into ServiceNow through CNET (our intranet) to view their tickets and the status of each.

ServiceNow is also used by our NOC. When our NOC detects an issue, the NOC staff log an alert to a central console. Depending on the severity of the issue, ServiceNow may issue a ticket and notify our on-call technical staff. ServiceNow categorizes incidents and problems by type of service and location to allow us to streamline tracking and reporting, so that we can spot any trends in the issues our front line users are experiencing, and develop action plans to eliminate any systemic issues. LHC's IT Liaison will be able to enter and view tickets online via ServiceNow to track their status and ensure successful resolution. ServiceNow is Information Technology Infrastructure Library (ITIL) driven and provides *automatic escalation* of trouble tickets to the appropriate Centene or LHC staff, based on customizable metrics, such as length of time a ticket is open; knowledge base resolution and activity reporting; keyword and full text searching against the knowledgebase; integrated problem management to assess whether a ticket is a one-time trouble-ticket or an indicator of systemic, longer-term performance and system problems; change and risk management planning with an automated approval process; asset management tracking from purchase, implementation, decommission through disposal; software license compliance tracking; and Service-Level Agreement (SLA) administration. ServiceNow automatically helps our Service Desk route front line user requests or issues to the appropriate Centene or LHC department for timely resolution.

Service Desk Response Standards. Our Service Desk staff classify incidents reported to the Service Desk by severity (SEV) level. If an incident is extremely serious, such as a significant network problem or a loss of service for one of our production applications, we consider this a SEV 1 incident and the Service Desk responds immediately. If the incident involves a loss of service for portions of an application, or where a specific group of users are impacted, we categorize this as a SEV 2 incident but our Service Desk *still* responds *immediately*. SEV 1 and SEV 2 incidents must be escalated from the Service Desk or the NOC to an Incident Manager, who initiates a call center conference call, bringing together our Emergency Management Team members to communicate the issues related to the SEV1/SEV 2 incident. When a SEV 1/SEV 2 incident occurs, the On Call Support Resources convene to begin troubleshooting the issue until it is resolved. System vendors are called in to assist when necessary. Once we resolve the SEV1/SEV2 incident, we document the root cause and solution into the ServiceNow system to develop an action plan to eliminate such issues in the future and/or use as a reference in future incident troubleshooting and analysis. While our Service Desk responds immediately to SEV 1 and 2 incidents, SEV 3 and 4 incidents are addressed as quickly and efficiently as possible, but no later than 2 and 7 business days, respectively, after the SEV 3 or SEV 4 issue is logged into ServiceNow. An example of a SEV 3 incident would be interruption of service to a single user; while adding a non-standard software package (like Microsoft Visio) is an example of a SEV 4 incident. (*Reference Figure R.3.G: Incident Management – Service Desk)*

Tiered Support Ensures Immediate and Appropriate Response. Centene assigns support roles into "tiers" to manage front line user incident resolution, and we mobilize resources from these tiers into the issue resolution process based on the issue severity. A Tier 1 role (Service Desk or NOC staff) initially identifies an incident and performs initial triage functions. The Incident Manager is accountable for following a SEV 1 incident through to resolution. The SWAT role is an on-call support resource team on heightened alert who may be convened when SEV 1/SEV 2 incidents arise. Senior management and/or system or network vendors, to whom SWAT teams can escalate issues, fill Tier 3 roles.

Figure R.3.G: Incident Management – Service Desk



Business Continuity / Disaster Recovery

Louisiana Healthcare Connections (LHC) along with our parent company, Centene Corporation (Centene), view Emergency Response and Business Continuity Planning (BCP) as more than a prudent business practice – it is an integral component of being a responsible employer, a responsive business partner and a service oriented organization. By ensuring solid business continuity plans are created and maintained for each of our health plans, combined with a series of tactical mitigation strategies that we have put in place to ensure resiliency in our organization, and finally socializing and exercising our plans with our employees and business partners on a routine basis, we are confident in our demonstrated ability to better withstand emergency events and even reduce potential negative impacts associated with those events. In addition to this, because LHC is a partnership between Centene and the Louisiana Partnership for Choice and Access (LPC&A), we will collaborate with and learn from the valuable experience of our partner in the unique Emergency Response requirements and activities required by DHH and the state of Louisiana.

Comprehensive Approach to Emergency Management, Disaster Recovery and Business Continuity. Centene has a dedicated Business Continuity Department reporting through Information Technology's Information Security Group up to the Chief Information Officer. Business Continuity Plans covering Emergency (Crisis) Management, Business Continuity, and Disaster Recovery exist for all Centene locations, including our Health Plans, such as LHC, and our subsidiary companies. These are created and maintained by the business leaders themselves, under the guidance of our experienced Business Continuity Planning (BCP) team. For more information on our Business Continuity Planning approach and methodology, and how we prepare our business operations for an emergency, please see our response to questions M1 and M2.

LHC along with Centene will be responsible for the LHC emergency response continuity of operations and disaster recovery plans, which we collectively refer to as our Business Continuity Plan (BCP). We will tailor our BCP for the specific requirements of LHC, DHH and Louisiana to specify the actions LHC and Centene will take to ensure the ongoing provision of health services to our Louisiana members, on-going coordination of service with our providers, and continuing responsibility to DHH in the event of an epidemic (pandemic), disaster or manmade emergency, including (but not limited to) localized acts of nature (hurricane, flood, etc.), accidents, and technological and/or attack-related emergencies.

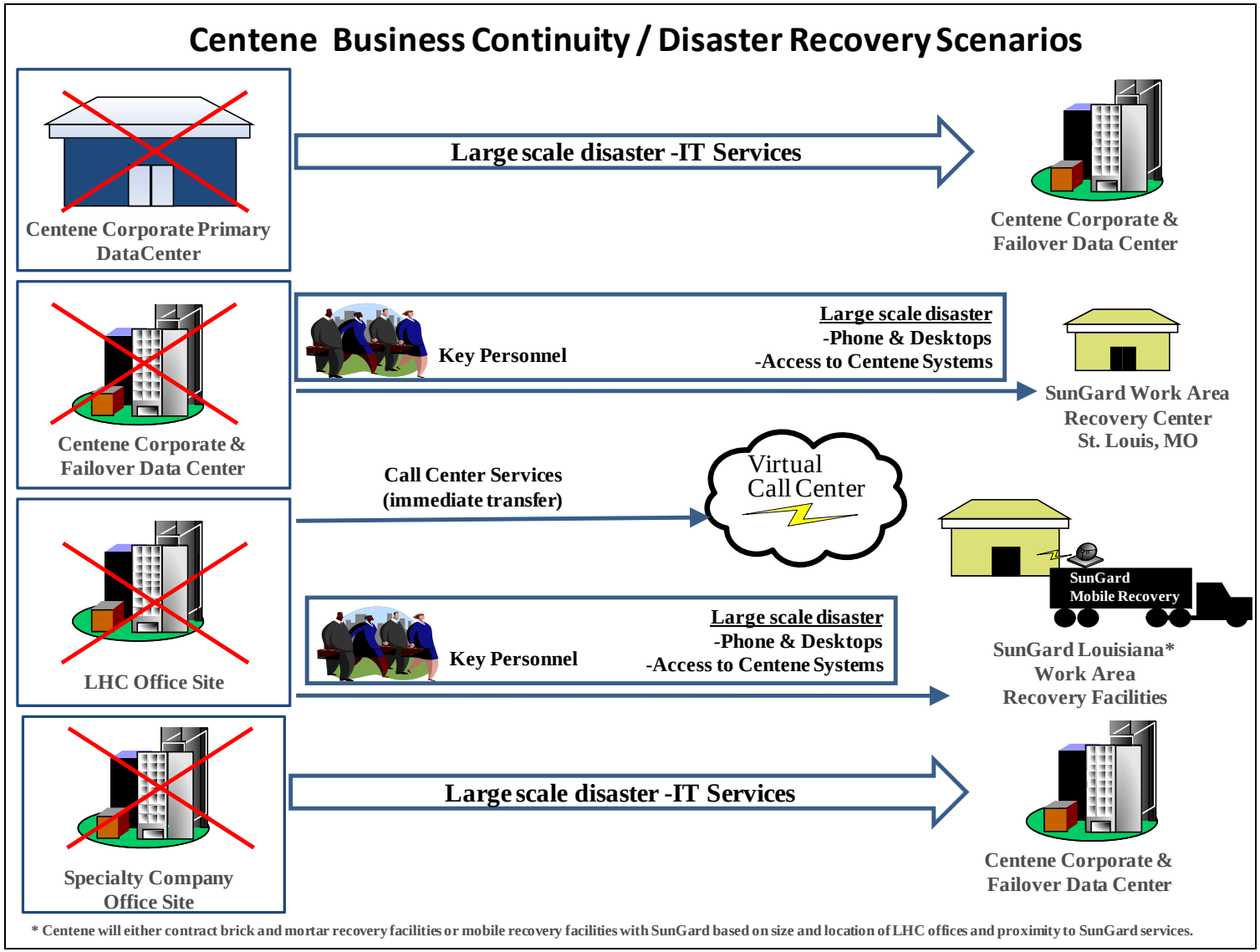
To support continuous access to data systems, the Business Continuity/Disaster Recovery (BC/DR) component of our BCP is supported by local work area recovery facilities for key personnel and if an event were to impact our Centene Corporate Data Center, we have in place a secondary data center in Philadelphia, PA, contracted through SunGard Recovery Services. We are also very pleased that we are on schedule to complete our new primary datacenter in 4th quarter 2011, which will allow us to make our current (and recently updated) datacenter our failover datacenter beginning in 2012. For a visual depiction of our recovery scenarios, please reference *Figure R.3.H: Centene Business Continuity / Disaster Recovery Scenarios* below.

We test our BC/DR plan annually, and results are communicated to all our health plan compliance officers and our state partners. A summary of our exercise and results is included below.

The BC/DR processes are designed to handle a worst-case disaster, such as total work site destruction, or loss of access to offices requiring recovery at alternate locations. In such situations, the Corporate Emergency Management Team, in coordination with the LHC Local Response Team, acts as a centralized command team to:

- Coordinate and allocate available resources.
- Resolve any resource allocation conflicts threatening the recovery team.
- Coordinate the recovery of all essential operations, providing direction and guidance where required.

Figure R.3.H: Centene Business Continuity / Disaster Recovery Scenarios



Business Continuity Plans. We maintain extensive documentation of targeted information on our BCP to ensure sufficient detail relative to the business area recovery and overall coordination of recovery efforts. The table below shows the categories of our BCP documents with a brief description of each:

Centene-LHC Business Continuity and Disaster Recovery Plan	
Documentation Categories	**Description**
Centene Corporate Crisis Management Plan / Emergency Response Procedures	Who, what, when, where and how with respect to an organized and consolidated approach for response and recovery activities at our corporate location following any unplanned incident or systems interruption to data or telecommunications.
Local Health Plan Management Team / Emergency Response Procedures	Details on considerations, assignments and tasks necessary for Local Health Plan Management Teams to respond, declare, manage and recover from an incident following any unplanned incident or systems interruption at their location. The plans detail the relationship, roles and responsibilities for the local plan (e.g. LHC) working with the Corporate Incident Management Team.
Business Unit Continuity Plans by Local Health Plan	Business Unit recovery plans detail the specific steps to be taken by the Business Unit teams after an incident has been declared. Plans detail the processes, tasks, contacts, vital records, and work space requirements needed by the local health plan team including relocation of physical site as may be required.
Centene Corporation Pandemic Operations Plan	Procedures to recover the business following a disruption due to a pandemic.
Employee Awareness Training	Presentation to new hires and available on the Intranet to educate employees about BCP at Centene Corporation, Local Health Plans and Subsidiaries.
Disaster Recovery Plan	Procedures and prioritization to recover Information Technology services, including relocation or repair of physical site and equipment.
System Recovery Plans	Outline the detailed steps needed to recover the IT and Telecommunications infrastructure, data, systems and tools needed by the business.

Each BCP provides extensive and detailed information on the specific activities to undertake to restore business operations in a safe, quick and effective manner. For example, the BCP includes call lists, alternate location instructions, key vendor listings and necessary special supplies to provide local resources with all relevant information they need in an emergency. In addition, the BCP explicitly details step-by-step processes in a prioritized manner to ensure those services most directly impacting members are restored first. The prioritized restoration of services allows our health plans to not only continue meeting member needs throughout an emergency, but also provides the necessary structure to restore business processes in the most feasible, reliable and consistent manner. Each department will also receive a detailed plan specifically for their team which outlines the recovery steps for their specific business processes. Our BCP software, LDRPS, also through SunGard, allows our teams to attach specific

documentation, policies and procedures, contact information, etc and is available through SunGard's externally hosted website, so they are always available to LHC and Centene in the event LHC systems were not available. Please see our response to M.1 for a list of department BCPs.

In the event of an emergency, all impacted team members are notified immediately using SunGard's Emergency Notification Service, NotiFind™. NotiFind is an externally hosted program that can be used to contact employees by phone and email during emergency and non-emergency events. Within NotiFind, we have pre-established call groups identified, for quick and easy notification. NotiFind is similar to the notification systems used by public schools and colleges to inform students and parents of an emergency event, such as approaching severe weather conditions. This software is utilized by LHC, Centene's Service Desk, Business Continuity team, Corporate Communications, and other selected health plans/specialty companies when important, time sensitive information needs to be communicated to employees. We use NotiFind throughout any event management activity, including our BCP/DR exercises, to communicate instructions to employees.

All BCPs are regularly updated to reflect the most current operational status and are published via multiple methods to ensure availability at the time of plan activation.

Datacenter Facilities - Designed for Dependable, Reliable Operations. LHC's Datacenter is managed by our parent company Centene in St. Louis, Missouri and is home to all of the core application services that are furnished to LHC. Our Datacenter is equipped with two diverse power feeds into the facility with redundant Uninterruptible Power Supplies (UPS) providing battery back-up power to all IT equipment. There are two separate power systems in the facility which provide redundant power to each rack of equipment on the Datacenter Floor. This capability allows for equipment within the electrical plant to be taken offline and maintained without power interruption to the computing equipment and provides continuous power in the event of the loss of power to either power feed entering the facility. In addition, the facility is also equipped with a diesel generator capable of supporting all IT services in the event of a loss of both power feeds entering the facility or a prolonged power outage. We execute a full load test quarterly, switching all power loads to the generator, to validate the generator's effectiveness. Less than 15 seconds is required to automatically switch to backup generator power. Battery backup systems provide power during the transition to generator power resulting in zero downtime for the IT infrastructure.

Environmental Safeguards. Temperature and humidity levels in the datacenter are controlled with a redundant chiller plant. The chiller plant utilizes a highly efficient water cooled system and is backed up by an air-cooled system to provide cooling in the event of loss of water to the facility. It is an N+1 design ensuring that the loss of any one unit does not affect our ability to maintain safe temperatures. All environmental systems are tied into Centene's security system and send an audible remote alarm when temperature or humidity falls outside of predefined ranges or water is detected. Environmental monitoring sensors are located within the server racks and wireless temperature sensors placed throughout our Datacenter that send out automated alerts when temperatures and/or humidity levels exceed defined thresholds. These alerts are sent to Centene's NOC and key IT technical and management staff enabling rapid response.

Fire Protection. Centene Datacenter facilities are protected by an advanced fire suppression system, which includes a VESDA (Very Early Smoke Detection Alarm) system. This system takes air samples throughout the Datacenter sensing particulates that are present in the air prior to actual combustion. The alarm system is integrated with the building alarm system which is connected to the local fire authorities. The fire suppression system is a Ecaro-25 Clean Agent Fire Suppression System. A pre-action water sprinkler system provides a second level of protection. Safeguards are in place to minimize the risk of accidental discharge of both the clean-agent and sprinkler suppression systems.

LHC Field Office. LHC's office in Baton Rouge will be equipped with full UPS, and backup power generator for prolonged power outages. Note that in any situation where local power in Baton Rouge were to be disabled for more than four days, the local Business Continuity Plan would be activated as described

below and LHC staff would be operating from a backup work area recovery mobile trailer site (please also see our responses to Section M, Questions M1 and M2).

Centene's New Datacenter. In the 4th Quarter of 2011, Centene will complete construction of our new, fully-functional, Tier 3 (concurrently maintainable equipment), 19,000 square foot datacenter, with capacity for over 167 IT racks; 6,000 square feet of datacenter floor; and fully redundant environmental, power, and network connectivity systems. It was designed to be fully HIPAA compliant and provides state of the art security measures. In the 1st Quarter of 2012, we will operate our two fully-redundant enterprise datacenters as mutual "*hot site*" backups. Each datacenter will have the capacity to assume operation of all **business critical** production systems if the other datacenter is rendered inoperable. *Reference Figure R.3-I Centene Datacenter Reference Architecture below.* Features include:

Scalability and Growth. The Datacenter was designed for a 20 year growth plan. All systems to support Centene operations today (datacenter floor, electrical, mechanical, fire systems) consume only 1/3 of the planned capacity for the facility. The datacenter floor was designed by creating 'Compute Pods'. Each pod is designed with 2 rows of 8 racks designed to be a self contained, mini datacenters on their own. We have the ability to outfit 4 full pods and 2 half pods at full capacity. Because each pod is designed to be fully autonomous, we can choose to take full advantage of new technologies as we deploy and outfit future pods. We currently have 1 of our 4 full pods outfitted and in use. Additional features include:

- 76 racks currently installed, with the ability to grow to 167 racks at maximum capacity.
- Two (2) additional water cooled chillers and one (1) additional air cooled chiller.
- Generator plant has been designed to grow by two (2) additional 1500kw generators
- Electrical system designed to grow to a full capacity of 6 UPS modules

Datacenter Hardening. The entire facility was designed to withstand penetration due to natural or other security threats.

- Designed for a 1.5 Seismic Importance Factor based on the IBC (International Building Code) Section 1604.5 standards. This design classification indicates a fully functional facility following an earthquake.
- Designed to withstand 165 MPH (F3 tornado) conditions
- Surrounded by an 8 foot security fence with security monitoring at the single entrance
- Equipped with security cameras which are broadcasted back to our Corporate security system

Fire Protection System. The facility has advanced fire detection and alert systems including:

- The Data Center, MDF, Lab, UPS rooms, and Demarc rooms are protected by a VESDA (very early smoke detection apparatus). This system has the ability to detect a very small amount of smoke and will send alert notification before a large fire event develops
- The Data Center, MDF, Lab, UPS rooms, and Demarc rooms are protected by an ECARO-25 Clean agent system. The Clean Agent system is designed to dump in the event of fire detection. This removes the necessary oxygen from the affected area in order to extinguish a fire. There is a total of 368 lbs of clean agent on site
- In the event the Clean Agent system is unsuccessful at extinguishing the fire we have a Fire Protection sprinkler system consisting of two (2) Pre-action systems and one (1) wet system that will deliver water to the fire automatically

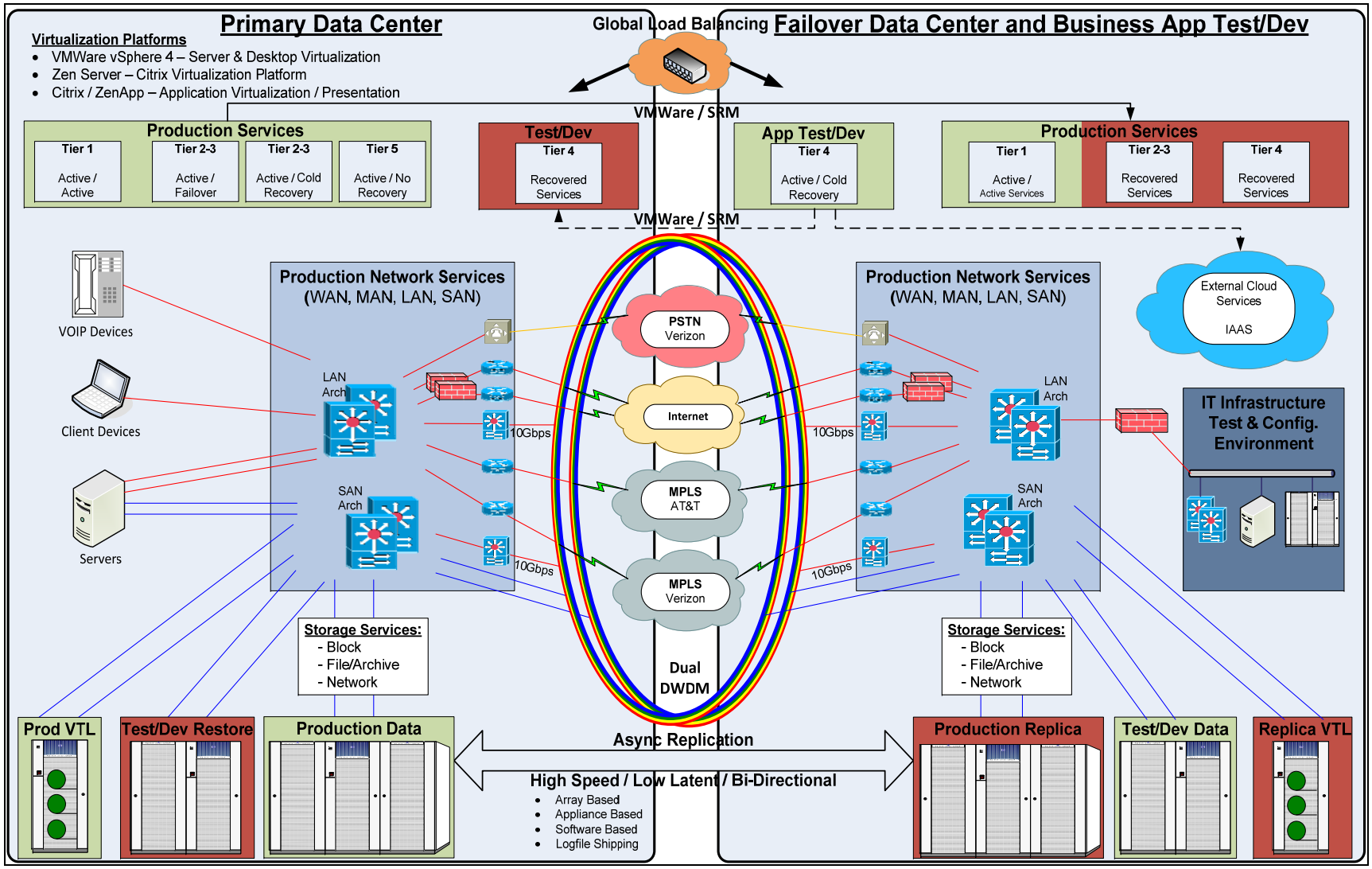
Network Access. *The facility was designed with fully redundant networking infrastructure and network circuits* between our two datacenter facilities to ensure that an outage by one of our telecommunications providers (AT&T & Qwest communications) will not result in our systems being rendered unavailable.

- Each network circuit reaches the facility from distinct path and terminates in a private network DMARC area. Each of the vendors are only allowed in their DMARC to provide full separation and security

Electrical Plant. The power infrastructure of Centene's datacenter was engineered and constructed to provide the highest levels of reliability, performance, and fault tolerance. It is monitored both on-site and at our corporate network operations center to ensure optimal performance is maintained. Redundant utility power feeds, UPS battery backup systems, and power feeds to the individual equipment racks, together with a diesel generator sized to handle the full power load of the datacenter and automated systems to manage the transfer of load between power systems, ensure that power events that would normally be disruptive, ranging in severity from a minor short in a power cord to a major extended outage of regional utility power, will be transparent to our systems, our users, and the members and providers that we serve.

Mechanical Plant. Datacenters generate a great deal of heat. As a result, the systems used to cool a datacenter are every bit as critical to operations as are the power systems. With that in mind, the Centene datacenter incorporates a high performing and highly efficient cooling system built to support our exacting standards for both reliability and fault tolerance. The redundancy that we have engineered and built into each component including chillers, pumps, condensers, air handlers, and reserve water tanks, together with our use of both water cooled and air cooled technologies, ensures that our systems will remain at optimal operating temperatures even if components of the cooling system fail or need to be taken off-line for service. What's more, Centene's use of "green technologies", such as a plate/frame heat exchanger and cooling tower system, enable us to use the ambient temperature of the outside air to cool the datacenter when the weather allows. Centene's environmentally conscious and well reasoned approach to datacenter cooling systems is one of the many factors that have contributed to our datacenter achieving the third-party Leadership in Energy & Environmental Design (LEED) certification.

Figure R.3-I- Centene Data Center Reference Architecture



Information Systems Disaster Recovery. If an emergency event disables our central datacenter, for any reason, we will invoke pre-established recovery procedures. Restoration of all critical business functions then begins at our alternate data facility. Currently, this is at the SunGard Mega Center facility in Philadelphia, Pennsylvania. As mentioned above, upon completion of our new Centene datacenter, we will move our disaster recovery to Centene's failover datacenter. Once the new datacenter is complete, our current datacenter will become our failover center in the event of a disaster. A temporary Command Center will be established and the Crisis Manager will utilize the published 800 disaster hotline. In this situation, LHC offices would be notified immediately of the situation (via NotiFind, our employee notification system, if necessary). Our telecommunications architecture is engineered so that mission critical phone communications remain available at all local sites. *Centene targets to restore all centralized MIS operations within **12 hours** of the declared disaster* as defined below. This is well before DHH's requirement of 72 hours.

Service Level Standards Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

All of our MIS services have been classified by the business into Tiers to streamline and categorize recovery efforts. We have further classified unplanned outages into three types with corresponding levels of **Recovery Time Objectives (RTO)** required for Tier 1 and Tier 2 services. Due to our current back-up strategy, described above, our **Recovery Point Objectives (RPO)** for all core systems is 2 hours. With our new datacenter, we intend to bring this gap to less than 30 minutes. Recovery Time Objectives for our business and IT Services are structured utilizing a Tiered approach based on the severity of the outage. For key MIS services for LHC and DHH these are defined as follows:

- Tier 1 Services include Telecommunications and Wide Area Network (WAN).
- Tier 2 Services include Amisys Advance, our eligibility and claims processing system; our TruCare health services management system; our MRM and PRM systems; our Member and Provider Portals; our Enterprise Data Warehouse; our Electronic Data Interchange Services; and all supporting infrastructure to recover these systems.

Standard Unplanned Outage - A single service outage. These may be due to equipment or software failure and will be recovered within the same datacenter (usually a reboot or restart of a service) and typically do not require restoration of data. Business and IT Services Recovery Time Objectives (RTO) are as follows:

- Tier 1 - Active / Active configuration with continuous operations providing no loss of services during failure event.
- Tier 2 - Active / Passive configuration with an RTO of 0-4 hours.

Extended – An extended outage is defined as a single (possibly multiple) service failure(s) that require service restoration (either data or server recovery). Recovery could be in either the same datacenter or in our failover datacenter depending on the scope of the recovery.

- Tier 1 - Active / Active configuration with continuous operations providing no loss of services during failure event.
- Tier 2 - Active / Passive configuration with RTO within 12 hours.

Disaster – Massive service failures, usually due to a building failure (power, fire, earthquake) or a significant shared technology failure (e.g. loss of enterprise storage). A disaster requires recovery at our secondary facility.

- Tier 1 - Active / Active configuration with continuous operations providing no loss of services during failure event.
- Tier 2 - Active / Passive configuration with RTO within 12 hours.

If the disaster is limited to a local office (such as LHC), our Local Response Team will work with the Corporate Crisis Management Team to execute the recovery plan. In the event the local office is inaccessible or destroyed, recovery services will be initiated at a SunGard Metro Center or Mobile

Recovery facility. This will provide for desktop computers and telephones so staff can resume activities quickly. LHC will continue to operate out of temporary offices until permanent facilities are re-established. Per the BCP, within minutes, member and provider calls will be re-routed to pre-designated Centene operations in other areas, and systems and servers will be gracefully shut down through remote controls except for environmental monitoring systems. Displaced employees will be reassigned to designated areas and will be able to log on to our system and continue to support the needs of our members and providers remotely. When the event is over, employees and systems will be rerouted back to LHC for normal operation.

Communication with DHH. In an emergency, our top priority is to preserve the health and safety of our staff and care for our members before proceeding to the Notification and Activation procedures. For more information on our Emergency Response and Continuity of Operations see our response to question M.1. Once the safety and welfare of our employees is addressed, we will notify DHH of any event that will or may potentially impede our ability to service our members, providers and DHH. Our Service Now system described above will be configured to notify LHC Local Response Team Lead, Compliance and Senior Management in the event of any Sev 1 or Sev 2 issue impacting LHC key systems, and the Local Response Team Lead or his/her alternate will be included on Emergency Management Team calls.

Local LHC plan management will be responsible for notifying DHH and will do so within the timeframes required by DHH. We will also provide DHH will contact information for all our key personnel both at LHC local offices and Centene Corporate so that DHH is able to reach out to LHC in the event of a large scale emergency. If the event affects an LHC office, rending it inaccessible, the Local Response Team will direct the business units to activate their business continuity plans while keeping the Emergency Management Team (which includes our Corporate Crisis Management Team and all Corporate Support Teams) apprised of the situation. The Emergency Management Team will provide support to the Local Response Team and their business units as needed. The Emergency Management Team will be in close contact with the Business Continuity Management Team and Executive Management throughout the event's duration. All impacted team members will be notified immediately using SunGard's Emergency Notification Service, NotiFind™, upon declaration of an Information Technology emergency.

Annual Business Continuity Planning Review and Exercise. Our entire BC program undergoes a formal review on an annual basis and the LHC team in Louisiana will go through the planning and annual review process as do all our locations. All departments and Senior Management participate in these reviews which include a read through of our current plan, an update of all materials, and a read through of the final plan after all changes have been made. Following this, we conduct a scenario-based exercise to assure the plan addresses all factors related to both short- and long-term emergencies that could cause an interruption in the flow of our operations. Additional BCP changes are made based on the scenario exercise to ensure the plan reflects the ideal response to an event. These activities are overseen by our Corporate Business Continuity Department which is staffed by a team of credentialed Business Continuity Planners with multiple years of experience in planning, maintenance and methodology who oversee and manage the tools for documentation and our contracts for recovery.

Corporate Information Technology Disaster Recovery Exercising. In addition to the annual refresh and testing of Business Continuity Plans, Centene conducts annual full-scale testing of our recovery capabilities by simulating the complete destruction of Centene's primary data center. As part of this exercise, we perform an annual "Hot-Site" information technology test, also known as a disaster recovery (DR) exercise.

Historically, Centene has tested its ability to recover critical Management Information System (MIS) capabilities by conducting a full scale planned exercise using our third party vendor, SunGard. Having successfully completed these exercises for multiple years, we chose to evolve our approach in 2010, exercising our ability to respond to an unannounced "mock event."

Using an “earthquake mock event” as the trigger, Centene Corporation conducted its annual exercise beginning on Tuesday, November 02, 2010. With the exception of the CIO and a few Senior IT Directors, no one on the recovery team was aware of the event. Beginning at 4:00 AM CST, notifications were sent and IT Infrastructure Management joined a bridge call by 4:15 AM where they were instructed to identify and contact primary resources asking them to assemble at 7:30 AM to receive the scope of the exercise --- or impact of the earthquake. With only access to our emergency online documentation repository, but no access to anything within the primary data center, or other resources, a team of 23 MIS professionals were asked to restore critical IT functions.

The Emergency Command Center was invoked using our third party notification service, NotiFind, which provides the ability to send out messages to multiple people and contact devices simultaneously without requiring Centene’s corporate Data Center be operational (i.e., phone or e-mail systems). Crisp communication inside the command center with external users and management was controlled through the following methods:

- Deployment of a dedicated Crisis Manager.
- An open 24x7 pre-established IT conference bridge where technical resources could join together to resolve issues throughout the exercise.
- A periodic management conference bridge to facilitate communication between the DR recovery facility and remote recovery management personnel.
- An on-site IT Service Desk was established to document problem tickets and track them through completion as they do in our production environment.

In the last stages of the exercise we were able to *successfully* validate critical services and business processes were functionally restored. Significant examples include:

- Eligibility and Claims Processing
- Secure Provider Portal Services
- Medical Management Systems

We make the results of our Disaster Recovery exercise available to each of our health plan compliance officers and to our state partners on request.

Question R.4

Interoperability of Key Production Systems

R.4 Describe in detail:

- How your key production systems are designed to interoperate. In your response address all of the following:
  - How identical or closely related data elements in different systems are named, formatted and maintained:
    - Are the data elements named consistently;
    - Are the data elements formatted similarly (# of characters, type-text, numeric, etc.);
    - Are the data elements updated/refreshed with the same frequency or in similar cycles; and
    - Are the data elements updated/refreshed in the same manner (manual input, data exchange, automated function, etc.).
  - All exchanges of data between key production systems.
    - How each data exchange is triggered: a manually initiated process, an automated process, etc.
    - The frequency/periodicity of each data exchange: "real-time" (through a live point to-point interface or an interface "engine"), daily/nightly as triggered by a system processing job, biweekly, monthly, etc.
- As part of your response, provide diagrams that illustrate:
  - point-to-point interfaces,
  - information flows,
  - internal controls and
  - the networking arrangement (AKA "network diagram") associated with the information systems profiled.

These diagrams should provide insight into how your Systems will be organized and interact with DHH systems for the purposes of exchanging Information and automating and/or facilitating specific functions associated with the Louisiana Medicaid CCN Program.

Experience in Managed Medicaid and CHIP Information Technology.

Centene's Management Information System (MIS) will supply the applications support and underlying technology for LHC. Nationwide, Centene's scalable MIS supports the goals of responsive, accountable, and coordinated care for 1.6 million Americans in our public sector full risk managed care plans in 11 states.

A Systems Approach that Integrates Functional Richness for Seamless CCN Administration

During our 27 years of experience in public sector IT architecture planning, integration, operations and reporting support; we have adhered to a central maxim in our approach to key production system design: a disciplined focus on *integrating applications* that deliver **best of breed functionality**. Our business continues to become more complex as we expand into new process support well beyond claims payment - with increasing emphasis on event driven clinical coordination; provider and member relationship management, engagement and intervention; as well as advanced informatics applications, predictive modeling, etc. Consequently our vendor best of breed application strategy has become even more *relevant* and *necessary*. That's because we firmly believe there is **no single software vendor** who can possibly deliver all the application functionality our state clients, providers, and members need and demand. Thus, through our operating history, we have focused not on application development, nor "sole sourcing" software, but on:

- Our core expertise in *public sector healthcare processes* and data

- Our ability to identify the *best software*, hardware, and communications technologies to constantly enhance existing processes and enable new processes; and, most germane to this discussion
- Our core competency on the *integration, interoperability and data management* of our industry leading software componentry in a consolidated, enterprise scale MIS.

Interoperability Through a Service Oriented Approach, Combined with Master Data Management.

Please refer to ***Figure R.4-A: Key Production Systems Diagram*** (R.4-A) below for the following discussion. Broadly speaking, we have a two-pronged approach to software interoperability among our best of breed functional applications, similar in basic approach to CMS' Medicaid Information Technology Architecture (MITA) for MMIS design:

- A **Master Data Management** (MDM) approach to data storage, persistence, quality assurance and distribution - to ensure that our data is represented and stored accurately, completely and uniquely for the use of our applications (e.g. no data discrepancies or duplicates)
- A **Service Oriented Architecture** (SOA) that communicates data between consuming applications: driven by event or schedule and using the right industry standard interface; depending on the specific business purpose of the interface.

In R.4-A, five applications represent our MDM *systems of record* for key production data:

- Item **A** in R.4-A is AMISYS Advance, our claims processing system, and the master of our "in process" and processed (or "finalized") claims data.
- Our Provider Relationship Management (PRM), item **B**, is our integrated set of modules for provider service inquiry management (ProviderConnect), contracting (Emptoris), outbound campaign management (ProviderReach), and provider data management (Portico). It is the Portico component of PRM that houses and manages our master provider records.
- TruCare (**C**) is our member-centric health management platform for collaborative care coordination; and case, behavioral health, disease, and utilization management; and houses our master health assessment and service authorization data.
- Member Relationship Management (MRM), item **E**, is analogous in overall functional purpose to PRM in that it supports our member service inquiry functions (MemberConnect), member outbound campaign management (MemberReach), and member data management, through our integrated Member Demographic System (MDS). MDS is a Microsoft Dynamics based application implemented with SQL/Server, and houses "all things member related," including member identifiers, demographics, eligibility, contact information, preferences (e.g. notifications by phone and/or e-mail), and other member data.
- Our encounter processing workflow system, Xpress Encounter Pro from Medical Data Express (Encounter Pro - item **F**) holds our master encounter records.

Centelligence™: Driving Interoperability Through SOA and Industry Standards. From a systems perspective, it is our **Centelligence™ data integration engine** (symbolized by item **D** in R.4-A) that is at the *heart* of both our MDM and SOA architecture. R.4-A depicts Centelligence™ system components: Our **Centelligence™ Data Service Bus** (**1**) is an integrated set of open interoperability standards and services, including Java Messaging Services (implemented through TIBCO EMS); Request/Reply and Publish/Subscribe transaction messaging services (implemented through our Informatica Change Data Capture (CDC) middleware); Extract/Transform / Load (ETL) processes (also implemented with Informatica middleware); and open database connectivity interfaces including Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC).

The **Enterprise Data Warehouse** (EDW - item **2**), is a high performance data warehousing and integration engine, implemented using Teradata®'s Extreme Data Appliance, allowing EDW to handle

truly large amounts of data with markedly superior speed. For example, with our upgrade to Teradata in 2010, we have been able to process member care gaps and health risk alerts on a bi-weekly basis - a significantly faster cycle than industry practice, which is generally quarterly or monthly (at best). EDW also houses our Enterprise Data Dictionary (EDD), which systematically maps all data elements across our applications (further discussion below); and EDW also contains the EDW Managed Data centralized repository of code lists - ensuring and enforcing the consistent use of code lists (e.g. diagnosis codes) across our MIS platform (more information below).

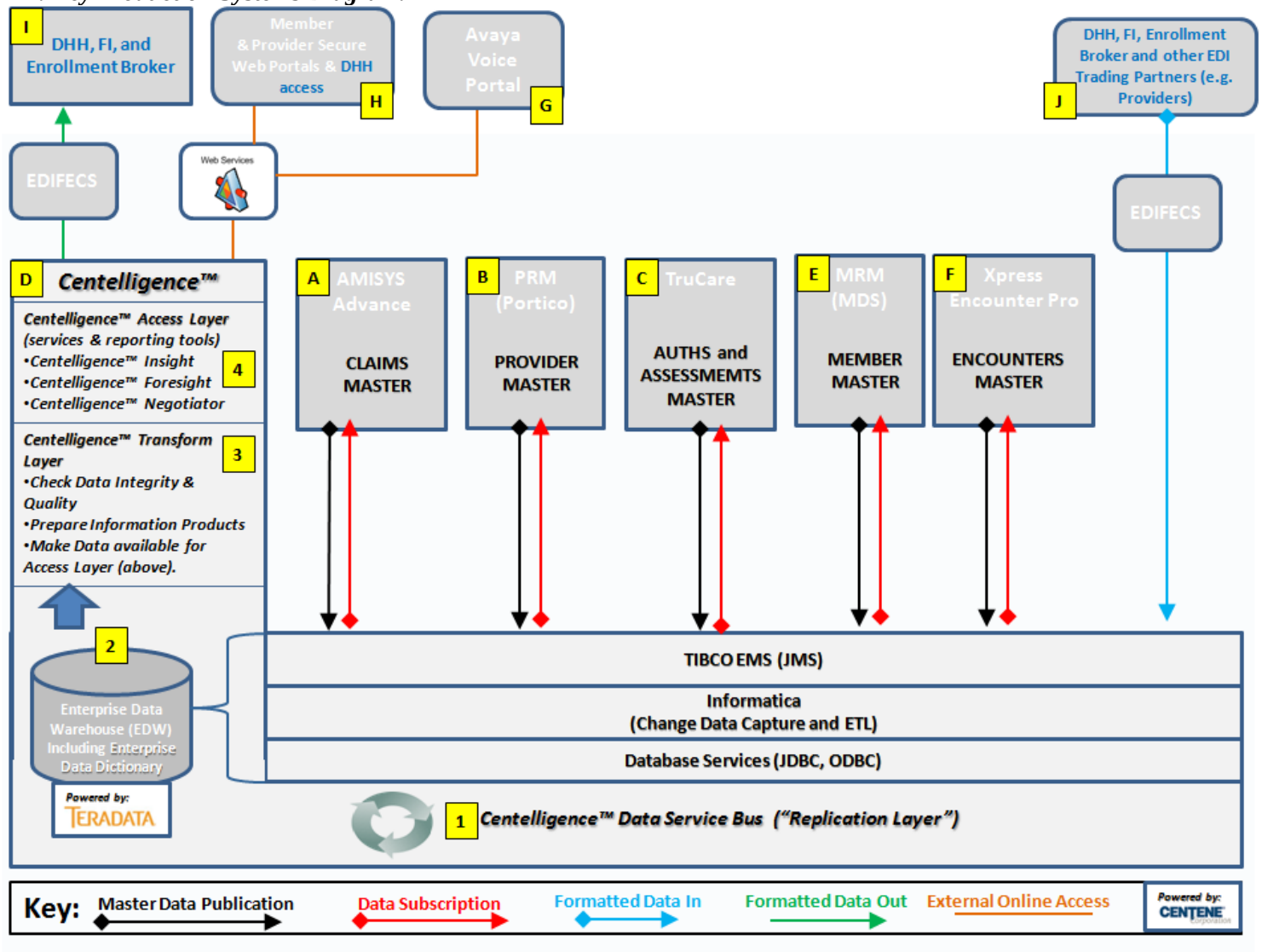
The Centelligence™ EDW **Transform Layer** (**3**) incorporates our systematic cross-application integrity controls. EDW performs quality checks horizontally, vertically, referentially and temporally (trending) to ensure both content quality and to prevent data duplication, and data over- or under-representation.

Access for DHH and DHH's Intermediaries. Finally, Centelligence™'s **Access Layer** (**4**) incorporates the informatics, business intelligence analytics, and standard and ad-hoc reporting tools available to internal and external end users - either directly or via consumable, secured web services. Note that we supply outbound HIPAA transaction files via our EDIFECS EDI system - and would supply encounter data in HIPAA 837 format as well as proprietary formatted files (such as the Provider Directory/Network Provider and Subcontractor Registry specified in Appendix G of the CCN-P Systems Companion Guide) to DHH's Fiscal Intermediary (FI); and member demographic update data in HIPAA 834 format to DHH's Enrollment Broker (item **I**); via the Centelligence™ Access Layer. Also note that we would provide online access for DHH to our Centelligence™ Access Layer - specifically our BusinessObjects Enterprise Suite of decision support reporting tools (**H**). Also shown in item **H**: members can query information and enter information (e.g. demographic updates) via our Member Portal (see Section K, Question K.5 for more information); and providers can conduct a number of self-service administrative operations and interact with clinical information via our secure Provider Portal (see R.15 and R.11 for more information). Our Avaya Voice Portal (**G**) also allows our providers and members to access and enter information via our Interactive Voice Response (IVR) unit. Users can use their touchtone keypad or speak with our voice recognition enable IVR - and essentially interact with the Centelligence™ Access Layer.

Inbound Formatted Data Supported With HIPAA Compliance. Item **J** in R.4-A symbolizes our EDI Trading Partners on the inbound side. We use our EDIFECS EDI system, in conjunction with our COVIANT multi-protocol file communications system, to receive HIPAA, HL7, and other ANSI EDI transactions (such as the TA1, 997 Functional Acknowledgement (FA) and, starting 1/1/12, the 999 FA). We also support any proprietary file formats that our state clients request; such as DHH's proprietary Provider Directory/Network Provider and Subcontractor Registry as specified by DHH in Appendix G of the CCN-P Systems Companion Guide. The "flow" of inbound file management is orchestrated via our TIBCO EMS Java Messaging Service (JMS) based middleware (see TIBCO layer in item **1** in R.14-A). Actual flow is dependent on the inbound file type. For example, . inbound 834 files are automatically processed through our EDIFECS EDI system for HIPAA 4010A or 5010 compliance validation and translation. EDIFECS, in conjunction with our TIBCO middleware also edits for duplicate member records, date criteria validity, field data integrity, and valid date spans. Enrollment and eligibility data passing those edits are then electronically posted into MRM (**E**).

Please see R.2, R.6, and R.7 for more information on our inbound processing of HIPAA 834 and 837 transactions, as well as proprietary format processing.

Figure R.4-A: Key Production Systems Diagram.



Data Element Naming and Formatting.

Data Naming. Our Enterprise Data Dictionary (EDD), is a metadata repository within our EDW and is the master cross reference of all Centene standardized data names and formats. EDD systematically maps each Centene data element name, semantic, and contextual use information with the equivalent metadata information for each best-of-breed key production application we use (meaning AMISYS Advance, MRM, PRM, TruCare, and Encounter Pro). Thus from an external user perspective, data has the same functional name and use - and - at the application database level - names are mapped via EDD. The EDD is administered and maintained by our Data Management Team (DMT), under the oversight of our Enterprise Data Architect.

EDD allows us to maintain high performance data integration, while affording us the flexibility to implement *new* applications in the future, by giving us a metadata abstraction layer that can accommodate any vendor software application in the future, or significant enhancements to applications we have in place today.

For example, in 2010 we upgraded our AMISYS Advance to the HIPAA 5010 compliant version. In line with HIPAA 5010, our AMISYS Advance vendor (DST Health Solutions) changed appropriate field lengths and formats for affected data elements. Through EDD, we were able to easily and effectively implement our new AMISYS Advance version - by simply updating the "AMISYS Advance" side of our EDD element definitions table. Incidentally, EDW is already able to accommodate all HIPAA 5010 and ICD-10 data element minimum length and format requirements.

Data Formatting. Through EDW's Managed Data centralized repository of code lists, we support and enforce all industry standard codesets and data formats for any data affected by those codesets - including HIPAA mandated sets (HIPAA Taxonomy, CPT, ICD, Revenue Codes, etc.), HL7, US Postal Service (USPS), etc.

For data formats that are not governed by an industry standard, we enforce the *format used in the system of record* of that data element. For example, TruCare is the system of record for health care assessments. Not all of the code lists for our assessment responses are an "industry standard," so it is TruCare's definition of those codes that is enforced across all applications by EDW's Managed Data facility.
In all cases, for all data naming and format conventions, our databases, including EDW, enforce American National Standards Institute (ANSI) standard data types, and all our databases are ANSI standard databases.

Our DMT administers and maintains the Managed Data repository, under the oversight of our Data Governance Board (DGB), comprised of representatives from our DMT, MIS Application Development, and representatives from our business areas (claims processing, medical management, call center operations, etc.). EDW's Managed Data repository also drives the business logic for building information assets based on a consistent set of business rules and provides a centralized location for modifications of standardized code lists by authorized individuals of the DGB, ensuring the propagation of those changes across all information assets that consume them (users, reporting tools, other applications). Managed Data lists are exposed to users of our web-based ad-hoc reporting tools, enabling those users to incorporate the same business logic in their reports, facilitating a consistent answer to a common business question both internally and for our external clients.

Data Element Updating and Refreshing. Within the confines of our MIS (our key production systems and Centelligence's four components of data management as depicted in R.14-A), we update data elements amongst consuming applications within the appropriate business cycle - depending on the specific data use, through the Centelligence™ Data Service Bus (item **1** in R.14-A).

Key Production System Data Exchanges: The Right Update Frequency for the Right Purpose. Some data updates need to be distributed as soon as an element is changed in the element's source system (in other

words: "in *real time*"). For example, if there is a change to a member's demographic information in MRM, that change is immediately detected by our Informatica Change Data Capture (CDC) service and immediately updated via a data base interface (in real time) to AMISYS Advance.

Some data updates only make sense on a 24 hour update schedule, because that is the underlying business cycle related to the update. For example, although EDW immediately detects a claim adjudication when that event occurs in AMISYS Advance, EDW does not publish that claim's finalized status (paid, paid amount, denied, etc.) until the end of the batch adjudication cycle in AMISYS Advance - which occurs nightly, every 24 hours. In other words: it does not make sense for Centelligence™'s Access Layer to "tell" an information consumer about the interim steps in claims adjudication (see Section Q, Question Q.1 for our description of the six stages of adjudication) until a claim finishes the adjudication cycle, either resulting in a pay/deny disposition, or a pend status that may require intervention.

Finally, some data updates require an intermediate level of promptness. For these situations, we use a Publish / Subscribe ("pub/sub") messaging approach - where Centelligence™ (through our Informatica middleware) allows our key production systems to subscribe to data updates, and receive those updates every 15 minutes (this parameter is tunable to any time interval, and can be adjusted based on business need), via subscription. For example: AMISYS Advance checks every 15 minutes its "subscription" to TruCare's publication of service authorization data. This allows AMISYS Advance to receive authorization data in NEAR real-time, while allowing AMISYS to avoid resource contention during large claim load or adjudication runs.

For ALL data changes in ANY of our key production systems, the "trigger" that notifies Centelligence™ of that change is any database "write" operation; that is: data creation, edit or delete (if allowed by the applicable system (e.g. TruCare, etc.). This real time Change Data Capture (CDC) trigger detection is possible because our Informatica middleware is constantly monitoring all the relational database management system (RDBMS) logs in all our key production systems, in real time. Because Informatica is monitoring these RDBMS logs, Centelligence can be notified of data updates with virtually no impact on the online performance of any of our key production systems. This CDC action of detecting a key production system data change in real time is depicted with the **black arrows** (labeled "Master Data Publication") in the key in R.4-A.

Conversely, when Centelligence (through EDW) needs to update a consuming key production system - as discussed above - this update occurs according to the specific update - some updates require real time action, some only make sense within the context of a 24 hour business cycle, and some are appropriate via the 15 minute subscription pull.

Please refer to ***Figure R.4-B: Key Production System Interfaces*** (R.4-B) below for a complete matrix of key production data interfaces (source and target), and the frequency and nature of their occurrence. Note that the identifying letters adjoining the Target System names correspond to the letters identifying the systems depicted in R.4-A.

Maintenance and Quality: The Role of MDM. We ensure centralized management and maintenance of data element naming, formatting, and quality through our disciplined approach to MDM administration and governance. In the context of *our* MIS, MDM is essentially the management of data derived from our key production transactional systems (AMISYS Advance, TruCare, MRM, PRM, and Encounter Pro), with all the unique process needs specific to our data warehouse, EDW.

Our Data Management Team (DMT) focuses on the maintenance of data quality and controls with the oversight of our Data Architect to coordinate our data stewardship. The DMT works with key business owners to gain consensus and to focus on in maintaining data quality at a level to support all business needs. In addition, Centelligence™'s (including EDW's) hardware platform is governed by our Architectural Review Board (with active representation from our DMT).

We establish a foundation of master data management, maintenance and quality by scoring the Transform Layer in Centelligence™ (item 3 in R.4-A) with the automated quality checks of data going into EDW for presentation and use by Centelligence's Access Layer (item 4 in R.4-A). A master data management scorecard is systematically generated by EDW (item 2) to provide full transparency into the level of data quality and is monitored by our DMT.

Maintaining Data Integrity Across Data Stored in the EDW. Our MDM process effectively combines data from all sources coming into EDW, and reconciliation processes ensure that data overlap between source systems is reconciled in the EDW - processes performed in our Transform Layer (item 3 in R.4-A). To further support our MDM approach, we have developed corporate governance standards, under the auspices of the DGB, that are strategically designed to promote the extensibility, efficiency, and performance of the data. Our governance strategy includes:

- Standard Business Naming, Formatting, Entity and Attribute Definitions - enforced systematically through our Transform Layer rules and our Enterprise Data Dictionary (EDD - see item 4 in R.4-A) and Managed Data repository as discussed above.
- Business Rules Specification
- Standard Calculation and Summarization Definitions
- Entity and Attribute Aliases

Continuous data quality and integrity controls: Data quality is enforced at several levels in our MIS. We have a number of controls for data coming into - and out of - our MIS: please see Question R.2 for details. Each of the service types in our Centelligence™ Data Service Bus (1), has syntactical edit and integrity checks, with built in error handling controls and with audit trail support. In addition, in our Transform Layer (item 3 in R.4-A) data are checked for conformance to published specification (using our EDD and Managed Data Repository in conjunction with EDW's business logic) on initial load and on each subsequent receipt of data from the key production systems (AMISYS Advance, etc.) via the Data Service Bus (item 1 in R.4-A). EDW presumes inbound data to be inappropriate for consumption until quality validations are complete and data errors are within tolerance range. Data can be rejected by EDW through automated validation and notification processes at the file level when the number of errors exceed tolerances and individual data is tagged with a full set of identifiers noting all issues with the data, in the event the number of errors are within tolerance but the individual data issues may be of interest to downstream systems and consuming applications. EDW performs data quality checks both horizontally, vertically, referentially (referential integrity checks) and temporally (trending) to ensure both content quality and prevent data duplication, and data over- or under-representation.

Figure R.4-B: Key Production System Interfaces.

Key Data Interfaces In Centene's MIS

	Target \ Source	AMISYS Advance	PRM (Portico)	TruCare	Centelligence ™	MRM	Encounter Pro	Avaya Voice Portal / IVR	Web Portals
A	AMISYS Advance		15m[1]	15m	24H[2]	R/T[3]			
B	Provider Relationship Mgt (Portico)			15m	24H				
C	TruCare		15m		24H				
D	Centelligence™	24H	24H	R/T		R/T	24H	R/T	R/T
E	Member Relationship Mgt (MRM)	15m	15m		R/T				
F	MDE xPress Encounter Pro				24H				
G	Avaya Voice Portal / IVR				24H				
H	Web Portals[4]								

Footnotes:

[1]**15m:** These interfaces are Informatica Change Data Capture (CDC) Publish-Subscribe message interfaces. Informatica detects data changes in the source system in real time and publishes these changes to our Centelligence™ *Data Service Bus*. Then the appropriate subscribing applications ("target") poll for published transactions ***every 15 minutes.***

[2]**24H:** Although Centelligence™ is updated on all key production data in REAL TIME, some data is made available to Centelligence™'s Access Layer in a 24 hour timeframe to be congruent with a particular business cycle. For example, Centelligence™ does not release claims data to the Access Layer until AMISYS Advance has FINALIZED the claims in the nightly batch adjudication cycle. SIMILARLY, for some interfaces Centelligence™ updates a production system in a 24 hour cycle, even though Centelligence™ "knows" the update prior to that update. We do this so as not to needlessly impact business hour online performance. For example: care gaps from Centelligence™'s Foresight Predictive Modeling system are based on data over a long span of time - in order to be valid. Thus, there is no purpose in Centelligence to interrupt TruCare during the business day for a care gap processing cycle that occurs bi-weekly.

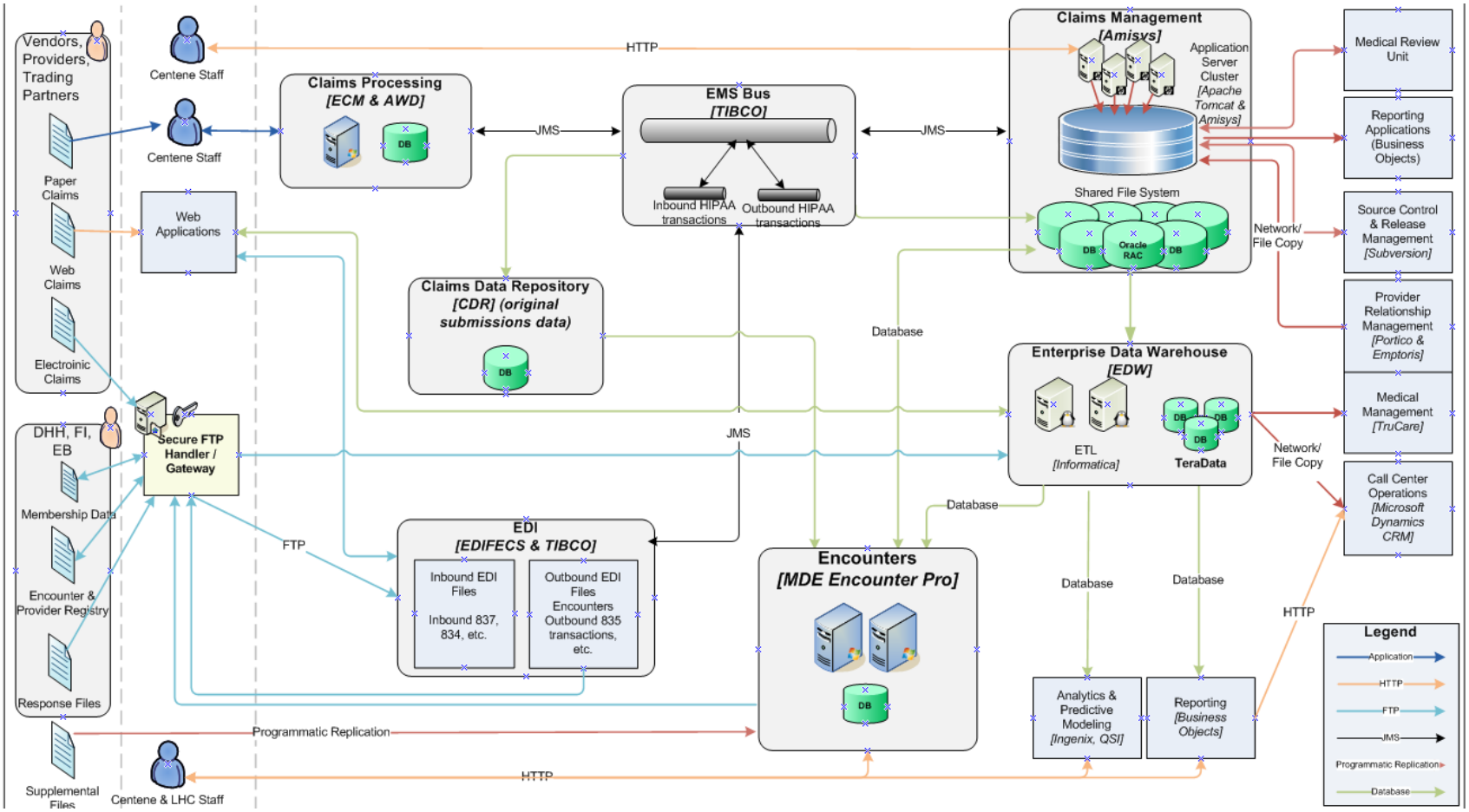
[3]**R/T:** These are **real/time transaction** message updates from Source to Target systems - for business cycles that demand this timeliness.

[4]Our **Web Portals** do not generate core production data. Instead, they access data via service calls to Centelligence™. In addition, users update our systems (for allowed data elements) through our Web Portals - but the Portals (in and of themselves) do not hold core production data.

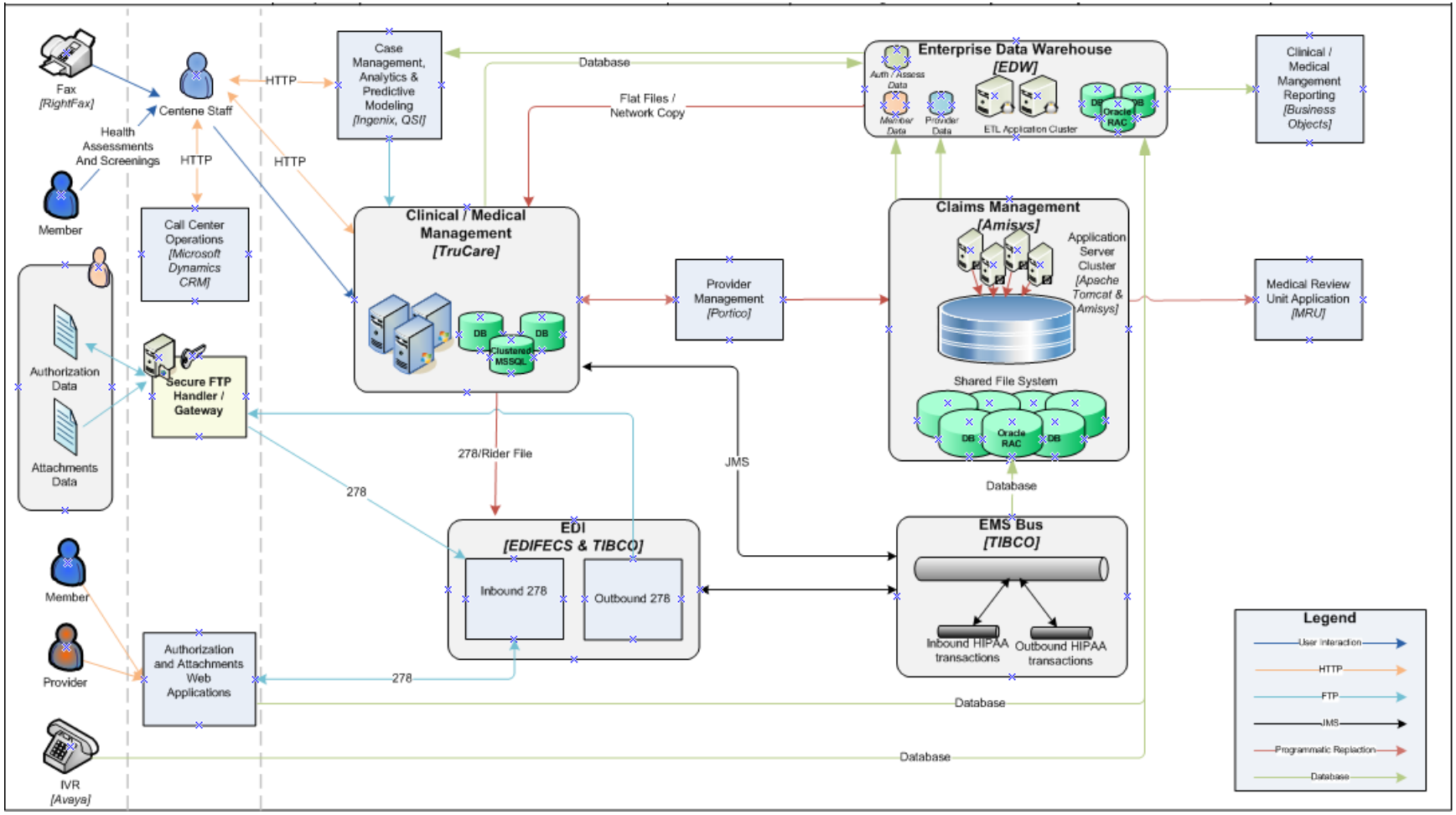
Additional Diagrammatic Information (Physical Level). Please see ***Figures R.4-C: EDW, Claims, Encounter Networking and R.4-D: TruCare, EDW Networking***, and ***R.4.E: EDW Architecture*** for additional diagrams on the physical implementation and networking of our application interoperability infrastructure.

In short, our MIS is engineered with best of breed functional applications and reliable, multi-faceted interoperability. Our MDM governance and open standards based SOA approach allows us to continually enhance our ability to securely and accurately handle data - from data collection, through data processing, information insight and ultimately actionable impact, providing a seamless flow of data across our organization from its entry source all the way through to our enterprise data warehouse (EDW) to information consuming applications and users. This allows us to eliminate errors because source data is entered only once and then used consistently across all of Centene's application platforms and systems.

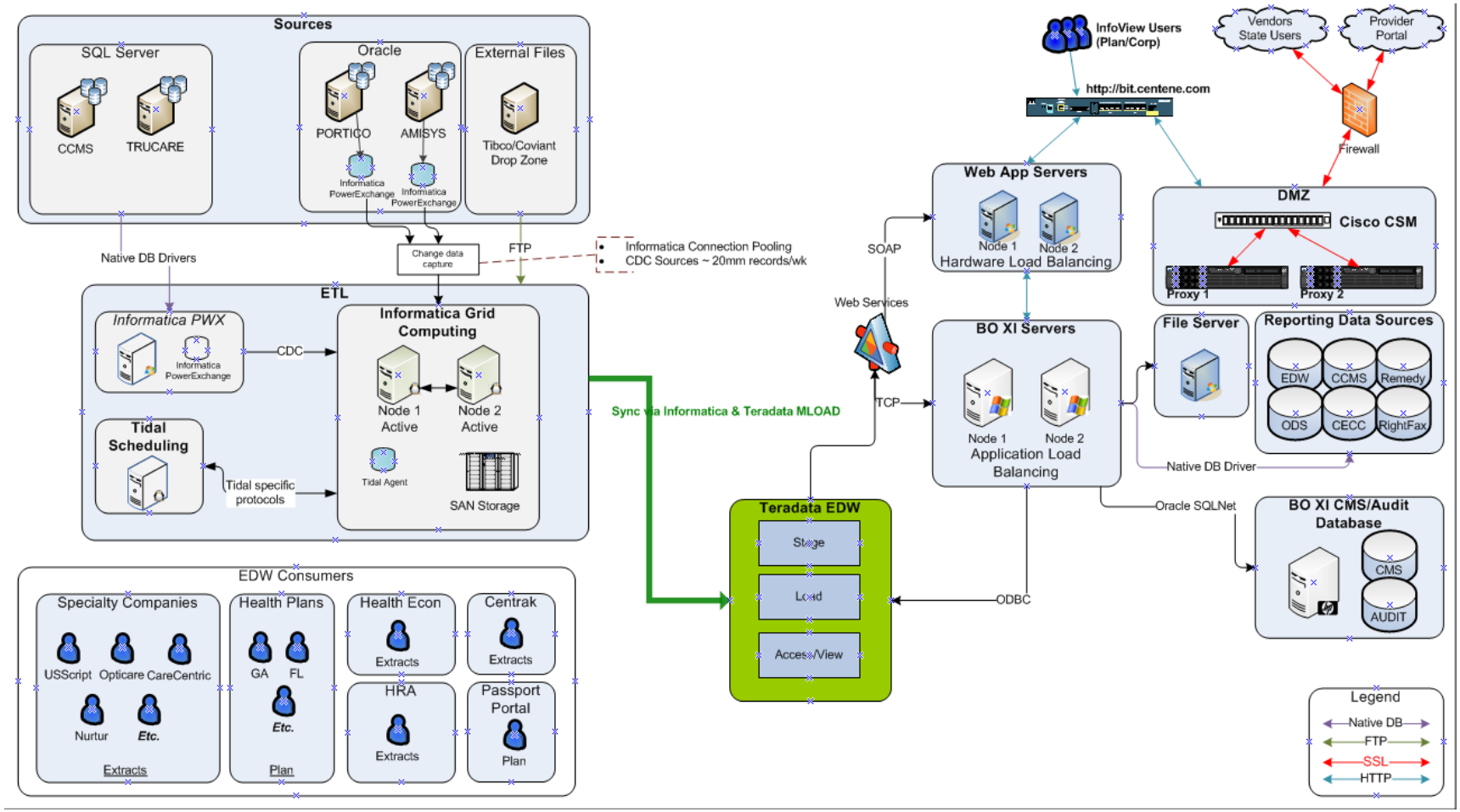
R.4.C: EDW, Claims, Encounter Networking.



R.4-D: TruCare, EDW Networking.



R.4-E: EDW Architecture.



Question R.5

Providing and Storing Encounter Data

R.5 Describe your ability to provide and store encounter data in accordance with the requirements in this RFP. In your response:

- Explain whether and how your systems meet (or exceed) each of these requirements.
- Cite at least three currently-live instances where you are successfully providing encounter data in accordance with DHH coding, data exchange format and transmission standards and specifications or similar standards and specifications, with at least two of these instances involving the provision of encounter information from providers with whom you have capitation arrangements. In elaborating on these instances, address all of the requirements in Section 17. Also, explain how that experience will apply to the Louisiana Medicaid CCN Program.
- If you are not able at present to meet a particular requirement contained in the aforementioned section, identify the applicable requirement and discuss the effort and time you will need to meet said requirement.
- Identify challenges and "lessons learned" from your implementation and operations experience in other states and describe how you will apply these lessons to this contract.

Encounter Submissions – People, Business Processes and Technology

Louisiana Healthcare Connections' (LHC) parent company, Centene Corporation (Centene), has over 25 years of experience submitting encounters for public sector health care programs. Centene currently processes and submits over 2.2 million encounters per month from over 100,000 medical and behavioral health providers across the 11 health plans for which we provide services. We will leverage our organizational structure, expertise, technology, and lessons learned to ensure the integrity, validity, and completeness of all data, including encounters, we exchange with DHH and DHH's fiscal intermediary.

LHC and Centene understand that successful encounter submissions are critical to the CCN Program (CCN-P) and that DHH will rely on accurate, timely, and complete encounter data for a number of purposes including, but not limited to, program and contract oversight, utilization of services, rate setting, and compliance reporting. Our systems will be ready to exchange encounter data with the DHH fiscal intermediary within 60 days of operations and in the format as specified in the Systems Companion Guide.

Local and Nationwide Experience Ensures Success. Centene will provide LHC with technology support, financial reconciliation services, and error review and resolution services, to support our encounter submission quality and error management processes. Our national experience will complement LHC's local experience with *best practice disciplines* to provide DHH with accurate, timely, and complete encounter submissions and an effective error management process. Centene health plans meet regularly to review encounter submission processes and discuss best practices. This allows us to leverage experiences learned from other states for use in our continuous improvement efforts. We will organize our Encounters Team at LHC and Centene to leverage the expertise of Centene so that we consistently provide excellent service to DHH.

Centene's Encounter Business Operations Unit. Centene's Encounter Business Operations (EBO) unit will serve LHC as a centralized resource supporting encounter submissions. The EBO fosters strong relationships with key functional areas critical to a successful encounters process such as Finance, Claims, and Information Technology. Although all of our state Medicaid contracts differ in encounter format, business rules, and contract requirements, our goal of accurate, timely, and complete encounter submissions is consistent. Through daily meetings between EBO and IT, we are able to quickly and confidently adjust to necessary changes in requirements, while understanding the impact to other items. These daily meetings are also an opportunity to learn from our accomplishments with other health plans and translate that into further enhancements and efficiencies by implementing similar changes with LHC.

Within the EBO, LHC will have an Encounter Specialist who will work with LHC encounter resources and DHH and, where necessary, leverage the nationwide expertise of other EBO resources to address any

new DHH requirements. The EBO team will be dedicated to successful LHC encounter processing, encounter submissions, responses, error corrections, and related follow-up activities. The EBO and LHC team will represent a service team focused *solely* on encounter reporting needs, and provides dedicated resources with the experience and expertise to ensure accurate and timely encounter reporting.

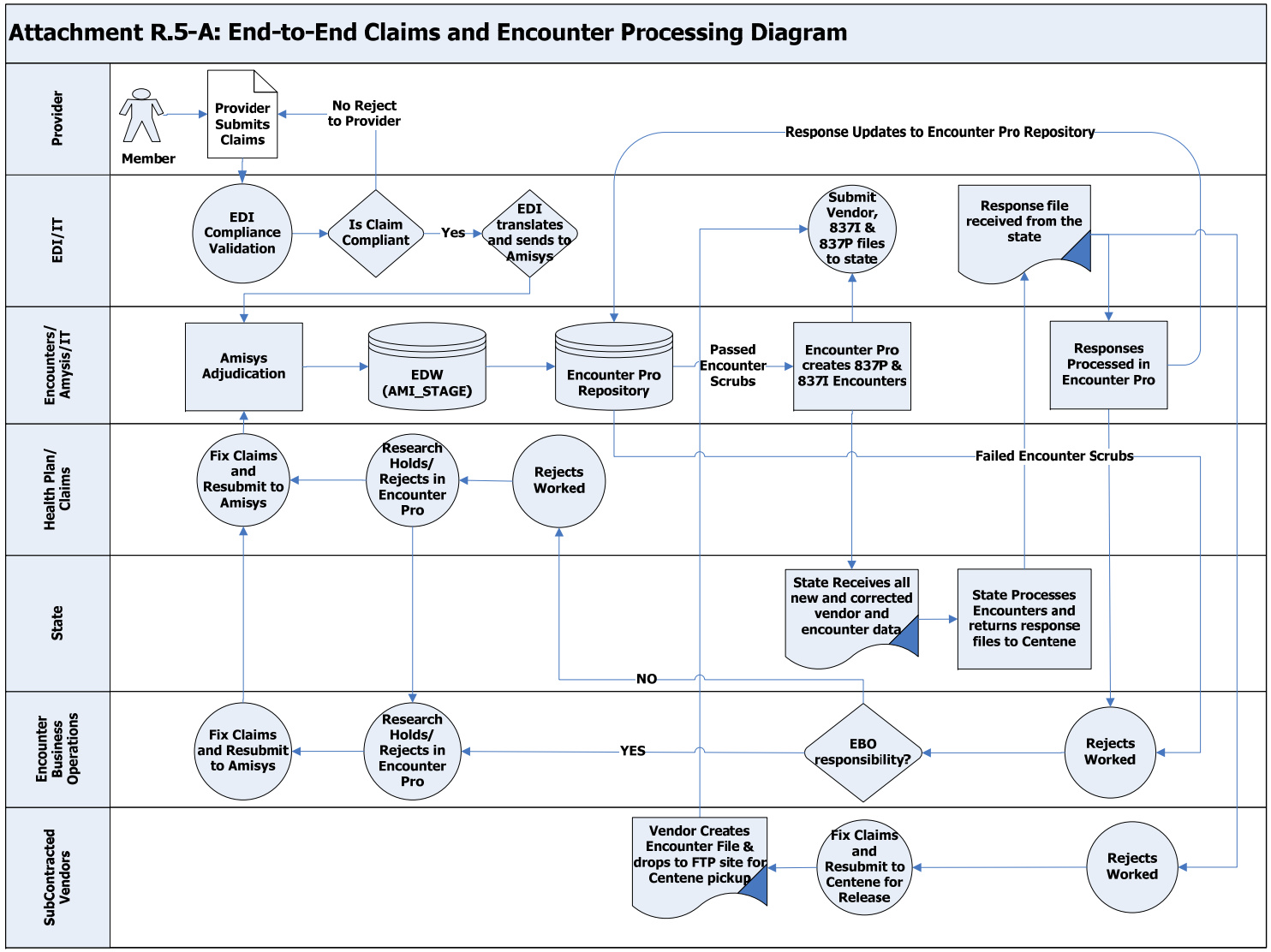
Local Partnership with DHH. LHC will provide an encounter analyst who will acquire the specific knowledge about DHH's encounter processing rules, and who will be responsible for the overall submission and correction of encounter data for LHC. They will provide critical feedback into the claims adjudication and encounter reporting processes, as they best understand DHH's requirements and expectations. LHC will provide DHH timely notification of any significant changes we make to our systems that could impact the integrity of our claims or encounter data, including new software and strategic partnerships. LHC and Centene view DHH as a *partner* in our encounter reporting process and we will continue to work openly and collaboratively to resolve technical issues and to meet any additional requirements that enhance DHH's administrative oversight processes. LHC's CEO or CFO will also provide attestation to the truthfulness, accuracy, and completeness of all encounter data submitted to DHH and the fiscal intermediary.

To ensure optimum encounter processing, Centene will facilitate and enable a strong partnership between LHC, our providers, DHH, and our corporate EBO team. This four-way partnership will ensure the entire encounter submission process comes together, starting with inbound claims submissions from providers; through accuracy and completeness checks performed by LHC; to submissions to DHH; receipt of DHH's acknowledgement and process results files; and subsequent reconciliation with DHH on each encounter. The result is a disciplined process coordinating the four parties to serve DHH needs and which has produced consistently positive results in other states.

Claims to Encounter Life Cycle – Delivering Results for DHH

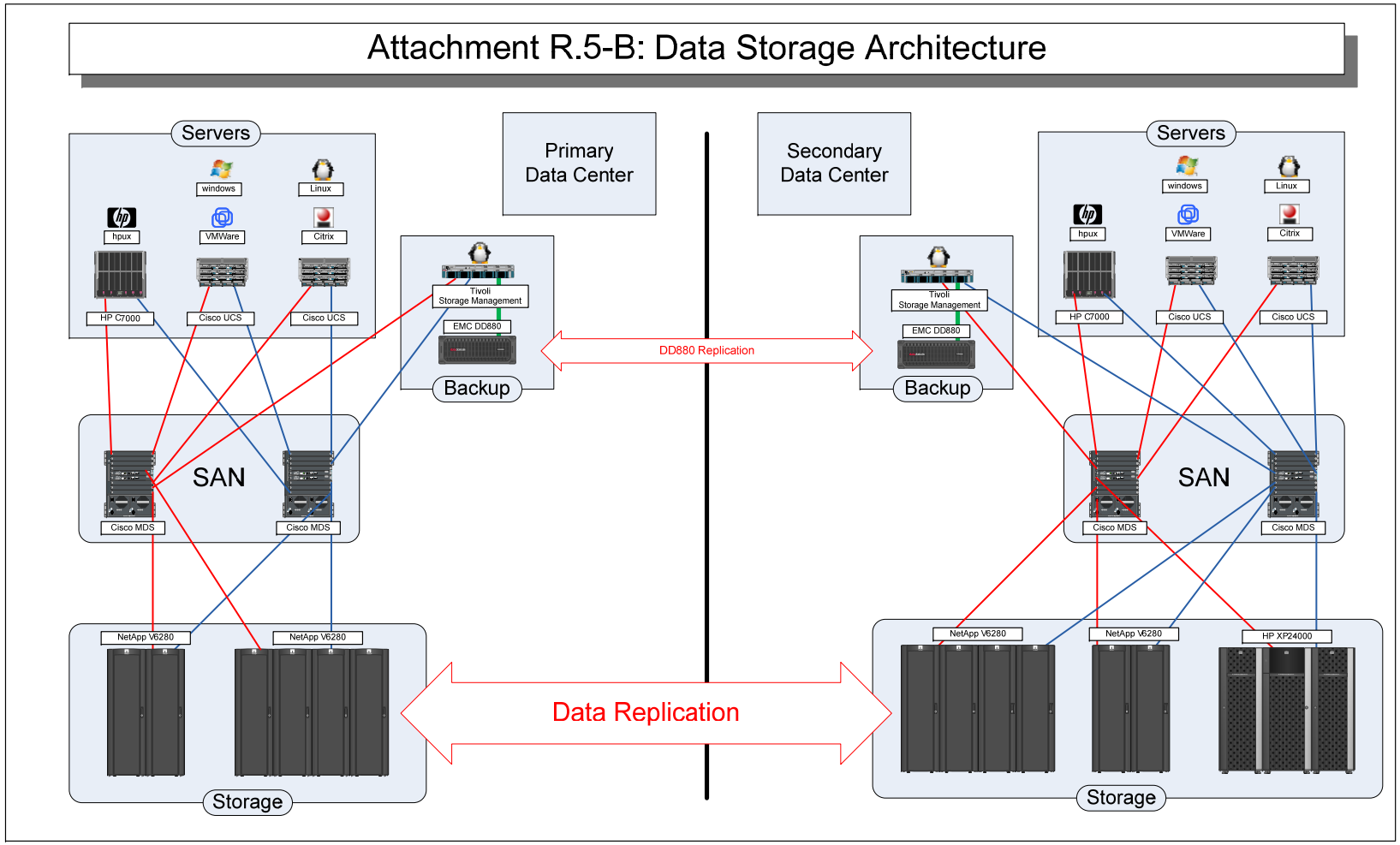
LHC and Centene view claims processing not just as an exercise in compliance with payment rules, but also as a critical opportunity to offer 'best practice' service to our providers and DHH. We also see the claims process as a critical data gathering aspect of our operation, since it supports our quality and utilization monitoring efforts, and results in ***supplying DHH with accurate, timely, and complete encounter information***. At each stage of the process, beginning when the provider submits a claim to LHC until we, in turn, submit the encounter to DHH, we will have an infrastructure comprised of people, technology, business processes, and system controls to ensure the highest quality encounter submissions to DHH. For the discussion below, please reference Figure R.5-A: End-to-End Claims and Encounter Processing Diagram for a visual representation of our claims and encounter life cycle.

Figure R.5-A: End-to-End Claims and Encounter Processing



Data Storage - Designed for Success. Our Enterprise Data Warehouse (EDW) is powered by Teradata®'s Extreme Data Appliance which enables Centene to house and manage enormous amounts of data. For a visual representation of our data storage technology, please reference Figure R.5-B: Data Storage Architecture. Centene has employed a best-of-breed Teradata enterprise data warehouse solution that has been recognized across the industry as the leader in data access performance and scalability. Teradata provides Centene and LHC with the ability to store and access encounter data with relative ease. EDW supports access to all data necessary to manage the entire encounter process, including any need for extended encounter data reporting, analytics, or reconciliation process. For more information on our EDW architecture, please reference our response in section R.4, Data Integrity and Interoperability and section R.10, Reporting.

Figure R.5-B: Data Storage Architecture



Automating the Encounter Submission Process. Once AMISYS Advance adjudicates claims to a finalized status, our MDE (Medical Data Express) Xpress Encounter Pro (Encounter Pro) workflow system will extract, prepare, and submit the data as encounters to DHH. MDE has a proven track record within the Medicaid industry of providing the necessary submission and correction functionality to meet encounter submission guidelines as required by all of our state partners. We will configure Encounter Pro to submit encounter data that complies with all DHH standards for electronic file submission, standard HIPAA file format (specifically including ANSI X12N 837 provider-to-payer-to-payer COB transaction format), file size, submission frequency, and submission method as required by DHH. Our encounters will capture the same line item detail regardless of the claim type, disposition (e.g., paid or denied), third party liability indicators, or capitation arrangements. We will include all rendered services, original and adjusted claims, application of retroactive fee or member changes, etc., in a *single* encounter file as appropriate for the claim type, inclusive of any encounters collected from our subcontracted vendors, for submission to the fiscal intermediary. We will also adhere to NCQA, AMA coding, UB-04 editor, NCCI, and DHH standards regarding the definition and treatment of certain data elements captured on claims, use of standard codes (including CPT Category I and II, HCPCS Level II and ICD-9-CM), counting methods, units, etc. As described below, we will conform to all current and future standard code sets in compliance with federal guidelines. Centene will retain all data elements in our claims history necessary for creating encounters in compliance with DHH and the fiscal intermediary requirements.

Specific functionality provided by Encounter Pro includes, but is not limited to:

- Support of DHH-specific business rules to “scrub” data prior to submission
- Automation of LHC defined actions, in conformance with DHH guidelines, to correct repairable encounters
- Linkage to base claim database, outbound encounters, and inbound acceptance reports to facilitate comprehensive encounter reconciliation efforts
- Automated prioritization of encounter correction activities
- Extensive operational and executive reporting to identify encounter trends, monitor acceptance rates, and proactively correct issues
- Automated extract and delivery mechanisms to minimize bottlenecks and the need for manual intervention

In addition to the edit process described above, Encounter Pro includes a module that provides a ‘pre-submission scrub’ mechanism to customize and apply edits to encounters, prior to DHH submission, as a final check for encounter accuracy prior to submission to the state. We will configure Encounter Pro to recognize conditions that will cause an encounter to deny at DHH and hold the claim for review. This will allow us to work with providers to correct any issues and/or reprocess the claims for a valid encounter submission.

Once processed, the encounter data is batched into appropriate HIPAA standard 837 files and will be submitted in accordance with DHH timeliness requirements. Encounter response files are processed by the Encounter Pro application, updating the encounter history and identifying encounters that must be reprocessed. Encounter Pro provides an online management tool and extended reporting for encounter submission and response analysis. For example, as errors are reported in the DHH response file, Encounter Pro provides a platform by which each error can be researched by our EBO and LHC encounter staff. Once the solution is determined, the claim will be reprocessed and the encounter is then resubmitted using the Encounter Pro application.

Root Cause Analysis and Resolution to Improve Encounter Submissions. Centene and LHC will follow a systematic approach to identify and resolve underlying causes of encounter submission errors and will not solely focus on data correction processes. Please refer to Figure R.5-C: Encounter Error Root Cause Analysis and Resolution Flowchart and Figure R.5-D: Encounter Process Continuous Quality Improvement for visual representations of this process. Centene and LHC’s Continuous Quality

Improvement (CQI) approach will focus on the entire life cycle of a claim from inbound claim submission through encounter acceptance. LHC and Centene staff will regularly perform a number of tasks designed to identify, quantify, and subsequently resolve potential provider claim issues that might ultimately impact encounter processing. For example, we will:

- Conduct a review of weekly check audit results to identify potential areas of concern
- Attend DHH encounter meetings to assist us in identifying additional areas of concern and opportunities to continuously improve our processes
- Utilize DHH provider billing manuals and incorporate them into our own manuals to guide provider claim and LHC encounter submission

When we identify a provider claim issue that impacts encounter submissions, LHC staff will review electronic claim images, AMISYS Advance configuration, and Encounter Pro edits to determine the specific reason behind the issue. Once we have reviewed all of this information, our staff will develop the appropriate corrective action(s) necessary to resolve the issue. For example, based on our highest reject reasons, we might identify specific edits that need to be moved to the front end of our claim processing system to reject or deny inaccurate claims submissions as early as possible in the process.

These activities allow the claim to be corrected and submitted accurately by the provider. We can then, in turn, submit an accurate, timely, and complete encounter to DHH.

Moving Edits Earlier in the Process for More Accurate Encounters. Centene is currently mid-stream in our organization-wide effort to move edits identified in the 'pre-submission scrub' process that identify potential encounter rejections, to the *front end* of our claims adjudication process. We have incorporated some of these encounter edits into AMISYS Advance and we anticipate many further edits will be integrated as part of our CQI process. As always, we will engage our providers and educate them about these changes in advance so that they are able to quickly correct their system and submit claims in an, even more, accurate and timely manner. Using this process, LHC will closely monitor compliance with conditions that are of particular interest to DHH (e.g., denials for medical necessity, member other insurance, prior authorization not on file, claim submitted after deadline and service not covered) to ensure we are proactively identifying and resolving any issues *before* claims processing and submission to DHH. Please refer to Figure R.5-E: Encounter Edit/Validation Placement Diagram for a depiction of current and future edits.

Figure R.5-C: Encounter Error Root Cause Analysis and Resolution

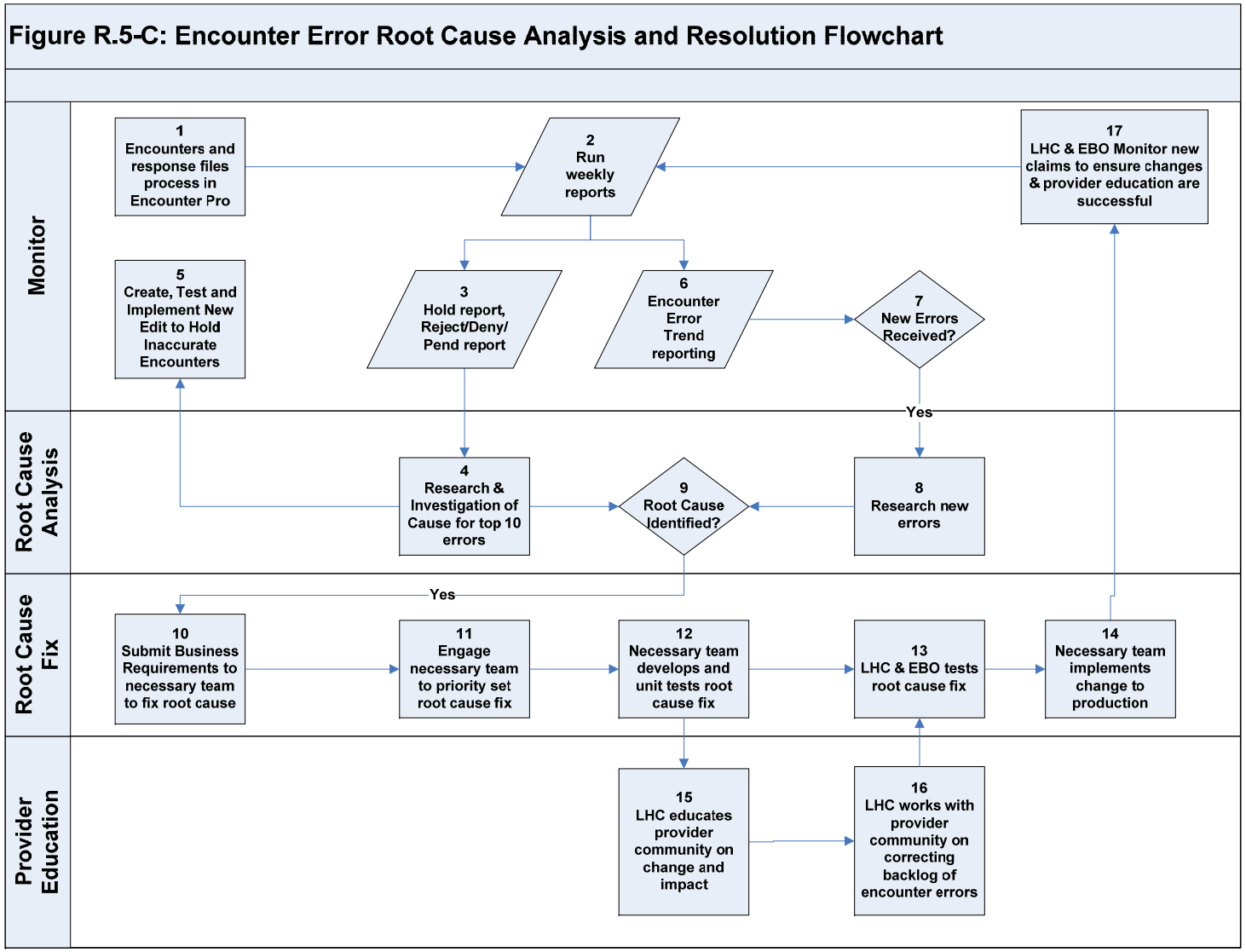
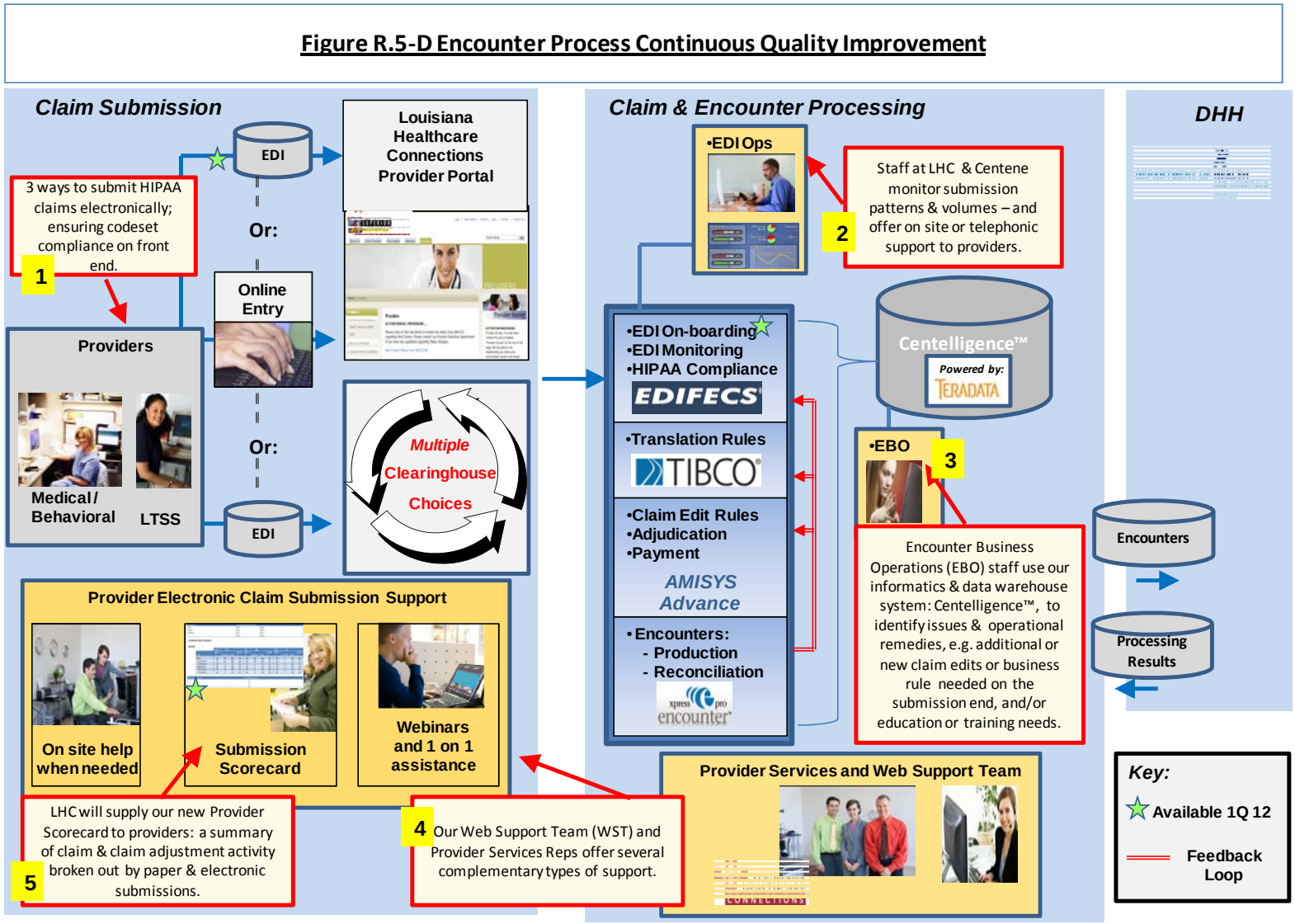
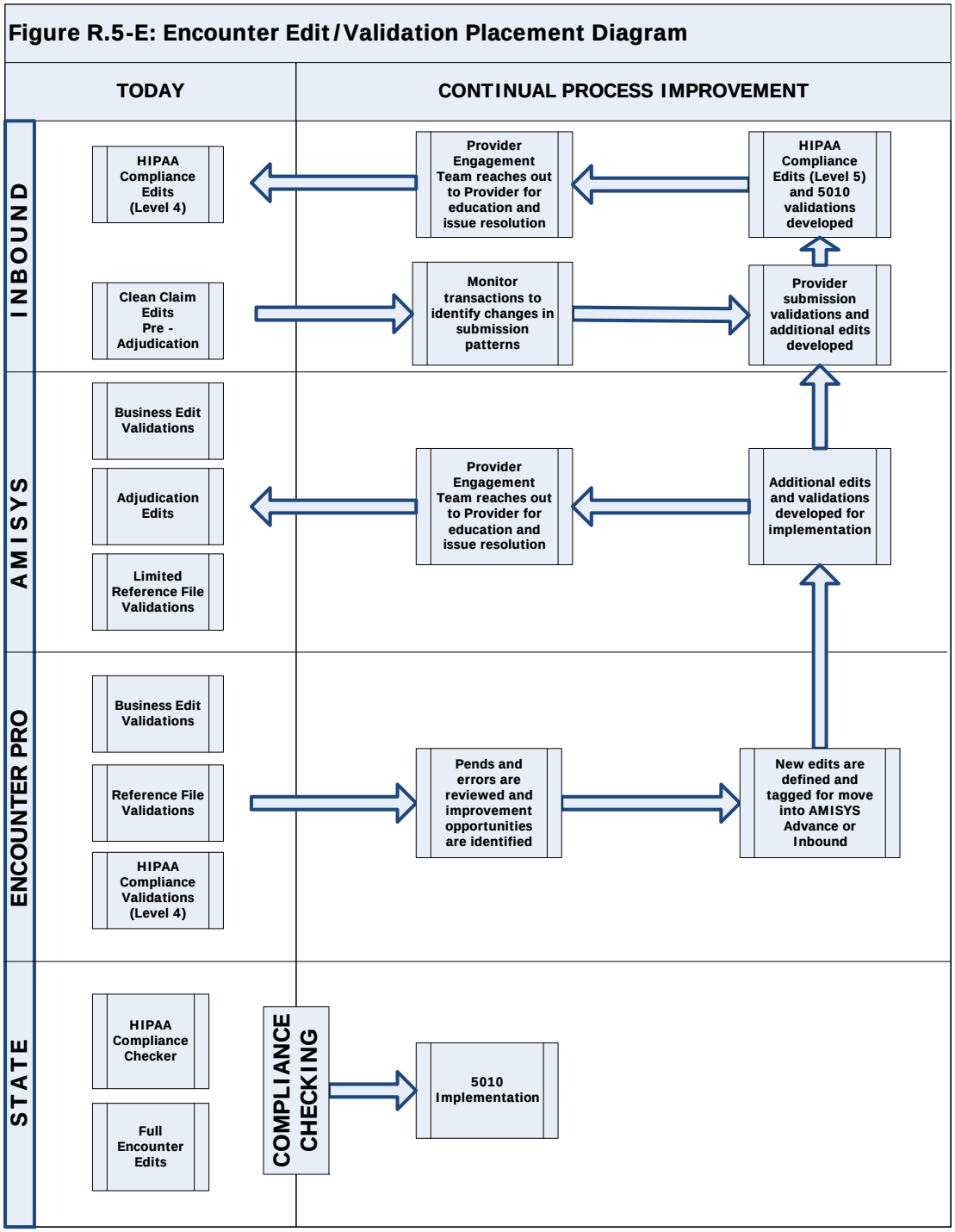


Figure R.5-D: Encounter Process Continuous Quality Improvement



R.5-E: Encounter Edit/Validation Placement Diagram



Provider Education. LHC's focus on encounter accuracy begins with our providers and the *claim submission process*, which is why we apply identical HIPAA compliance and other DHH-specific business validation rules to all claims we receive, no matter the media (EDI, web, or paper). We employ multiple stages of systematically controlled claims and encounter editing and processing to ensure submitted encounter batches are accurate and valid. Our EBO *monitors* encounter accuracy by regularly validating a random sample of encounter records against the source claim data in AMISYS Advance. LHC will incorporate assessment standards, jointly developed with DHH, into our Encounter Data Quality Validations. LHC will support our Louisiana providers by guiding and assisting them with timely and complete claims submissions. When a provider joins the LHC network, through one-to-one training opportunities, through webinars, or targeted instruction, LHC will provide comprehensive training on claims submission processes. Via our Provider Portal and Provider Operations Manual, we will provide reference materials and resources needed to submit complete and accurate claims to our providers. We will encourage them to submit claims using one of the electronic submission processes we make available to them, including submitting professional and institutional claims, using our online template or via batch 837 claims Electronic Data Interchange (EDI) files through any one of the 60 trading partners we currently support, or with any clearinghouse they select who can meet our EDI standards.

Based on our expertise in other states, LHC and Centene staff will regularly perform a number of tasks designed to identify, quantify, and subsequently resolve potential provider claim issues that might ultimately impact encounter processing. For example, we will:

- Conduct a review of weekly check audit results to identify potential areas of concern
- Perform audits for new providers within 90 days of contracting with LHC to identify and resolve claims issues early, before they have a significant adverse impact on the provider's operations
- Present DHH-oriented workshops to providers focusing on claims submission and processing, and answering provider questions
- Perform onsite visits and orientations to individual provider offices to specifically discuss claims and encounter processing and to resolve any existing problems

The effort to educate and work with Louisiana providers directly, combined with technology and controls in the claim submission process will provide a solid foundation for the submission of quality LHC encounters to DHH and the fiscal intermediary.

A History of Success in Delivering Results – Our Experience in Other States

Accuracy. Currently, Centene submits, on average, more than 2.2 million encounters per month across all of our plans, with an average first time success rate of over 97%. When we do have errors, we systematically review these to identify and resolve issues as described above.

The EBO ensures encounter accuracy by regularly validating a random sample of encounter records against the source data in AMISYS Advance. We perform this audit, at a minimum, whenever we modify or change our software configuration or whenever we discover that an incorrect encounter record was submitted and that our usual correction processes cannot correct the error.

The following table illustrates the experience of Centene's health plan subsidiaries in submitting encounter data for our affiliate health plans.

Acceptance Rates – 12-Month History

Month	AZ-LTC	FL	GA	IN	MA	OH	SC	TX	WI
Jun-10	96.79%	99.92%	99.96%	99.38%	99.94%	98.25%	98.98%	99.88%	78.07%
Jul-10	96.09%	98.43%	99.95%	99.76%	99.90%	99.11%	99.65%	99.87%	99.34%
Aug-10	95.04%	98.39%	99.93%	99.93%	99.50%	99.42%	99.00%	99.91%	99.90%
Sep-10	97.59%	98.76%	99.94%	99.85%	99.30%	99.30%	99.54%	99.93%	99.70%
Oct-10	95.08%	98.64%	99.91%	99.91%	91.55%	99.70%	99.39%	99.89%	97.90%
Nov-10	96.17%	98.20%	Held	99.93%	79.91%	99.62%	99.04%	99.88%	99.60%
6-Mo Avg	**96.13%**	**98.72%**	**99.94%**	**99.79%**	**95.02%**	**99.23%**	**99.27%**	**99.89%**	**95.75%**
Dec-10	96.73%	99.46%	Held	99.34%	99.47%	98.18%	99.59%	98.55%	99.70%
Jan-11	95.61%	99.62%	97.82%	95.51%	67.55%	97.14%	98.92%	99.92%	99.74%
Feb-11	95.60%	99.97%	95.18%	99.37%	98.29%	99.62%	96.96%	99.53%	99.68%
Mar-11	95.99%	99.99%	92.12%	99.96%	97.62%	98.38%	99.72%	98.54%	97.97%
Apr-11	83.54%	99.95%	98.02%	99.90%	99.99%	99.99%	94.41%	99.62%	99.62%
May-11	95.69%	95.21%	97.74%	99.98%	99.96%	99.67%	97.78%	99.96%	99.68%
12-Mo Avg	**94.99%**	**98.30%**	**98.06%**	**99.40%**	**94.42%**	**98.87%**	**98.58%**	**99.62%**	**97.58%**

Meets Centene Submission Standards
Short-term fall below internal standards
Significant change required (e.g. state change)

Notes: GA encounter submissions were held per state request in November and December 2010 due to the transition to a new Fiscal Agent. We experienced challenges with submitting encounter data to the new FI when we restarted submissions; however, we have made the necessary changes in our system to ensure we increased our acceptance rates appropriately.

Timeliness. Centene creates encounters for each claims payable run and we currently meet or exceed the timeliness standards established by our state clients. The EBO and LHC will closely manage timely error resolution. Checks on job completion are conducted for each submission and errors are rectified by *on call* programming staff or through our change control process. LHC and our EBO team will create and submit encounter files to DHH on a fixed weekly or monthly schedule, but can easily adjust our submission schedule based on self-monitored metrics (e.g., volume) or at the special request of DHH. LHC and our EBO monitor and ensure all standards are met as defined in the DHH Companion Guides. LHC commits to submitting at least 95% of *all* encounter data on a monthly basis no later than the 25th calendar day of the month following the month the claim was adjudicated, including encounters with a zero dollar pay, if applicable. We will also correct encounters failing quality standards within DHH-established timeframes, including 90% of repairable errors addressed within 30 calendar days and 99% of repairable errors within 60 calendar days. One important aspect of timeliness is having an appropriate mechanism for ensuring delivery and receipt of encounter submissions. Centene can receive encounter acknowledgement and process results files back from DHH in a variety of formats including proprietary, HIPAA/ANSI 835, ANSI 824, or unsolicited 277 formats.

Completeness. LHC's encounter submissions will include *all* paid claims and encounters adjudicated for our members, including those submitted by non-participating providers and our subcontractors, *and* will include both fee-for-service payments and capitated services. LHC does not anticipate a significant

number of capitated arrangements, if any, and; therefore, the impact of zero dollar encounters is mitigated. However, LHC will nonetheless maintain local resources to monitor and analyze submitted claims and encounters to ensure LHC collects and subsequently submitted *all* required data to DHH and the fiscal intermediary. Through continual provider interaction and claims trend reporting, LHC will verify providers are submitting valid claims for services provided.

Reconciliation. Each month, LHC will balance paid claims and encounters to ensure submitted encounter batches are complete. Using our Centelligence™ Insight reporting platform (see response to section R.10 for information on Centelligence™ Insight), we will compare total claims payment amounts to the total payment amounts processed within Encounter Pro on a monthly basis**.** These totals are then compared to the total paid amounts contained in that month's encounter submission. Using this process, we account for every paid dollar and we verify that all finalized claims have been processed as encounters and is inclusive of all payment adjustments, settlements, pends, and denials.

Experience Meeting DHH Objectives in Other Markets

Centene has successfully implemented encounter submissions for all of our health plans. That experience, in conjunction with the configuration capability of our xPress Encounter Pro system, will make the work we do for LHC a low-risk, incremental-change proposition. Centene actively works to leverage lessons learned from other states and applies them as part of our continuous process improvement efforts (see Lessons Learned section below). For example, the VPs of Finance for all of our health plans meet regularly to review processes and discuss best practices, including encounter submissions. Each health plan has learned from the other and made combined recommendations to Centene for consideration. The result is a tremendous amount of experience and success in deploying effective technology solutions and resources with experience processing encounters in multiple states. Our technology, combined with a staffing model designed to leverage our nation-wide experience with Louisiana-based resources, positions LHC to meet any encounter submission requirements as may be required by DHH. Centene's effective testing and validation process is a critical component in our approach to encounter processing and we look forward to iterative end-to-end testing cycles with DHH and the DHH's fiscal intermediary.

National Experience, Local Results. Centene currently supports the submission of encounters for 11 health plans operating in support of public sector programs. In aggregate, Centene's historical and on-going experience serves as an invaluable asset as we look to implement new programs such as CCN-P. Centene will bring knowledgeable and experienced resources familiar with DHH encounter requirements to provide a seamless and comprehensive encounter implementation. To illustrate our national experience, we provide three specific examples in which we currently submit encounter data in a similar manner as that defined by DHH.

Current Experience Processing Data. Centene currently manages the encounter submission process in each of the states in which we operate a health plan. We utilize state required formats to submit data in each state, as seen in the table below. Regardless of format, each has unique (though similar) pend or denial correction protocols. In all cases, we regularly meet local state technology and business requirements in the submission of accurate, timely, and complete encounter data.
A key differentiator for Centene is our organizational focus on public sector Medicaid programs. The submission of Medicaid encounter data to various state agencies presents distinct challenges Centene has been able to overcome throughout our years of processing data. Over the years, Centene has developed Medicaid-specific business processes, controls, and technologies designed *specifically* and *exclusively* for the continued successful submission of Medicaid encounter data.

As evidenced by the table below, Centene's experience with encounter data extends from 27 years of operating a health plan in Wisconsin to recent implementations completed in 2011. Centene's breadth of experience demonstrates success in submitting encounter data over an extended length of time, inclusive of the many changes necessitated by federal or state requirements. The more recent implementations provided us with recent and *relevant* experience submitting encounter data within the current regulatory

environment. This means Louisiana gets the best of both worlds with Centene: depth of experience gained only through consistent encounter management processing over time plus recent understanding of how encounter data is utilized to support newer regulations and business operations.

Centene Operated Plan	* Current / Future Utilization of HIPAA 837?	HIPAA Level	First Year of Operation**
Wisconsin	Yes – Q4 2011	Current - State Proprietary	1984
Indiana	Yes	Level 5	1994
Texas	Yes	Level 3+	1999
Ohio	Yes – 8/4/2011	Current - State Proprietary	2004
Arizona	Yes	Level 5	2006
Georgia	Yes	Level 4	2006
South Carolina	No	Level 4	2007
Florida	Yes	State Proprietary	2007
Massachusetts	No	Level 4	2009
Mississippi	Yes	State Proprietary	2011
Illinois	Yes	Level 2	2011

* Note: Indicates current or planned use of HIPAA 837 files. ** Indicates year Centene began managing health care services for the state. All HIPAA 837 implementations occurred on or after 2003.

For Louisiana, Centene and LHC will leverage our existing encounter management experience to submit timely, accurate, and complete encounter data to DHH and its fiscal intermediary (or any other DHH agent as required) in compliance with the requirements specified in the RFP and as described above in response to this question. Our experience in the Medicaid industry has given us the tools and skills necessary to meet all DHH-specified coding, data exchange formats, and transmission protocols. We strive to leverage data standards across all of our health plans for ease of processing but retain extensive flexibility in our technology and business approach to accommodate state-specific needs. Our demonstrated success in processing Medicaid data for 11 public sector programs has prepared us with a multitude of experienced resources and targeted technology solutions relevant to the Louisiana program. We look forward to bringing our experience to Louisiana and applying our solutions to the benefit of the CCN-P Program.

We also provide three specific examples below as further demonstration of our experience submitting encounter data. Within each example, we also present details on how we have resolved or managed a unique encounter processing scenario. We will use the same customized approach with DHH and the fiscal intermediary to establish an efficient and productive encounter management process. Although each of the health plans we manage have unique situations and specifications particular to their Medicaid program, all present similar requirements to that as defined by DHH. Given our breadth of experience over time, we do not anticipate issues in meeting the DHH or fiscal intermediary requirements.

In each example below, we manage capitated arrangements with providers and are familiar working with providers to ensure all capitated services are reflected appropriately in our encounter submissions. For example, in Florida, we conducted a focused analysis to evaluate the level of services reported by each of our capitated providers in comparison to the established capitation rate we were currently paying. As a result, we were able to identify which providers were not fulfilling their contractual obligations by submitting complete encounter data. Subsequently, using this analysis, we were able to work with those

providers to actively work towards documenting and submitting all requisite encounters to us for submission to our state client. Similar processes are actively in use with our capitated providers in both Texas and Georgia in the examples below. We will bring this level of experience and understanding to Louisiana to ensure the level of encounters we submit to DHH and their fiscal intermediary accurately reflect the actual services provided to our members.

Example #1 – Texas. Centene has been processing and submitting encounters for our affiliate Superior HealthPlan (Superior) in Texas for 12 years. For Superior, we regularly reconcile financial and encounter data on a quarterly basis, including the data for our capitated providers. Our state client, the Texas Health and Human Services Commission (HHSC), requires a 98% completion rate for each of the service areas (SAs) in which we operate. To meet these requirements, Centene takes a proactive stance to ascertain and resolve potential encounter data integrity issues. For example, Centene's EBO unit runs a weekly encounter reconciliation report utilizing internal encounter data to identify potential completeness issues and also performs a monthly comparison of encounter data to our financial lag data.

To complete our weekly monitoring and reconciliation process, Centene's EBO unit utilizes a standard Encounter Pro report that identifies current encounter status records and groups them into categories by month of payment so we can assess whether all appropriate encounters are being captured and subsequently submitted. This process helps us ensure all claims are being submitted and processed by our state client as expected. Through this analysis, we can identify records that do not conform to the normal processing schedule and conduct focused drill-down analyses to identify and resolve the root cause and also repair any records that may have been rejected as a result of that issue.

To compare encounter data to our financial lag, we utilize monthly lag data and compare "claim-to-claim" and "dollar-to-dollar" with those claims maintained in our Encounter Pro system. If any gap or difference is identified, encounter resources conduct a focused analysis to identify the root cause and resolve the discrepancy. This process has helped Centene overcome previous obstacles in submitting encounter data to HHSC. For example, when Centene implemented our encounter-specific Encounter Pro system, we experienced challenges in tracking encounter submission status codes. Discrepancies were identified via our monthly reconciliation processes and were subsequently resolved. They key, however, was that we were able to leverage this experience and further scrutinize historical encounter status codes on future Encounter Pro implementation, thereby mitigating future risks. As a result, we are currently able to match our data with financial information and have a fundamental understanding of any non-material discrepancy that may exist (i.e., due to inherent data timing).

Although our goal is to always submit encounters with 100% accuracy, timeliness, and completeness, we have the requisite experience to understand that issues can and do arise and we position ourselves, through lessons learned in previous implementations and operations, to quickly identify and resolve issues to the benefit of all current and future clients. Due to our proactive stance in managing and reconciling encounter data, Superior has been able to meet or exceed the 98% completion rate for all of our SAs on a recurring basis.

Example #2 – Georgia. Centene has processed and submitted encounters for our Peach State Health Plan (Peach State) in Georgia for five years. In Georgia, the Department of Community Health (DCH) performs a monthly reconciliation between the Cash Disbursement Journal (CDJ) and submitted encounters with a 99% completeness goal over a rolling 24-month paid claims time period. To meet this goal, Centene's EBO unit routinely performs a weekly self-monitoring process in which we calculate our internal reconciliation rate and shares that information with Peach State for validation. Our internal reconciliation rate compares the CDJ data to what we have stored and maintained in Encounter Pro and, as with Texas affiliate, we compare claim-to-claim and dollar-to-dollar by paid month. We also routinely monitor our capitated providers through the processes described above.

Our Centene and Peach State encounter resources work closely with our state client, DCH, and their intermediaries to understand all aspects of the reconciliation process and how our encounter data is

ultimately utilized. As a result, we have learned from operational experience in submitting encounters nationwide, the importance of establishing and maintaining a close working partnership with our state clients and their fiscal intermediaries. We look forward to establishing a similar partnership and working collaboratively with DHH and their fiscal intermediary to ensure we thoroughly understand their encounter submission requirements and reconciliation calculations. We commit to meeting DHH requirements and will initiate an internal monitoring process to proactively review and resolve encounter issues that may impact our timely, accurate, and completeness rates.

Example #3- Indiana. Centene has processed and submitted encounters for our Managed Health Services (MHS) in Indiana for 17 years. MHS is evaluated on a monthly basis for encounter acceptance rates and quarterly for completeness. Similar to our other examples highlighted above, MHS has taken a proactive approach to monitoring both of these metrics. Analysis is completed weekly to understand the acceptance rates received on the encounter submissions that week. If at any time the monthly acceptance rate is at risk, the encounter resources work together to quickly identify and resolve the issues so we maintain an acceptable monthly encounter acceptance rate. On a quarterly basis, the state conducts a reconciliation of paid claim volumes to accepted encounter volumes. EBO proactively manages our reconciliation rate on a monthly basis in conjunction with our finance team. Doing so has resulted in achieving and *exceeding* the required reconciliation rate consistently.

Ability to Meet or Exceed DHH Requirements

We have reviewed in detail the encounter submission and related reporting requirements in the RFP, Section 17 (including, in particular, Section 17.5.4), Sections 18.4 and 18.8, and the CCN-P Systems Companion Guide. Centene and LHC have the capability to meet or exceed these requirements. While the table below (***DHH Requirements by Example Market***) does not illustrate the full breadth of our encounter experience across all of our markets, it does clearly illustrate our experience in meeting each of the DHH requirements in the examples cited above. We look forward to working with DHH to share our experience, best practices, and *lessons learned* (see below) to implement an efficient and effective program focused on delivering timely encounter data of the highest quality.

DHH Requirements by Example Market

Requirement		Will Meet in LHC	Currently Meet in Example Markets			Comments
			Texas	Georgia	Indiana	
17.5.4.	Encounter Data.	**X**	**X**	**X**	**X**	
17.5.4.1.	Ability to transmit to and receive encounter data from the DHH FI's system.	**X**	**X**	**X**	**X**	
17.5.4.2.	Readiness to submit encounter data to the FI in a provider-to-payer-to-payer COB format within sixty (60) days of operation.	**X**	**X**	**N/A**	**X**	Multiple market expansions and implementations in both Texas and Indiana were accomplished in <60 days.
17.5.4.3.	Provision of complete and accurate encounter data.	**X**	**X**	**X**	**X**	
17.5.4.4.	Ability to update CPT/HCPCS, ICD-9-CM, and other codes based on HIPAA standards.	**X**	**X**	**X**	**X**	
17.5.4.5.	Mandatory utilization of ICD-9-CM and other national coding standards and HCPCS Level II and Category II CPT codes.	**X**	**X**	**X**	**X**	

Requirement		Will Meet in LHC	Currently Meet in Example Markets			Comments
			Texas	Georgia	Indiana	
17.5.4.6.	Capability to convert all claims from hard copy paper claims to electronic encounter data for submission to DHH.	**X**	**X**	**X**	**X**	
17.5.4.7.	Utilization of a DHH-approved version of the claims processing system to identify valid and invalid encounter records.	**X**	**X**	**X**	**X**	
17.5.4.8.	Determining appropriate encounter edits, setting encounter edits to "pay" or "deny". Determining “repairable” or “non-repairable” encounter denial codes.	**X**	**X**	**X**	**X**	
17.5.4.9.	Denial reasons of particular interest: Denied for Medical Necessity, Member has other insurance, Prior authorization not on file, Claim submitted after filing deadline, Service not covered by CCN.	**X**	**X**	**X**	**X**	
17.5.4.10	Knowledge and utilization of the DHH provider billing manuals and claims data elements. Retention of all required data elements in claims history.	**X**	**X**	**X**	**X**	
17.5.4.11	Addressing ninety percent (90%) of reported repairable errors within thirty (30) calendar days and ninety-nine percent (99%) within sixty (60) calendar days or within a negotiated timeframe approved by DHH.	**X**	**X***			* Historically, when initial rejects were higher, we met this requirement, although TX, IN, and GA now use a metric based on overall reconciliation to our financial statements, in recognition of our +99.5% initial submission rate. Since very few records miss the reconcile deadline, and are by definition the most problematic encounters requiring extensive investigation, these states recognize that requiring a % TAT for the remaining small fraction of encounters results in an unrepresentative measure of our performance.

Requirement		Will Meet in LHC	Currently Meet in Example Markets			Comments
			Texas	Georgia	Indiana	
17.5.4.12	Submitting ninety-five (95%) of encounter data at least monthly due no later than the twenty-fifth (25th) calendar day of the month in which they were processed and approved/paid.	**X**	**X**	**N/A**	**N/A**	
17.5.4.13	Incorporating all encounter data from a contractor in a single file - multiple files allowed in a week.	**X**	**X***	**X***	**X***	* Normal practice is to separate HCFA and UB claims, but can (and have) accommodated, either in one file, or separating by day, based on DHH preference.
17.5.4.14	Ensuring that files contain settled claims and claim adjustments or voids.	**X**	**X**	**X**	**X**	
17.5.4.15	Ensuring that the levels of detail are equivalent for encounters from providers with capitation arrangement and for fee-for-service claims.	**X**	**X**	**X**	**X**	
17.5.4.16	Adherence to federal and/or department payment rules in the definition and treatment of certain data elements (e.g. units of service that are a standard field in the encounter data submissions).	**X**	**X**	**X**	**X**	
17.5.4.17	Submission of encounter records such that payment for discrete services submitted in a single claim can be ascertained in accordance with the CCNs applicable reimbursement methodology.	**X**	**X**	**X**	**X**	
18.4.1	Compliance with the required format provided by DHH	**X**	**X**	**X**	**X**	
18.4.2	Providing notice of changes to subcontractors (upon the 150 days' written notice of DHH Encounter Data Transaction requirements)	**X**	**X**	**X**	**X**	
18.8	Weekly encounter submission file	**X**	**X**	**X**	**X**	

Lessons Learned

Over the more than 27 years Centene has submitted encounter data on behalf of our affiliate health plans, changes in submission formats, methods, and protocols have been driven by many different sources, including federal and state regulations, state-specific requirements, and improving business processes. Centene has consistently managed these processes and improved upon them based on lessons learned across our health plans. A key aspect of our entire operation, and the lessons we learn, is that we *exclusively* work with public sector (e.g., Medicaid) providers in all of our health plans. Examples of lessons learned in current operations or previous implementations include:

Standardization of System Tools. In previous years, Centene utilized a proprietary system to automate the submission, correction, and maintenance of encounter data to our state clients. Over time, the tool became cumbersome to manage and led to instances in which the quality of our encounter data was no longer consistent enough to warrant continued usage. Rather than continue to struggle with an antiquated system that became more disparate for each of our health plans, we decided to invest the time and resources to identify, implement, and operate a best-of-breed encounter management tool designed specifically for the submission of encounter data for the Medicaid industry.

As a result of this decision, we have implemented Encounter Pro as a standard application for all of our health plans. In that time, we have seen a dramatic increase in the efficiency of our encounter submissions. The tool's design provides us with the flexibility to meet changing or new state requirements while maintaining a fundamentally consistent, overall architecture to leverage commonalities and consistencies. Through this effort, we have learned the value of utilizing a standardized, yet flexible, tool to submit encounters across our health plans and the importance of committing the necessary resources, both time and people, to implement and use it in an effective manner. We continue to look for ways to identify and embrace new system capabilities to further enhance our ability to submit "best-in-class" encounter data for all of our state clients.

Leveraging Claim Edits Early in the Adjudication Process. Based on continual and ongoing analysis of encounter data errors identified prior to state submission, we have learned that many of pre-submission edits (i.e., those edits that are designed to mimic the state MMIS edits to prevent submission of invalid encounter data) can be moved further to the front end of the claims-encounter life cycle, including to the provider claim preparation stage.

As a result, over the past two years, Centene has introduced technology and implemented changes that have improved performance in both claims adjudication and encounter acceptance rates. Centene is currently refining the claims payment and encounter submission process as we continue to monitor and analyze our encounter submissions. Currently, Centene is moving edits from within the Encounter Pro pre-submission edit process to the front end of our claims adjudication process. Based on analyses conducted in other states, Centene has already identified and incorporated several new edits into AMISYS Advance and we anticipate many further edits will be integrated as part of our continual quality improvement process.

For example, in Texas we manage providers in approximately 170 rural counties, including atypical providers providing wraparound services. We have learned to effectively work closely with these providers since many are not familiar with the data and operational aspects of submitting "clean" claims. As we move edits to the front end of the claim-encounter life cycle, we understand how important it is to engage the providers and customize our provider training orientations and curricula for specific Medicaid provider types. In other words, we may provide one type of curricula for FQHCs and another for traditional primary care providers; we may develop one type of training program and support for rural providers and targeted web-based tools for atypical providers.

New Implementation Testing. Having performed a number of new health plan implementations, we have learned the value of integrating encounter submission and data exchange testing as part of an overall suite of end-to-end testing with our new state clients and providers. To be more specific, we do eligibility

testing then move into claims processing testing, using the same data from both, we begin our encounter testing, validating our encounter processes early. We continue testing with our state partners once we begin to receive production claims, as we have learned that regional claim submission patterns can impact early results of encounter submissions. We encourage and support direct partner testing between each of our health plans and our state partners as part of the new implementation, and with any changes made to the encounter process or format.

Integrated Encounter Team. Our experience has shown us that the right cross-functional team has been critical in creating a successful overall encounter submission, tracking, and correction process. We created an integrated team of encounter specialists, claim experts, and IT analysts and programmers to ensure the appropriate focus is given to the priorities that encounter submissions create. This team meets regularly with each health plan, our state partners, finance, and claims to proactively address any upcoming changes or process improvement initiatives, which leads to a more seamless integration of new features for all parties involved.

Policies and Procedures Supporting State Encounter Data. Centene and LHC will maintain a comprehensive set of policies and procedures (P&Ps) to manage the encounter submission process. All P&Ps will be designed specifically for LHC programs and will be updated to reflect additional programs as necessary. Due to the length of the documents, all P&Ps will be made available to DHH upon request in electronic format or via onsite visits, as may be appropriate. P&Ps are easily accessible to all responsible parties involved with encounter processing. Additional P&Ps will also be in place for claims-oriented activities that may impact encounter submissions. Our claims and encounter operation staff are required to follow established protocols to ensure a consistent process. All P&Ps will be updated regularly as necessary to accommodate changes in health plan, DHH, or federal guidelines.

Meeting Current and Future Mandates

As a publicly held entity subject to federal SOX regulations, Centene has continuously refined our processes for the systematic and early identification of federal mandates germane to our health plans. To ensure the coordinated, phased transitioning of mandates to meet compliance effective dates, we expeditiously assess the impact of mandates on our IT infrastructure and operations, develop and implement remediation plans resulting from those assessments, and formulate and execute Level I (internal) and Level II (external) testing plans, working collaboratively with our state clients and providers. Centene and LHC will conform to future federal and DHH standards required for encounter data exchanges within 120 calendar days prior to the effective date as required by DHH and/or CMS.

LHC’s Compliance Department and Centene's Legal and IT Security Departments will work closely together to monitor relevant announced federal mandates *at large* (e.g. published in the Federal Register), IT mandates related to security, and federal mandates relevant to our DHH contract and state mandates.

Centene began HIPAA 5010 planning activities in 2008 under the direction of our Manager of EDI Services. We completed our internal gap assessment in early 2010 and implemented the HIPAA 5010 compliant version of our core eligibility and claims processing subsystems (AMISYS Advance Release 4) in Q4 of 2009. We completed Level I (internal) HIPAA 5010 testing in early 2011 and we are beginning Level 2 (external) HIPAA 5010 testing during Q2 of 2011 with providers who are ready to test with us. **We remain solidly on target to meet the HIPAA 5010 mandate and deadline, as are our subcontractors affected by the 5010 rule.**

In addition, in 2010, we instituted our enterprise level ICD-10 compliance initiative led by our Chief Technology Officer (CTO), who reports to our Executive ICD-10 Steering Committee. The Committee is comprised of business leadership from all departments affected by the US Department of Health and Human Services Final Rule modifying 45 CFR Part 162 to mandate the use of ICD-10 CM and ICD-10 PCS (ICD-10) codesets in HIPAA transactions effective October 1, 2013. In late 2012 or early 2013, we will upgrade our AMISYS Advance system to its ICD-10 compliant version, along with requisite upgrades to our TruCare health services management platform; Centelligence™ reporting and decision

support system; and MDE Encounter system. We anticipate completing Level 1 testing by the end of 2012, and Level 2 testing by mid-2013.

Managing Subcontractor Encounter Submissions

LHC will manage encounter-related contracts and service level agreements with our subcontractors via our established delegation oversight process in close collaboration with Centene. Our vendor contracts call for accurate, complete, and timely encounter submissions to our EBO, where we oversee all aspects of that subcontractor's encounter operations. Our subcontractors are required to comply with the same encounter submission requirements as LHC. In the event a subcontractor does not comply with encounter requirements, we will activate our corrective action processes, which can include monetary penalties, for non-compliance.

Question R.6

Receiving, Processing, and Updating Eligibility/Enrollment, Provider Data, and Encounter Data to and from DHH and Agents

R.6 Describe your ability to receive, process, and update eligibility/enrollment, provider data, and encounter data to and from the Department and its agents. In your response:

- Explain whether and how your systems meet (or exceed) each of these requirements.
- Cite at least three currently-live instances where you are successfully receiving, processing and updating eligibility/enrollment data in accordance with DHH coding, data exchange format and transmission standards and specifications or similar standards and specifications. In elaborating on these instances, address all of the requirements in Sections 16 and 17, and CCN-P Systems Companion Guide. Also, explain how that experience will apply to the Louisiana Medicaid CCN Program.
- If you are not able at present to meet a particular requirement contained in the aforementioned sections, identify the applicable requirement and discuss the effort and time you will need to meet said requirement.
- Identify challenges and "lessons learned" from implementation in other states and describe how you will apply these lessons to this contract.

National Experience Exchanging Data with States and Their Intermediaries

Centene Corporation (Centene) will operate and manage the data exchange and processing requirements for Louisiana Healthcare Connections (LHC). Centene has over 27 years of experience processing two-way exchanges (data to/from our state clients) of eligibility, enrollment, provider and encounter data for public sector health care programs in 11 states, and on behalf of over 1.6 million members and a nationwide network of over 100,000 physicians, medical homes, specialists, hospitals, behavioral health clinicians, and ancillary providers. Today, we support all HIPAA transaction formats, including those pertaining to eligibility/enrollment and encounter data exchanges with our state clients or their intermediaries:

- The HIPAA 834 - both for receiving enrollment and eligibility data and for issuing demographic member updates back to our state clients or their intermediaries
- The HIPAA 837 for encounter submissions
- The HIPAA 835 for encounter adjudication result reporting (we will make a request in writing to DHH in advance of encounter testing in order to obtain 835 support)
- We also support the ANSI ASC X12 277U (Unsolicited 277), should DHH decide to implement this HIPAA based encounter status transaction
- Please note that we also support the HIPAA 820 Premium Payment transaction, and will implement the use of the 820 per Question #227 in the document from DHH: CCN PREPAID RFP QUESTIONS AND ANSWERS, dated 5/23/2011.

For provider data exchanges, we support state or state Fiscal Intermediary (FI) proprietary formats and we both send and receive provider data as frequently as daily, depending on our state client needs.

We have reviewed in detail all requirements in Sections 16 and 17 of the RFP, as well as the CCN-P Systems Guide included with the RFP and we will meet or exceed these requirements, and in fact, do we support these requirements today for Centene's health plans in other states. ***In addition to the discussion below***, please refer to R.7 for details on how we meet each requirement in Section 16 of the RFP, and refer to R.2 and R.5 as well as Q.1, Q.2, and Q.3 for details on how we meet or exceed each requirement in Section 17 of the RFP.

Protecting Data in Our Exchanges with the State

We employ HIPAA compliant administrative, technical and physical security safeguards under the guidance of LHC's and Centene's Compliance Officers, General Counsel, and our Chief Information

Security Officer (CISO), to meet or exceed all HIPAA Privacy and Security requirements. Please see R.7 and R.16 for more information on our controls for availability, data integrity, and confidentiality.

Receiving, Processing and Updating Data

As part of our normal business support capabilities, Centene successfully receives, processes, acknowledges, updates, and transmits formatted data to and from our integrated Management Information System (MIS) from a wide variety of Trading Partners (state agencies, fiscal intermediaries, enrollment brokers, claims clearinghouses, medical test labs, providers, etc.) through all industry standard methods (VPN, Secure FTP, https, etc.).

Eligibility and Enrollment Data. Today we process inbound HIPAA 834 transactions on a daily, semi-monthly, and monthly basis from our state clients or their Fiscal Intermediaries (FI) or Enrollment Broker (EB), and in accordance with companion guide specifications per state, FI or EB. We can accommodate any 834 transaction schedules desired by DHH, including the daily update and weekly and monthly 834 membership reconciliation processes called for in the RFP. We receive and transmit HIPAA 834 transaction files via our secure file exchange management system, Coviant Diplomat (Coviant). Our TIDAL job scheduling software manages member load processes for overall process integrity. Inbound 834 files are automatically processed through our EDIFECS EDI system for HIPAA 4010A and 5010 compliance validation and translation. EDIFECS, in conjunction with our TIBCO middleware also edits for duplicate member records, date criteria validity, field data integrity, and valid date spans. Any member records that trigger edits default into an Exception Report where they are systematically corrected using data correction routines prior to subsequent processing.

We will process HIPAA 834 files from DHH's EB through our EDIFECS system using HIPAA 5010 compliance checks (for go-live on 1/1/12), and load this data into our Member Relationship Management (MRM) member data management system through Add, Delete, and Modify transactions with accurate begin and end dates - all within 24 hours of receiving the HIPAA 834 from DHH's EB. In fact, this 24 hour processing turnaround time has and remains our normal mode of operations across our health plans. MRM is our "system of record" and master data store for "all things member" related - including demographic (member identifiers, address and contact information, confirmed or potential family linkages, special needs, and numerous other attributes), administrative, member preferences (e.g. communication options such as e-mail, phone, mail) - along with history for these attributes.

MRM also houses our master member index (MMI) - an internal global member identifier, similar to a master patient index, to tie together alternate or historic member identifiers. MRM allows us to systematically link information about the member across that member's relationships with us or DHH, or prior health coverage spans (where we have such history). Once member data populates MRM, it is systematically promulgated to our other systems including (via TIBCO middleware) AMISYS Advance, our core claims processing system; our TruCare integrated health services management platform; our MACESS EXP paper scanning and MACESS FormWorks Optical Character Recognition (OCR) system; our Automatic Work Distributor (AWD) claims workflow engine; and our Enterprise Data Warehouse (EDW) data integration engine via our Informatica near real-time Extract, Transport, and Load (ETL) middleware. Through EDW, we also make member eligibility data securely accessible to our providers online via our Provider Portal. We securely transmit member eligibility data to any subcontractors we are working with for a particular plan. For LHC, we will be sending this eligibility data to OptiCare Managed Vision® (OptiCare) – LHCs affiliated vision benefits subsidiary and subcontractor. Our MRM can maintain LHC's member historical data indefinitely, subject to DHH retention requirements.

Based on Centene's experiences with our affiliate health plans, below are some example scenarios where we would work with DHH or the DHH Enrollment Broker to address specific enrollment and eligibility file issues (we will, of course, work out specifics in consultation with DHH and the Enrollment Broker):

Identifying Duplicate Enrollment/Eligiblity Records. During the initial load process referenced above, using EDIFECS and TIBCO, we identify duplicate eligibility and enrollment records in a particular

HIPAA 834 load file. These duplicate records are output on a load report and are worked by our Eligibility Specialists. If we confirm that the records are duplicates, we will report this fact in the manner prescribed by DHH.

Member on DHH file, not Active with LHC. The Eligibility Specialist will work with DHH and DHH's Enrollment Broker to validate member additions if not flagged as such on the DHH file prior to adding to the Membership Subsystem.

Member Information Inconsistent with DHH File. (Date of birth, category of aid, address, phone number). The Eligibility Specialist will work with DHH and have Member Services staff contact the member to ask that they update address and phone changes with the appropriate county office.

Selected PCP on DHH File not Assigned to Member. The Eligibility Specialist will investigate the reason for error (i.e. PCP not accepting new members) and work with Member Services staff to ensure the member is assigned a medical home.

Member not Reported on DHH File. The Eligibility Specialist will work with DHH to confirm eligibility or termination. For newborns admitted to the NICU, the assigned Case Manager will work with the Eligibility Specialist until that member is added to the DHH eligibility file. Our Integrated Care Teams will work with the Eligibility Specialist when a member is identified as requiring a service, verified by the state verification system as eligible but not present on the enrollment file, to resolve membership conflicts.

Multiple Identifiers for Same Person. When we load processed member records into MDS (MDS is our Member Demographics System - MRM's central relational database), we identify any potential duplicate members "at the person level" - meaning the system looks for members (perhaps with different identifiers) who potentially may be the same person. Our Eligibility Specialists work these records as well and once we confirm with the state the correct identifier and demographics for a member, MDS distributes that information to all our internal systems so that we systematically link claim records, clinical case management records, member service records, etc. to the corrected member identifier.

For example, should our Eligibilty Specialist identify two records with two different eligibility spans, and two different Medicaid ID numbers, but where it is possible that the two records apply to the same person (e.g. name, address, date of birth), our Eligibility Specialist will validate this fact by working with the EB and other records we may have on the member, and possibly contact the member directly to confirm that the multiple records are - in fact - one person. If we confirm that the records are for one person, we link those records to our master member index for that member in MDS, allowing us to consolidate history (e.g. claims) at the person level.

Sharing Member Data. Today, we support the ability to transmit member demographic changes, such as changes in address or telephone number, to any of our state clients who request this information. We support HIPAA 834 formats for this purpose; and can also accommodate a state, Fiscal Intermediary or Enrollment Broker proprietary format as may be specified by DHH. To capture member "self reported" changes, we efficiently capture member demographic changes via our MemberConnect contact relationship management (CRM) system. Our Member Services Representatives (MSR's) can enter new member contact information in fields that do not overwrite the information we have received from DHH, their Fiscal Intermediary or Enrollment Broker so that we can maintain data integrity - keeping data issued to us by the state separate from self-reported information from the member. We then extract and send this updated data to the state or state designated entity. Members can also provide demographic changes to us via our secure web based Member Portal, and we can integrate this information with any updates recorded through MemberConnect into one consolidated member information change file for use by DHH or the DHH's Fiscal Intermediary or Enrollment Broker.

For additional information on our eligibility and enrollment data - including how we utilize this information across our MIS - please see our response to R.7 and R.11.

Provider Data. LHC and Centene will use our innovative, integrated Provider Relationship Management system (PRM) to maintain contracting and provider data and ensure the integrity of provider data through PRM's systematic controls, data entry tools and interfaces.

At the heart of PRM is our *Portico* provider data management system which integrates provider related information across our other MIS components needing to use provider data. Portico provides a single repository for all provider functions (in line with our Master Data Management (MDM) architecture), including: prospecting and recruiting; provider enrollment; credentialing; financial affiliation configuration; data management; and provider directory management.

Provider Data Validation. As part of the provider contracting process, LHC will enter demographic, specialty, location, affiliation and related information in our PRM system, including provider name, group name, W-9's containing the legal entity name and tax identification number (TIN), taxonomy code, address, effective date, end date, primary specialty, Medicaid identification (ID) number, payment information, National Provider Identifier (NPI), and licensing/credentialing information. Prior to provider enrollment, LHC and Centene will also conduct federal and state mandated background checks on each provider and we will require our providers to do the same for all their employees on at least an annual basis. If an LHC member obtains services from an out-of-network provider who is not housed in our system, the provider's data will be added to PRM as a *non-participating* (non-par) provider. At a minimum, we require the following for non-pars: TIN, NPI, taxonomy code, and ZIP+4.

Our provider data management processes support HIPAA's National Provider Identifier (NPI) and Atypical Provider Identifier (API) IDs and we also regularly perform ongoing reconciliation with CMS' NPPES (National Plan and Provider Enumeration System) and will develop similar reconciliation processes with DHH-specific files to improve the collection, confirmation, and reconciliation of provider data.

Enhancing Provider Data Quality. In 2011, we are augmenting our provider data management operations by integrating PRM with data and interface services from Enclarity, Inc. Enclarity is the nation's leading commercial provider data supplier, a recognized expert in sourcing, maintaining, and validating provider demographic, specialty, licensure, and sanction information. Through a singular focus on "all things provider," Enclarity maintains a storehouse of correct, current, and comprehensive information by continually reviewing the most trusted sources of data in the industry, a "universe" of provider information representing over 140 million records: all synchronized and normalized in Enclarity's Master Provider Referential Database (MPRD). Through both "on demand" real time and scheduled batch provider data interfaces with our PRM, Enclarity enables LHC to recruit, contract, administer, and manage the ongoing quality of our CCN-P provider network with enhanced accuracy and responsiveness. For example, during the credentialing process, PDM Coordinators will cross-reference attested provider data obtained during credentialing with Enclarity's secure online database search tool (the database includes out-of-network providers) and will investigate any discrepancies between attested provider information and Enclarity data.

Enclarity also integrates with our PRM in "real time"- with several significant benefits. For example, should our Provider Relations or other LHC staff identify a particular provider that we would like to recruit and contract with (e.g. to offer additional specialty service capacity in a geographic area); our staff can retrieve the latest demographic, licensure, sanction, and sub-specialty information on that provider, simply by inquiring directly from our Portico system, which interfaces securely, in *real time*, with Enclarity. This "on demand" feature greatly strengthens our ability to quickly fortify our network wherever we need to, whenever we need to.

Finally, Enclarity ensures on a regular basis that the provider data we house in PRM is accurate across all provider informational dimensions. Every quarter, Enclarity electronically sends us a validation file for

all records housed in PRM's Portico database. Portico can then update any information from this Enclarity "synchronization file." Per DHH requirements, we will also reflect these updates in the Provider Registry file we send to DHH's Fiscal Intermediary, per the CCN-P Systems Guide, Appendix G.

Provider Data Integration in Our MIS. Centene has created automated electronic interfaces between PRM and our other core systems for tighter data integration between business functions, including: AMISYS Advance for claims processing and payment; TruCare, our utilization and clinical care management application; MDE Xpress Encounter Pro (Encounter Pro) for encounter management; ProviderConnect (the Microsoft Dynamics Customer Relationship Management (CRM) component of PRM); and finally to our Enterprise Data Warehouse (EDW) for provider profiling and reporting purposes. Provider data is fully audited and reconciled in Portico before being promulgated to these other systems ensuring the consistency and integrity of the data throughout our MIS and operations**.**

Maintaining and Exchanging Provider Data. We will transmit provider registry data (at DHH's direction and per Appendix G of the CCN-P System Companion Guide) to allow DHH's FI to validate provider information in our encounter submissions. We will also work with (at DHH's direction) the FI and DHH's Enrollment Broker (EB) to ensure that we supply the correct provider data on an ongoing basis to the EB for enrollment related applications - most notably: member PCP selection.

We will utilize information published via www.lamedicaid.com or any other DHH-specified resource to utilize Louisiana Medicaid data including, but not limited to: provider types, specialty codes and sub-specialty codes. LHC and Centene will develop appropriate processes to coordinate provider enrollment using the same code sets as DHH and the Enrollment Broker.

Please refer to the table below for a description of how PRM, including Portico and our other PRM modules, support the requirements of Section 16.9.4.

Requirement	How We Support The Requirement
Audit trail and history of changes made to the master provider data	Portico supports full audit trail and history tracking by electronically stamping the effective date of provider data transactions; enabling full historic audit trail support.
Automated interfaces with all licensing and medical boards	Automated interfaces are supported via Enclarity's provider data service.
Automated alerts when provider licenses are nearing expiration	As part of our PRM, Portico maintains licensure dates and alerts our Provider Relations staff when a provider's licensure is nearing expiration, and via our ProviderConnect provider services application, alerts our Provider Service Representatives (PSR) for potential follow/up or to remind the provider when they contact our provider services desk.
Retention of NPI requirements	The Portico data management subsystem of our PRM fully supports NPI capture, storage, and administration.
System generated letters to providers when their licenses are nearing expiration	As part of our PRM, Portico maintains licensure dates, and leveraging these dates, we will deploy a monthly process whereby providers nearing a licensure expiration date will be notified via the ProviderReach integrated outbound provider campaign module of our PRM. ProviderReach will notify providers nearing licensure expiration via

Requirement	How We Support The Requirement
	automated e-mail or letter or Predictive Auto Dialer (PAD) notification using our Avaya Voice Portal. The communication mode we use will depend on the provider's preference.
Linkages of individual providers to groups	Many-to- many linkages and affiliations between individual providers and provider groups are fully supported in Portico.
Credentialing information	We support a very wide variety of credentialing information in Portico, including support for all credentials obtained through primary source verification.
Provider office hours	Fully supported in Portico.
Provider languages spoken	Fully supported in Portico.

In addition to the above, our PRM system supports provider prospecting and recruitment processes, support for multiple provider locations and location contacts, and support for multiple individual level provider service locations.

Encounter Data. LHC and Centene view claims data as a fundamental and base source data for the encounter data we will eventually submit to DHH or DHH's FI. We focus our efforts on obtaining accurate, high quality data from our providers to help ensure our encounter data will meet all requirements such as those specified in the RFP and the CCN-P Systems Companion Guide.

We also see the claims process as a critical data gathering aspect of our operation, since it supports our quality and utilization monitoring efforts, and results in *supplying DHH with accurate, timely, and complete encounter information.* At each stage of the process, beginning when the provider submits a claim to LHC, until we in turn submit the encounter to DHH, we have an infrastructure in place today comprised of people, technology, business processes, and system controls to ensure the highest quality encounter submissions to DHH. For specific detail regarding our encounter submission process, please reference our response to Question R.5 where we discuss our encounter resources, business processes and technologies. Also please reference our response to Question R.2 and R.4 for additional information on the data integrity controls we use to ensure encounter data quality.

Ensuring Quality in EDI Submissions. Today, more than 85% of claims submitted to us are submitted as HIPAA EDI transactions and we have a long-standing and large investment in processes and controls to ensure the systematic and "up front" validation of HIPAA claims. We validate all electronically submitted claims data, including the HIPAA 837 Professional (837P) and 837 Institutional (837I) claims transactions, using EDIFECS XEngine (XEngine) software. XEngine supports HIPAA compliance standards as defined by the Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP), and allows us to configure edits and testing scenarios, for our specific business rules. XEngine validates data against X12 syntax and rules for data structure; tests to ensure conditional rules requiring secondary fields are completed accurately and completely; and ensures all data is in compliance with our HIPAA Companion Guides (we will review LHC's HIPAA Companion Guides with DHH and/or DHH's FI during implementation activities). These upfront edits not only ensure that transactions are compliant with Federal mandates and DHH rules, but also allow us to recognize and immediately communicate to providers and Trading Partners (e.g. clearinghouses) any problematic claim submissions in the earliest stage of the process, through our transmission of ANSI TA1 and ANSI 997 Functional Acknowledgements (FA), and the ANSI 999 FA for HIPAA 5010 transactions, which we will support beginning 1/1/2012.

We have recently offered providers the option of submitting HIPAA EDI claims to us *directly* (in lieu of submission via a clearinghouse), and we are enhancing our EDI support for directly submitting providers

or other Trading Partners (e.g. billing agents) with our introduction of EDIFECS Ramp Manager in the second half of 2011. Ramp Manager validates against our transaction rules and provides immediate feedback on any errors that the provider or other Trading Partner can then correct. Our overall objectives with Ramp Manager are: i) to further assist providers in their efforts to capitalize on the speed and efficiencies offered through EDI processes; and ii) for Centene and LHC to obtain the highest quality data possible for health plan operations and submission to DHH.

We currently validate EDI claims submitted to us to SNIP Level 4 (Situational Compliance) and are beginning to test Level 5 (Codeset Compliance), and have the capability of enforcing up to a HIPAA Level 7 leveraging EDIFECS XEngine and Ramp Manager tools, and 2011 we will increase the number of front end EDI validation edits we make to include code set and code combinations. We will work closely with DHH as we define the timeline and key milestones as we move to Level 5 (or higher), and we will support this transition through our provider education programs. In our experience, it is critical to increase compliance levels *smoothly* and in *synch* with the EDI capabilities in the provider community - balancing the need for providers to file claims and have them accepted by LHC swiftly with the need to collect "clean data" for subsequent state reporting.

Ensuring Data Quality From Paper Claims. Approximately 90 percent of all paper claims we receive can be indexed and converted into machine readable data through the use of Optical Character Recognition (OCR). We use MACESS EXP Form Works Optical Character Recognition (OCR) software to greatly enhance the accuracy of machine readable data from the paper and fax claims we receive from providers. We encourage, train, and support our provider to move to electronic claims submission; or to use standard "OCR friendly" red ink paper claim forms with typed or clearly written data if a provider must use paper. Once we have captured the claims data into machine readable form, that "paper claim" data is ***treated identically*** to EDI claims we receive, or claims that our providers enter directly via our Provider Portal using our DDE online claim entry application.

Identical Validation and Edits for Electronic and Paper Claims. All claims data we receive (paper or electronic) is loaded into pre-adjudication tables managed by our *TIBCO BusinessWorks*™ (BusinessWorks) for validation of member and provider fields. For example, BusinessWorks compares the member data we have on file in our Member Relationship Management (MRM: our enterprise master data management system for "all data member related") with member information on the submitted claim on the claim. If a claim transaction is rejected for any of the specific reasons configured in BusinessWorks, a notification is automatically provided to the EDI Trading Partner or provider outlining the reason for the claim rejection. The types of edits performed in BusinessWorks include (among a number of other data quality checks):

- Member Validation– confirms presence of member record in our systems.
- Provider Validation - confirms presence of provider record in our systems.
- Validate Dates of Service – confirms that the claim date of service is valid and does not contain a future date.
- Diagnosis Code Validation/ICD9 tables – confirms the presence and accuracy of ICD9 codes.

Adjudication in AMISYS Advance. Claims data that passes all HIPAA compliance, codeset edits, and data validation is then systematically loaded into our AMISYS Advance claims processing system for adjudication, including application of health plan rules (covered services), verification of member eligibility for the dates of service on the claim, matching (if applicable) of claim to service authorizations, application of appropriate fee schedule based on the provider information on the claim, edit checks for third party liability, and several other automated edits and processes, until the claim is finalized to a paid or denied status. Please see Section Q, Question Q.1 for more information for details on our claims adjudication process, including our real time automated process to handle any claim pends.

Encounter Record Preparation. Once AMISYS Advance adjudicates claims to a finalized status, our MDE Xpress Encounter Pro (Encounter Pro) encounter workflow system will extract, prepare and submit

the data as encounters to DHH, via EDW and EDIFECS (for application of HIPAA compliance rules of our outbound HIPAA 837 encounter data). MDE (the creator and supplier of Xpress Encounter Pro) has a proven track record within the Medicaid industry of providing "best of breed" submission and correction functionality to meet encounter submission guidelines as required by all our state partners. We will configure Encounter Pro to submit encounter data that complies with all DHH standards for electronic file submission, standard HIPAA file format (specifically including ANSI X12N HIPAA 837 provider-to-payer-to-payer COB transaction format), file size, submission frequency, and submission method as required by DHH. Our encounters capture the same line item detail regardless of the claim type, disposition (e.g., paid or denied), third party liability indicators or capitation arrangements. We include all rendered services, original and adjusted claims, application of retroactive fee or member changes, etc., in a *single* encounter file as appropriate for the claim type, and we can include encounters we receive from OptiCare Managed Vision® (OptiCare), LHCs affiliated vision benefits subsidiary and subcontractor, for submission to DHH's FI. We also adhere to NCQA, AMA coding, UB-04 editor, NCCI, and DHH standards regarding the definition and treatment of certain data elements captured on claims, use of standard codes (including CPT Category I and II , HCPCS Level II and ICD-9-CM), counting methods, units, etc.

Centene will retain all data elements in our claims history necessary for creating encounters in compliance with DHH and the Fiscal Intermediary requirements.

Specific functionality provided by Encounter Pro includes, but is not limited to:

- Support of DHH-specific business rules to “scrub” data prior to submission
- Automation of LHC defined actions, in conformance with DHH guidelines, to correct *repairable* encounters
- Linkage to our base claim database, outbound encounters, and inbound acceptance reports to facilitate comprehensive encounter reconciliation efforts - from provider submission, through claims processing, to encounter production
- Automated prioritization of encounter correction activities
- Extensive operational and executive reporting to identify encounter trends, monitor acceptance rates, and proactively correct issues, through integration with our Centelligence™ Insight desktop reporting system
- Automated extract and delivery mechanisms to minimize bottlenecks and the need for manual intervention - assuring process consistency.

As mentioned above, Encounter Pro includes a module which provides a ‘pre-submission scrub’ mechanism to customize and apply edits as a final check for encounter accuracy prior to submission to the state. We will configure Encounter Pro to recognize conditions that will cause an encounter to deny at DHH and hold the encounter record and corresponding claim for review. This will allow us to work with providers to correct any issues and/or reprocess the claim for a valid encounter submission to DHH.

Once processed, the encounter data is batched into appropriate HIPAA standard 837 files and will be submitted in accordance with DHH timeliness requirements via our secure, auditable, COVIANT file transfer system (see discussion above). Encounter response files are also processed by our Encounter Pro application, updating the encounter history and identifying encounters that must be re-processed. Encounter Pro provides an online management tool and extended reporting for encounter submission and response analysis. For example, if errors are reported in the DHH response file, Encounter Pro provides a platform by which each error can be researched by our Encounter Business Operations (EBO - our Centene nationwide encounter processing center of excellence) and LHC encounter staff. Once we determine the solution to the error, we re-process the claim in AMISYS Advance and the encounter is then resubmitted through Encounter Pro.

Centene will retain all data elements in our claims history necessary for creating encounters in compliance with DHH and the Fiscal Intermediary requirements. Please see our response to R.5 for additional detail.

Current Experience Processing Data

Centene currently receives, processes and updates enrollment/eligibility data in each of the states in which we operate a health plan. As described above, we utilize a standard HIPAA 834 file to load and update member enrollment and eligibility data into our MIS for each of the states we serve. In certain situations, we also utilize supplemental, proprietary data files to incorporate state-specific information necessary for the management of the program. In all cases, we meet or exceed local state technology and business requirements and compliance guidelines to utilize data in a consistent, accurate and effective manner.

A key differentiator for Centene is our organizational focus on public sector healthcare programs. The administration and use of Medicaid and CHIP enrollment/eligibility data differs significantly from private or commercial health insurance programs. Over the years, Centene has developed specific business processes, controls and technologies designed *specifically* and *exclusively* for the continued successful processing of state Medicaid and CHIP data.

As evidenced by the table below, Centene has extensive experience utilizing state-provided enrollment/eligibility data to manage 11 programs across the country. Our experience extends from 27 years operating a health plan to recent implementation in 2011. What this means for DHH is a successful history of data processing capabilities maintained over an extended period of time, inclusive of the many changes necessitated by federal or state requirements. In addition, we also have recent and *relevant* experience implementing new health plans within the current regulatory environment.

Centene Operated Plan	[1]Utilization of HIPAA 834?	[2]HIPAA Level	First Year of Operation
Wisconsin	Yes	1	1984
Indiana	Yes	1	1994
Texas	Yes	4	1999
Ohio	Yes	1	2004
Arizona	Yes	1	2006
Georgia	Yes	4	2006
South Carolina	Yes	1	2007
Florida	Yes	1	2007
Massachusetts	Yes	1	2009
Mississippi	Yes	1	2011
Illinois	Yes	1	2011

[1] We have been exchanging HIPAA 834 transactions with all our plans since 2003.

[2] Please note that HIPAA Compliance Levels listed in this column are the Compliance Levels requested by our state clients or their enrollment brokers. We can support a broad variety of formats and HIPAA compliance standards, and for our largest markets we have encouraged and requested a higher HIPAA compliance level to improve our ability to automate eligibility processing (Texas and Georgia).

For the CCN-P program, Centene and LHC will leverage our existing operational experience to utilize eligibility/enrollment data provided by the DHH Enrollment Broker in accordance with the requirements specified in the RFP and as described above in response to this question. Our experience in the Medicaid industry has given us the tools and skills necessary to meet all DHH-specified coding, data exchange formats and transmission protocols. We strive to leverage data standards across all our health plans for ease of processing but retain extensive flexibility in our technology and business approach to accommodate state-specific needs. Our demonstrated success in processing Medicaid data for eleven public sector programs has prepared us with a multitude of experienced resources and targeted technology solutions relevant to the Louisiana program. We look forward to bringing our experience to Louisiana and applying our solutions to the benefit of the CCN-P program.

Lessons Learned & Working with DHH, the Fiscal Intermediary and the Enrollment Broker

We have learned, through years of firsthand experience, that implementing Medicaid and CHIP based managed care programs have a variety of logistical, cultural, and operational challenges - *particularly* in service areas where managed care and coordinated care concepts are new to members and providers. From a data interfacing perspective, new programs (such as CCN-P) face a different set of implementation challenges. Below we have enumerated three "lessons" from prior experience that we feel are particularly important for DHH, the FI and EB, and CCN's to use to inform the data interface aspects of CCN implementation.

Lesson 1: Provider Data Interface Definition Needs Top Priority Early in the Implementation Process.
Although there are challenges and important considerations with all interfaces we configure with our state clients, we have found that it is *provider data exchanges* which need to be treated as "first among equals" - particularly in terms of defining these interfaces with complete clarity early in the implementation, well before the start of operations. We believe there are several reasons why provider data exchanges have become relatively more problematic than other data interfaces:

- **Reason 1**: Unlike enrollment, eligibility, and encounter data - there is no HIPAA transaction standard, nor any other "de facto" convention, for the structure of provider file exchanges. Although the HIPAA transaction standards are not perfect, they certainly do provide a more mature "lingua franca" for data usage and a common file structure for enrollment and eligibility (the HIPAA 834) and encounter records (the HIPAA 837) than proprietary provider file interfaces. The result: it is painfully easy for two Trading Partners to *misunderstand* the exact meaning and use of provider data - in terms of definitional meaning and contextual use.
  - For example, during one implementation, our state client requested a provider file to demonstrate we were meeting network adequacy requirements. We were happy to provide the file in the prescribed format and for the express purpose of evaluating provider network adequacy. However, unknown to us, the state also utilized the file for PCP auto-assignment. Unfortunately, the original file we provided did not contain an appropriate level of detail that would be best-suited for PCP Assignment (i.e., rather than at an individual practitioner level, the file contained group-level information). Although we were able to resolve all issues in a timely manner and meet state needs, this underscored the importance of fully understanding the state's process goals and intended data usage requirements in as much excruciating detail as possible rather than simply relying on the technical data file requirements.
- **Reason 2**: As compared to membership or encounter data, neither the state nor Centene has as much control over provider information attributes such as demographic, specialty, licensure, location and affiliation data. Provider information is more volatile, and changes stem from many different parties - not just the provider (e.g. board certification, affiliation arrangements). The result: the opportunity is much higher for an "out of data synch" condition between Centene, the state, the FI, and even the Enrollment Broker with provider data - than with membership or encounter information.

We do not claim to have found a perfect solution to the above challenges; but we have undertaken several measures to mitigate issues with provider data interfaces:

- From an *implementation planning* perspective, we now emphasize with our clients the need to focus on provider data as "step one" in our data interface planning - even before eligibility and encounter analysis and configuration. The CCN-P Systems Companion Guide (Appendix G) is a very good starting point for detailed review with DHH and other CCN's (see lesson 2 below), and we would recommend extended discussion and documented questions and answers regarding the "Appendix G" exchange and other provider data exchange details (questions #147 and #227 in DHH's document: CCN PREPAID RFP QUESTIONS AND ANSWERS, dated 5/23/2011; are good examples). We have noted, for example, in DHH's RFP for Enrollment Brokers, the need for a daily provider interface between the Enrollment Broker and the CCN. We can (and do) support the import of daily provider data, but of course DHH's CCN's will need to know the exact nature and processing purpose of daily provider data feeds to CCN's.
- From a *data quality perspective*, we have enhanced our provider master data management, via the implementation of our PRM system. PRM is our integrated approach to provider contracting (the Emptoris component of PRM), provider inquiry tracking and management (ProviderConnect: our Microsoft Dynamics Customer Relationship Management (CRM) application), and master provider data management (Portico: the heart of our PRM). PRM is the "system of record" in our integrated MIS for "all things provider", greatly mitigating the risk of disparate provider data within the confines of our overall MIS.
- Also from a provider data quality perspective: we are implementing integrated provider data services with *Enclarity* (please see discussion above). Enclarity affords us (and our state clients) with a 'trusted third party source' of provider data - by focusing on the best sources of provider data among the countless sources of that data in health care arena.

Lesson 2: It is Virtually Impossible to "Over Specify" or "Over Communicate" Data Interface Specifications.

Looking back at the 27 years of implementations we have performed alongside our state clients, their intermediaries, our subcontractors and providers (in other words: all our Trading Partners); we can synthesize another lesson: it is necessary, *but not sufficient*, to share clearly documented data interface specifications amongst Trading Partners. These interfaces must be rigorously vetted, discussed and paraphrased via both written formal documentation, and extended meetings with small working groups. For example, in one of our recent implementations, the full MIS implementation team (meaning the state, their intermediary, and our fellow Managed Care Organizations (MCO's - the equivalent in this case of CCN's) agreed that each MCO would document detailed questions regarding enrollment, eligibility, provider and encounter interfaces; followed by meetings driven in part by discussion and documenting responses to those questions - with answers distributed to all parties. We *strongly encourage* this technique for the CCN-P Program implementation - especially with multiple CCN's operating in the GSA's. In our experience, the best implementations (at least from a data interface perspective) involve multiple, regular meetings beginning immediately after contract execution, with limited (but regularly attending) participants from all MCO's (CCN's) and the state and/or FI and/or Enrollment Broker; with the early focus on a consistent and detailed understanding of each interface. We have found that, in the past, all Trading Partners (ourselves included) tend to *underestimate* the time and effort needed for arriving at a workable understanding of data interface requirements. The bottom line of this lesson regarding data interface requirements: when in doubt, **over-specify**.

To help our implementation efforts for meetings such as the above, we make extended use of screen sharing over the web (e.g. WebEx). An even more powerful assist is the use of video teleconferencing, and we have recently implemented *Cisco Telepresence* equipment in our corporate offices. Should DHH

or DHH's FI (or Enrollment Broker) employ video conferencing equipment, we have found this "face to face" use for small meetings very effective.

To further align our "systems syntax" and technology framework with our clients, we have adopted a view of Medicaid Management Information Systems (MMIS) in line with CMS' Medicaid Information Technology Architecture (MITA). Thus, similar to MITA, our MIS adopts a Service Oriented Architecture (SOA) view of business and technical services applied to public sector healthcare; Master Data Management (MDM); and other architectural components and nomenclature as they pertain to MMIS design. We are adopting a MITA view in order to be better able to "talk a common technology" language with our clients, and execute smoother data interface implementations in support of eligibility, enrollment, provider data and encounter processes. Please see R.4 and R.2 for more information on our SOA and MDM architecture.

Lesson 3: Perform End to End Testing. As emphasized in MITA (see above), we have learned that it is important to avoid viewing individual data interfaces as "silos" of isolated data exchanges. We have found that it is not enough to test individual exchanges (e.g. receipt of eligibility data, transmission of test encounter data) with our state clients and Trading Partners without progressing through an entire cycle of information processing that spans all the core functions served by enrollment, eligibility, provider, claims, and encounter data in holistic "end to end" scenarios.

Part of the challenge in performing this "end to end" or "full cycle" testing is to obtain higher quality test data (i.e., test data that more closely resembles production data) and test "scenarios". For example, in one recent implementation, we were able to work with our state client to get "full scenario" test data - e.g. test member data in the enrollment file linked to a particular PCP on the test provider file subsequently authorized for a covered service, with claims from that provider for that member processed in a specific encounter encompassing the entire "cycle". This approach not only allowed us to validate each data exchange, it also allowed us to simulate the scenario throughout our member and provider inquiry services applications, our reporting applications, and our web portal applications. "End to end" scenario testing such as this is, in our judgment, the most practical way to uncover implementation nuances and challenges that might not otherwise surface.

Question R.7

System Compliance with Requirements in Section §16

R.7 Describe the ability within your systems to meet (or exceed) each of the requirements in Section §16. Address each requirement. If you are not able at present to meet a particular requirement contained in the aforementioned section, identify the applicable requirement and discuss the effort and time you will need to meet said requirement.

Systems Focused On Louisiana's CCN Needs

Nationwide, Centene's scalable MIS supports the goals of responsive, accountable, and coordinated care for almost 1.6 million Americans in our public sector, full risk managed care plans in 11 states. We accomplish this through an architecture engineered for integrated medical and behavioral application support, reliability, availability, and interoperability. Centene's MIS currently supports all population types that will be served by the Coordinated Care Network-Prepaid (CCN-P) including Temporary Aid to Needy Families (TANF); Aged, Blind, and Disabled (ABD); and Children's Health Insurance Plan (CHIP). Centene will support LHC with 27 years of Medicaid and CHIP processing experience and over 275 Information Technology (IT) professionals focused solely on the automation requirements to regularly meet and surpass our state clients' needs.

We have reviewed in detail all requirements in Section 16 of the RFP, as well as the CCN-P Systems Guide included with the RFP. We will meet or exceed all of these requirements and, in fact, do support these requirements today for Centene's plans in other states.

Below we have enumerated each requirement in Section 16 of the RFP and describe how we meet or exceed each requirement.

16.1. General Requirements

16.1.1. Overall Function and Compliance. Our MIS is fully compliant with HIPAA mandates, rules, and standards per HIPAA Security and Privacy (45 CFR 160 and 164), and HIPAA Transaction and Code Set (TCS) regulations (45 CFR 162); and applicable privacy and security regulations originating from the American Recovery and Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health Act (HITECH). Please refer to 16.2 and 16.10 below, as well as Section R.15 and R.16, for more information on our security safeguards and adherence to federal mandates.

As it does today for LHC affiliates, Centene will configure and securely operate its integrated MIS for all applicable LHC processes and DHH requirements, including enrollment; eligibility; clinical care management and authorization (medical and behavioral); claims; encounter processing; telephony; secure web and health information exchange support; predictive modeling, informatics and reporting functionality; and support for DHH access.

16.1.2. Relational Databases. The entire database layer in our enterprise MIS is based on industry standard relational database management systems (RDBMS), including our approach to logical database modeling and corresponding tools; physical database implementations; RDBMS integrity controls; database replication and communications; and industry standard Structured Query Language (SQL) decision support tools. All of our production transaction databases use RDBMS technology from Oracle (Oracle 10g), Microsoft (SQL/Server), and Teradata (Extreme Data Appliance). We use and support several widely available database interface technologies, including Open Database Connectivity (ODBC); Object Linking and Embedding (OLE); and standard Extract, Transform, and Load (ETL) interfaces from widely available vendors such as Informatica and TIBCO. Please see the table in 16.1.4 (Capacity and Scalability) below for more information. We use RDBMS business intelligence tools from the Business Objects Enterprise XI R2 Premium tool suite, including Crystal Reports XI and Web Intelligence XI for reporting, ad hoc query, and analysis. Please see Section R.10 for more information.

16.1.3. DHH Interoperability and Standards

Desktop Workstation Hardware and Software. Over the past two years, we have evolved our desktop workstation configuration from our legacy "PC client/server" approach to an enterprise architecture that more tightly integrates with our overall MIS and delivers us critical advantages in secure data

management, performance, and systems administration and management. These are all important factors for our clients, such as DHH, who demand reliable solutions for business continuity, data integrity, and availability. In answer to these needs, today we use a *virtual desktop*, "thin client" based architecture to deliver responsive and secure application and data access to all our health plan end users, including LHC. Centene was selected as a finalist in the 2010 Citrix Innovation Award for our rapid deployment of virtual desktops. The combination of our virtual desktop infrastructure and thin client hardware exceeds the performance of the PC desktop client hardware configuration specified in Section 16.3.11.1 of the RFP, and offers several important advantages over a traditional PC desktop approach to end user computing:

- All data is stored in Centene's datacenter in St. Louis, Missouri, with all the advantages of large scale computing power, communications bandwidth, secured storage, and fault tolerant systems and environmental controls that come with enterprise scale installations. This means critical business data is not stored on local PC drives; is not lost or damaged in the event of local office emergencies; and is maintained with greater integrity (no redundant data is stored on desktop PCs).
- All end user applications, including both our core health care applications (eligibility, enrollment, member and provider service, claims and encounter processing, decision support, etc.), as well as end user office tools, such as Microsoft Office 2010, Microsoft Exchange, and Internet Explorer are all managed and updated from our central datacenter. This means software updates can be distributed uniformly and rapidly. It also means our IT professionals have complete and systematic control over the software provisioned for all desktop workstations, with the result that our users cannot install software on their desktop without assistance from our IT staff, further protecting us from viruses and malware.

Our standard desktop workstation hardware is the Wyse Viance Desktop Appliance for Citrix XenDesktop, with virtual desktop and remote application support using Citrix XenDesktop, XenServer, and XenApp products. The desktop operating systems include Desktop Windows Server 2003, SP2 with Citrix XenApp 4.5 for thin clients, and Windows XP for laptops. Please see the table below, which correlates RFP Workstation Hardware and Software requirements with Centene and LHC deployments.

Component	RFP Requirement	Centene Configuration for LHC	Comment
Desktop Processor	Dual Core Processor (2.66 GHz, 6MB cache, 1333 MHz FSB)	*Via C7-Eden* in thin client, with client processing performed in *Cisco Unified Computing Services (UCS)* servers	Exceeds requirement. The combined processing power of our thin client and application and database servers exceeds the equivalent performance of traditional client/server implementation for the types of applications LHC will be running. In our thin client configuration, the computing power for ***all*** business logic and data operations is sourced from the processor in the server(s) that hosts the virtual desktop or application (our Cisco UCS servers). Please see Question R.3 for more information.
RAM	4 GB	4 GB	Meets requirement. In our thin client architecture, desktop applications can request more than 4 GB RAM from the Cisco UCS servers, on demand.
Disk Storage	250 GB HDD	LAN and SAN storage	Exceeds requirement. Our thin client desktop has no hard disk drive for security and data integrity reasons;

Component	RFP Requirement	Centene Configuration for LHC	Comment
			however, storage available to our thin client significantly exceeds 250 GB and includes local LHC LAN and Centene Storage Area Network (SAN) architectures.
Discrete Video Memory	256 MB	256MB	Meets requirement.
Monitor	A color monitor or LCD capable of at least 800x640 screen resolution	VESA color monitor support with Display Data Control (DDC) for automatic setting of resolution and refresh rate and 24-bit/16.7M colors, up to 1600x1200 resolution	Exceeds requirement.
Optical Media	DVD +/-RW and CD-ROM drive capable of reading and writing to both media	DVD +/-RW and CD-ROM drive capable of reading and writing to both media	Meets requirement. Please note: as a part of our defense-in-depth strategy, Centene strictly limits the availability of writeable DVD and CD drives to *only those users with a demonstrated need*. We enforce this well reasoned approach to mitigate the risk of Protected Health Information (PHI) or other confidential data being written to portable media without proper authorization. Where such drives are allowed, our system controls ensure that any data written to removable media is appropriately ***encrypted.***
USB Ports	Enough to accommodate thumb drives, etc.	3	Meets requirement. Please note: our systems encrypt all data written to thumb drives for Protected Health Information (PHI) security.
Network Interface Cards	1 gigabyte Ethernet card	1 gigabyte Ethernet card	Meets requirement.
Printer	Printer compatible with hardware and software required	HP LaserJet Printer	Meets requirement.
Operating System	Microsoft Windows XP SP3	Microsoft Windows XP SP3	Meets requirement.
Web Browser	Microsoft Internet Explorer V7.0	Microsoft Internet Explorer V7.0	Meets requirement. Our browser implementation is capable of resolving JavaScript and ActiveX scripts.
E-mail Client	Microsoft Outlook compatible	Microsoft Outlook	Meets requirement.
Office productivity suite	Microsoft Office 2007 compatible	Microsoft Office 2007	Meets requirement.
Internet Access	Access to high speed Internet	All LHC workstations will have secure, high speed and continuous access to the Internet.	Meets requirement.
Anti-virus, antispam, and anti-	Each workstation connected to the Internet should have	We use McAfee ePolicy Orchestrator Enterprise Agent running McAfee Virus Scan 8.7 and	Meets requirement. In addition, users cannot install software on their thin clients, further protecting our MIS

Component	RFP Requirement	Centene Configuration for LHC	Comment
malware software	anti-virus, antispam, and anti-malware software. Regular and frequent updates of the virus definitions and security parameters of these software applications should be established and administered	McAfee Host Intrusion Prevention System (HIPS). IronPort Spam filter along with Sophos Anti-Virus software further protects email.	environment from viruses and malware.
Compression software	Compatible with WinZIP v11.0	WinZIP v11.2 (compatible with WinZIP v11.0)	Meets requirement.
Encryption Software	All workstations, laptops, and portable communication devices shall be installed with full disk encryption software.	All of our laptops and portable communication devices have MacAfee's Safeboot encryption software (our thin client desktops have no hard drive and no stored data). In ***addition***, all mobile devices are equipped with Absolute tracking software so that a device (e.g. laptop or PDA) can be physically located when connected to a network. In order to prevent disclosure of PHI, if a device is lost or stolen, access to that device (laptop, Blackberry, etc.) is systematically revoked and authorized MIS staff delete data remotely.	Exceeds requirement. Please see Question R.16 for more information.
Security Controls	Compliant with industry-standard physical and procedural safeguards for confidential information (NIST 800-53A, ISO 17788, etc.)	We implement controls compliant and supportive with both NIST and ISO standards, as well as those mandated in HIPAA Security (45 CFR 164), HIPAA Privacy (45 CFR 160 and 164), and in accordance with Sarbanes-Oxley Section 404.	Meets Requirement. Please see Question R.16 for more information.

In addition to above, our standards for laptops are Dell "E" models, with encrypted hard drives and a minimum of 4GB RAM.

Network. As with our existing Centene health plan field offices, LHC offices and staff will be connected to Centene's datacenter via our secured high-performance, fault-tolerant Wide Area Network (WAN), consisting of a virtual full-mesh, private IP Multiprotocol Layer Switching (MPLS) network. We have a standard LAN configuration using 1GB Mbps T100 Network Interface Cards and Cat5 dual port wiring at a minimum. One of the many advantages of Centene's thin-client virtualized desktop environment is that all resource intensive processing occurs on the server-side of the architecture. As such, the network bandwidth requirements to the end-point are significantly lower than traditional thick-client models. LHC Internet access will be provided through our OC-3 circuit and 155Mbps Internet service is supported through a Cisco router, connected to redundant corporate firewalls (Cisco 6500s). Intrusion Detection Systems (IDS) are located within our trusted and untrusted segments. We also have De-Militarized Zones (DMZs) to provide segments for Web Servers, Domain Name System (DNS) Servers, and Secure Access Gateways. We provide remote access to our internal network through a Virtual Private Network (VPN)

using Cisco's VPN 3000 Concentrator and also through encrypted sessions using Citrix Secure Gateways. Please refer to Question R.3 for additional information on our network.***Backup Processes.*** LHC's program data records (enrollment, eligibility, clinical care management, claims, inquiries, grievances, appeals, provider, historical reports, and any other files processed in LHC's office on our secure LAN in Baton Rouge) will be housed in St. Louis as an integrated part of our MIS. In St. Louis, Centene's backup strategy allows us to manage a recovery scenario in the most efficient and reliable way possible through:

- automated, operator-less backup/restore processes and the use of and enterprise class data storage management system from IBM (Tivoli Storage Manager)
- fast online backups to high speed media backup storage device (EMC DD880) and monthly tapes
- optimized single file, database, and full system recovery
- full function tape management facility to manage the location and protection of all tape media
- complete catalog containing a history of all backup data at its location on media
- replicated backup storage device and automated tape copies for offsite storage and Disaster Recovery needs

Please refer to R.3 for more details on our backup procedures.

Power Surge Protection and Backup

Datacenter Facilities. Centene's datacenter in St. Louis, Missouri, is home to all of the core application services that will support LHC. Our datacenter is equipped with two diverse power feeds into the facility with redundant Uninterruptible Power Supplies (UPS) providing battery backup power to all IT equipment. Two separate power systems in the facility (A and B) provide redundant (2N) power to each rack of equipment on the datacenter floor. This allows equipment within the electrical plant to be taken offline and maintained without power interruption to the computing equipment and provides continuous power in the event of the loss of power to either power feed entering the facility. In addition, the facility is equipped with a diesel generator capable of supporting all IT services in the event of a loss of both power feeds entering the facility or a prolonged power outage, **well beyond four days**. We execute a full load test quarterly to validate the generator's effectiveness.

Second Datacenter. In Q4 2011, we will complete production implementation of our new Tier 3, 19,000 square foot datacenter, with capacity for over 165 IT racks; 6,000 square feet of datacenter floor; and fully redundant environmental, power, and network connectivity systems. Our new datacenter has a seismic importance factor of 1.5 (fully operational following an earthquake); and is rated to withstand winds up to 165 MPH (an F3 tornado). Beginning in Q1 2012, we will operate our 2 datacenters as mutual "hot site" backups whereby each datacenter will be able to assume operation of critical production systems if the other datacenter becomes inoperable, within *seconds* of a site disabling outage.

LHC Field Office. LHC's office in Baton Rouge will be equipped with full UPS, and backup power generator for prolonged power outages, up to a minimum of four days. Note that in any situation where local power in Baton Rouge were to be disabled for more than four days, LHC staff and/or backup Centene staff would most likely be operating from our fully equipped Mobile Recovery Trailers, and/or one of our backup sites. Please see our responses to Section M.1, M.2, and R.3 for additional information on the assets, plans, and procedures supporting our Business Continuity Plan.

16.1.4. Capacity and Scalability. Today, Centene's MIS responsively and reliably administers full risk, public sector managed care programs for approximately 1.6 million members in 11 states. We have the computing power and communications bandwidth in place today to support LHC and can efficiently scale up to meet the needs of LHC for any number of Louisiana CCN-P members we have the privilege to serve.

Business Systems Scalability. We employ clustering, load-balancing, and virtualization technologies, combined with disciplined systems engineering, to support both horizontal and vertical scalability. Vertical scaling is accomplished by adding more CPU, memory, and/or disk resources to the individual server nodes in a cluster. Horizontal scaling comes from adding new server nodes to an existing cluster.

By employing both of these techniques, the Centene MIS infrastructure can accommodate rapid incremental growth in capacity while simultaneously maintaining, or even improving, the performance experienced by the end-user.

Database Scalability. From a database layer perspective, we employ a multi-path SAN optimized for transaction data applications and a best-of-breed Teradata enterprise data warehouse solution that has been recognized across the industry as the leader in data access performance and scalability. Teradata has provided Centene with the ability to access and perform analytics across large, rapidly expanding data sets. This in turn has enabled strategic development of new and creative knowledge-mining tools that allow us to further enhance delivery on our mission to provide better health outcomes at lower costs even as our member population and service offerings experience rapid growth. The table below offers more specifics on the scalable aspects of our MIS:

MIS Layer	Capacity and Scalability
Business System Layer	Five HP 9000 servers running HP/UX Unix power AMISYS Advance, our core enrollment, eligibility and claims processing system. Three *application* servers operate as a cluster using Veritas technology and are configured with 4 CPUs and 64 GB of main memory, each scalable to 8 CPUs and 192 GB of memory. Two *database* servers use Oracle 10g Real Application Clustering (RAC) for high availability and are configured with 4 CPUs and 48 GB of main memory, each scalable to 8 CPUs and 192 GB of memory. For our Clinical Applications (including our TruCare health services management system), we use rack mounted Windows/Intel ("WinTel") blade servers operating in a virtual environment using EMC's VMware virtualization software technology. Please refer to R.3 for more information.
Database Layer	All core LHC data will be stored on our fully redundant Storage Area Network (SAN) which supports access to 2 highly available arrays: a NetApp SAN attached Storage Array with Independent Disk (RAID) 5 and RAID 6 configuration; and an HP StorageWorks XP24000 configured for RAID 5 storage. The XP24000 can scale up to 1.13 PB and is currently configured at 146.5 TB. Our Centelligence™ family of reporting, health informatics, predictive modeling, and decision support applications is powered by our Teradata® Extreme Data Appliance. Please refer to R.3 for more information.

16.2 HIPAA Standards and Code Sets

The HIPAA EDI infrastructure component of our MIS includes an integrated combination of our Coviant secure file exchange management system; TIBCO middleware; our EDIFECS EDI processing engine with HIPAA 4010A and 5010 compliance transaction checking, validation, and translation; and AMISYS Advance, our core enrollment, eligibility and claim processing system.

16.2.1. HIPAA Transaction Processing. Our COVIANT Diplomat Transaction Manager (COVIANT) handles our automated, scheduled production file exchanges (transmission and receipt) with our state clients and/or their fiscal intermediaries (FI). We support all standard industry data communication protocols such as Secure FTP–SFTP (SSH), FTPS (TLS/SSL), PGP encryption over the internet or via a Virtual Private Network (VPN). COVIANT will protect LHC's file exchanges with access control, authentication, and secure configuration features. From an internal data networking perspective, our network backbone is highly redundant through a mesh design that provides multiple paths to and from each point, allowing maximum network availability to submitting providers or clearinghouses, our corporate Datacenter and LHC's local office, enabling us to meet our DHH transmission schedules.

In addition to the above, we already support multiple methods for HIPAA transaction exchanges with our providers:

- We support over 60 Clearinghouse trading partners nationwide, including EMDEON, Inc. (EMDEON) and Availity, both with significant presence in Louisiana.
- Providers can also submit HIPAA 837 P or 837 I claim files to us directly through our secure web based Provider Portal.
- Providers can also enter professional or institutional claims directly through our HIPAA Direct Data Entry (DDE) compliant, online, claim entry feature, also on our Provider Portal.

We process inbound and outbound HIPAA transactions through our EDIFECS EDI system for HIPAA 4010A and 5010 compliance validation and translation and load via TIBCO middleware into AMISYS Advance, our core claims processing and eligibility system. Today, Centene processes about 2.2 Million HIPAA compliant medical and behavioral encounters per month for all our plans nationwide.

All of the above capabilities are in place today and will be configured for LHC for MIS readiness review activities.

We have reviewed in detail all requirements the CCN-P Systems Guide included with the RFP and can support all formats included in that document.

16.2.2. HIPAA Transaction Compliance. Today, we use the EDIFECS suite of HIPAA transaction products integrated with our communications, workflow, and transaction processing systems to support HIPAA inbound and outbound exchanges. We use EDIFECS Ramp Manager, Trading Partner Management, Transaction Management, and X-Engine to "on board" Trading Partners (TP), manage our relationship with our TPs, route HIPAA transactions appropriately, and enforce any level of HIPAA compliance called for by our TP (commensurate with TP's capabilities), including our state clients and FI's. EDIFECS X-Engine is the leading industry-standard compliance checker, and will support any level of HIPAA compliance, enabling LHC to exchange data at the highest level supported by DHH. We maintain HIPAA Business Associate Agreements (BAA), both as a Covered Entity (e.g. with our subcontractors) and as a Business Associate (e.g. with our state clients).

16.2.3. HIPAA Transaction Support. Today, we support the HIPAA 837P, 837I, 270/271, 278, 276/277, 834, 835, and 820 transactions wherever our providers and state clients can support the HIPAA standard and/or require its use. Our provider data management processes support HIPAA's National Provider Identifier (NPI), as well as state specific identifiers (such as those that DHH may specify at a later date in Appendix G of the CCN-P Systems Guide). In 2010, 85% of the claims we received were via HIPAA EDI, and we expect this percentage to increase as we continue offering more support and electronic submission alternatives for providers. Please see R.13 for more information.

We are on target to support the HIPAA 5010 transaction set (Errata version) on January 1, 2012, per CMS' final rule. Please see Section R.15 for more information on our HIPAA 5010 compliance plan.

16.2.4. HIPAA Transaction Adherence. We will not revise or modify standardized forms or formats, except to be in compliance with federal regulations and DHH standards and companion guides. All of our HIPAA transaction formats are modified through our disciplined change management methodology and through the oversight of our Chief Information Security Officer (CISO).

16.2.5. HIPAA Transaction Standards and Regulations. As we have since HIPAA's initial compliance date in 2002, we will comply with applicable federal and HIPAA standards and regulations as they occur. Please see R.15 for more information on our ongoing monitoring of federal and HIPAA rules and regulations.

16.2.6. DHH and Federal Compliance. Centene and LHC will adhere to national standards and standardized instructions and definitions that are consistent with industry norms and that are developed jointly with DHH. These shall include, but are not limited to, HIPAA based standards and federal safeguard requirements, including signature requirements described in the CMS State Medicaid Manual. We systematically manage compliance with our state client contracts through the use of our Compliance 360 system. Centene's Compliance Department uses Compliance 360 software, which incorporates updated databases of federal, state, HIPAA, and accreditation agency regulations. LHC's Compliance Officer will use this same centralized system to manage and track our ongoing compliance to DHH standards and contract terms.

16.3. Connectivity

16.3.1. Interfaces with DHH and DHH Designates. We have the capability to establish any industry standard real time, online access method, batch file exchange, HIPAA transaction, or HL7 interface with (at DHH's direction) DHH, DHH's FI, DHH's Enrollment Broker (EB) and/or other DHH, FI, or EB Trading Partners. We support Virtual Private Network (VPN) connectivity, secure FTP exchanges over the internet, and/or direct leased line connectivity if needed. We support Public Key Infrastructure (PKI) security methods such as PGP encryption, secure FTP– SFTP (SSH), or FTPS (TLS/SSL) for HIPAA compliant security, encryption, and sender authentication. For interactive access needs, we support web browser interfaces, Citrix based solutions, including Virtual Desktop Infrastructure (VDI), or Windows Remote Desktop Services.

We also support secure email communications (e.g. for any communication containing Protected Health Information (PHI)) between systems, sites, and/or domains through Transport Layer Security (TLS), an industry standard protocol for securing electronic communication. Our messaging systems also support industry standard protocols such as S/MIME and SSL.

16.3.2. Document Standards. We are fully capable of supporting DHH and DHH's FI document management standards. Below we have listed DHH's requirements from CCN Prepaid RFP Questions and Answers, dated May 23, 2011, in response to question #256 in that document, along with a description of our capabilities:

Requirement	How We Support The Requirement
Retain paper documents for a minimum of 3 years, (which may be in imaged form)	We scan paper claims and associated documentation, and member and provider paper correspondence, immediately upon receipt. We store the paper originals off-site indefinitely through our HIPAA compliant off-site storage vendor, Recall; and we store images online indefinitely. All other paper documentation (for example, a contract or legal document) is scanned using our Zasio Versatile Enterprise™ system and available as images indefinitely. Our Provider Network Management staff scan, index, and store provider contracts in the Emptoris provider contracting module of our Provider Relationship Management (PRM) system and these documents are available online indefinitely. Please see 16.13.1 (Document Retention Periods and Retrieval Requirements) below for more information.

Requirement	How We Support The Requirement
Establish appropriate document indexing, archival and retrieval capabilities, whether paper- or image-based	We index claims, associated claims documentation, and member and provider correspondence by multiple indices including (where applicable), Internal Control Number (unique claim number), member and provider identifiers. This allows our users, including Member and Provider Service Representatives, Claims Processors, Internal Auditors, or any other authorized user to rapidly retrieve images. Please see 16.13.1 (Document Retention Periods and Retrieval Requirements) below for more information.
Provide DHH personnel with ability to request and obtain copies of document(s), whether paper- or image-based.	As we do in the service of all our state clients, we will provide DHH with multiple ways to request and obtain document copies, including via fax. Centene and LHC will provide a dedicated telephone number for DHH to use to directly contact LHC offices in Louisiana, to help ensure our responsiveness to DHH record requests. Please see 16.13.1 (Document Retention Periods and Retrieval Requirements) below for more information.

We also support standard transaction *codesets* where applicable, per DHH and DHH's FI requirement and per HIPAA rules and regulations.

16.3.3. USPS Standards. Our MIS today uses mailing address standards in accordance with the United States Postal Service (USPS) and we will continue to adhere to USPS standards for LHC's CCN-P Program.

16.3.4. PHR or EHR. We look forward to working with DHH (at DHH's direction) to implement, within a reasonable timeframe, a secure, web-accessible health record for members, such as Personal Health Record (PHR) or Electronic Health Records (EHR).

Electronic Health Records. Interim to DHH's request, we will offer all of our network providers in Louisiana access to our secure Provider Portal. In addition to a number of administrative self-service applications (e.g. eligibility verification, claim submission) available on our Portal, we offer a number of *clinical tools* for authorized Portal users, which we refer to collectively as our *Clinical Portal* (also available to all LHC network providers). Among the facilities available on the Clinical Portal are our summary Member Health Record (MHR), which is a summary electronic health record based on medical, behavioral, and pharmacy claims data.

In addition to above, for our PCP and Federally Qualified Health Center (FQHC) providers who have achieved NCQA or JCAHO medical home recognition, (or for providers committed to medical home recognition), we are offering access to our CenTraCare Clinical Portal (CenTraCare). CenTraCare is specifically designed to assist those of our providers implementing the significant change in care delivery, accountability, and coordination that comes with the medical home model. CenTraCare is a more powerful version of our Clinical Portal, offering access to even more clinical information; medical home level HEDIS reports and clinical quality and cost indicators; expanded health records; and more interactivity with clinical data in general for several meaningful use applications. For example, our Medical Home network providers will have expanded access to MHR information, beyond the summary "face sheet" record offered in the Clinical Portal, with full member-specific clinical profiles; lab data with trending analysis; and the capability to “drill-down” into data to obtain specific information. CenTraCare users will also be able to print the MHR as a PDF and/or export the MHR in Continuity of Care Record (CCR) or Continuity of Care Document (CCD) XML format for subsequent import into a standards based Electronic Medical Record (EMR) system.

CCR is an electronic health record standard developed jointly by ASTM International (ASTM), the Massachusetts Medical Society, the Healthcare Information and Management Systems Society (HIMSS), the American Academy of Family Physicians (AAFP), and the American Academy of Pediatrics (AAP). The CCD standard is an HL7 implementation of the CCR formulated through HL7 and ASTM. Both the CCR and CCD formats have been adopted by the US Department of Health and Human Services as a

Patient Summary Record standard in Title 45 Section 170, Subparts B and C: Standards, Implementation Specifications, and Certification Criteria for HIT, issued by HHS in July of 2010.

Please see R.15 for more information on our EHR capabilities and plans for Louisiana.

Personal Health Records. We also propose to allow LHC members (or their parents or legal guardians) to permit us, strictly on an "Opt-In" basis, to supply their Microsoft HealthVault enabled Personal Health Record (PHR) with the member's medical data we have in our MIS on a regular update basis. Through this offering, we will help the interested member (or their parent or legal guardian) to set/up their free Microsoft HealthVault powered PHR and we will securely transmit medical data to Microsoft to update that member's PHR with any information we may have on that member.

By having important personal health information securely stored in HealthVault, our members will be able to view, retrieve, and share that information with any provider they choose; with obviously important ramifications in wide-scale emergency situations (e.g. hurricanes); as well as any number of other care coordination scenarios, including the transition of the member from one CCN-P plan to another, or to any other health plan.

Please see K.5 and M.1 for more details on our PHR proposal for LHC's CCN Program.

16.3.5. Health Information Exchange (HIE). We welcome the opportunity, at DHH's direction, to participate in statewide efforts to incorporate all hospital, physician, and other provider information into a statewide health information exchange.

Interim to DHH's request, we propose during 2012 to pilot the exchange of standard EHR data with several FQHCs who are NCQA or JCAHO recognized Medical Homes in the New Orleans area. We are targeting this pilot with the FQHCs who have begun implementing Federal Office of the National Coordinator for Health Information Technology (ONC) certified Electronic Medical Record (EMR) systems. We are also proposing to pilot EHR data exchange with two non-FQHC PCPs, who have earned (or are in the process of certification for) Medical Home accreditation. We plan to work in close cooperation and coordination with the Louisiana Health Information Technology (LHIT) Resource Center to share implementation ideas and experiences.

Our pilot will demonstrate EHR connectivity directly with Centene, and through a commercial HIE connectivity vendor, such as Availity, LLC, Passport Health, Inc., etc. We will also work, at DHH's direction, with the Louisiana Health Care Quality Forum and the LaHIE project and explore the possibility of connectivity with LaHIE or other statewide HIE. Please see R.15 for more information on our EHR data integration pilot.

Centene has also been active in Texas and Arizona, where we are working with HIE efforts in both states, including the Health Information Network of Arizona, along with the Arizona Department of Health Services (ADHS); and in Texas, the Texas Health and Human Services Commission (HHSC). We continue to aggressively work with these HIEs as well as the respective states' claims and eligibility vendors, large hospitals and provider groups, and other key health care organizations to enable us to exchange clinical and demographic data across our respective platforms and to inform our HIE efforts in a collaborative spirit with each state in which we operate.

16.3.6. DHH Work Groups. We look forward to meeting and actively participating, as requested by DHH, in workgroups or committees to coordinate activities and develop system strategies that actively reinforce the health care reform initiative. We are actively engaged in a variety of teams and initiatives with our other state clients, including activities such as ongoing operational status and management, coordinating efforts to enhance processes, implementing HIPAA 5010 and ICD-10 mandates, and working towards effective implementation of Health Information Exchanges.

16.3.7. DHH Data Ownership. Centene and LHC recognize that all information, whether data, or documentation and reports that contain or reference information involving or arising out of the Contract,

is owned by DHH. We recognize that we are expressly prohibited from sharing or publishing DHH's information and reports without the prior written consent of DHH.

Centene has administered Medicaid based managed care plans for state clients since 1984 and we recognize our role as trusted custodian of our state clients' information and data.

16.3.8. Future MMIS. We agree to comply with any transitional requirements as necessary should DHH contract with a new FI during the Contract, at no cost to DHH or its FI. We have relevant experience among our other state clients with just this scenario. For example, in 2010, one of our state clients moved to a new FI and a new MMIS. In anticipation of that cutover, and working with the state and the new FI, we successfully implemented, tested, and deployed changes to support new:

- Enrollment and eligibility file exchanges
- Encounter and associated file exchanges
- Additional reference file exchanges

We accomplished all of the above, and more, at no cost to our state client or the FI.

16.3.9. DHH Connectivity Costs. LHC will be responsible for initial and recurring costs required for access to DHH system(s), as well as DHH access to LHC system(s). We understand that these costs include, but are not limited to, hardware, software, licensing, and authority/permission to utilize any patents, annual maintenance, support, and connectivity with DHH, the FI, and the enrollment broker.

16.3.10. Information Systems Capabilities Assessment (ISCA). Centene and LHC will complete an Information Systems Capabilities Assessment (ISCA), which will be provided by DHH, no later than 30 days from the date LHC signs the Contract with DHH.

We have a working familiarity with the ISCA format and look forward to receiving the ISCA questionnaire that DHH plans to customize and post on its website in June 2011 (per DHH's response to Question #649 in CCN Prepaid RFP Questions and Answers, dated May 23, 2011, from DHH).

16.3.11. Hardware and Software. We will meet, and in some cases, exceed all DHH requirements for 16.3.11. Please see our response above to 16.1.3. (DHH Interoperability and Standards) for details on each DHH standard and how we will meet or exceed **each requirement** of 16.3.11.

16.4. Resource Availability and Systems Changes

16.4.1 Resource Availability.

Year Round Availability. Centene will support LHC and our MIS users at DHH, including DHH's FI and enrollment broker users with authorized direct access to our MIS, with our fully staffed technical *Service Desk* located at Centene headquarters in St. Louis, Missouri. The Service Desk is available to users 24/7, 365 days a year through a dedicated toll-free number or internally to LHC staff through a 5-digit extension.

Our Service Desk is staffed by a minimum of two agents from 6:00 a.m. to 7:00 p.m. Central Time, Monday through Friday, with on call staff available after hours and on weekends, all year long. Our Service Desk phone line also allows the caller to leave a voice message and our Service Desk staff return all calls by noon of the next business day (usually earlier).

LHC's Information Management and Systems Director (LHC MIS Director) will assist in the coordination, management, and tracking of all open requests related to applications, hardware, and business data analysis and reporting. The LHC MIS Director will also participate in monthly technical meetings and weekly WebEx calls with the Service Desk to coordinate support activities, as do the MIS Administrators from all Centene health plans.

Efficient Support. Centene's Service Desk employs a "one call and done" approach to user calls whenever possible. Centene trains Service Desk representatives in a wide variety of systems, services, and applications to ensure that calls and emails sent to the Service Desk are handled efficiently by the Service Desk agent themselves without needless escalation. Service Desk employees are required to

attend periodic training courses and seminars related to improving customer satisfaction, diplomacy, and call center techniques. Service Desk technicians also receive a minimum of two weeks intensive training at the Centene Datacenter in St. Louis, Missouri, with technical, in depth topics ranging from PC hardware troubleshooting to AMISYS Advance (our claims processing system) to Centelligence™ report creation. In addition, we offer our Service Desk representatives the latest Computer Based Training (CBT) courses, such as CompTIA A+, N+, and Server+, as well as the Microsoft Certified Professional curriculum. As front line support, the Service Desk is also at the center of crisis management and coordinates with our Network Operations Center (NOC) and key crisis management staff. A core team of systems support analysts, engineers, and management are on standby 24/7 to respond to any crisis call initiated by the Service Desk.

Service Support Automation. Our Service Desk uses ServiceNow (on-demand IT Service Management and helpdesk ticketing system) as an integrated incident support management solution to submit, monitor, and manage calls and change requests from front line users through to completion. Service Desk staff document all calls and requests into ServiceNow where a unique ticket number is assigned. ServiceNow then issues a notification email to the Centene, LHC, or other user who contacted the Service Desk. This email contains the ticket number and a summary of the user's issue or request. Once the user receives an email with a ServiceNow ticket number, they can log into ServiceNow through CNET (our intranet) to view their tickets and the status of each.

ServiceNow is also used by our Network Operations Center (NOC). When our NOC detects an issue, the NOC staff log an alert to a central console. Depending on the severity of the issue, ServiceNow may issue a ticket and notify our on-call technical staff. ServiceNow categorizes incidents and problems by type of service and location to allow us to streamline tracking and reporting, so that we can spot any trends in the issues our front line users are experiencing and develop action plans to eliminate any systemic issues. LHC's MIS staff will be able to enter and view tickets online via ServiceNow to track their status and ensure successful resolution. ServiceNow is Information Technology Infrastructure Library (ITIL) driven and provides *automatic escalation* of trouble tickets to the appropriate Centene or LHC staff, based on customizable metrics such as length of time a ticket is open; knowledge base resolution and activity reporting; keyword and full text searching against the knowledgebase. ServiceNow also:

- enables integrated problem management to assess whether a ticket is a one-time trouble-ticket or an indicator of systemic, longer-term performance and system problems
- facilitates change and risk management planning with an automated approval process
- provides asset management tracking from purchase, implementation, decommission through disposal
- allows us to perform software license compliance tracking
- provides us with a platform for Service-Level Agreement (SLA) administration

16.4.2. Information Systems Documentation. Centene has technical staff and end user documentation for purchased software applications, as well as documentation for our custom software applications and our operations. We regularly update documentation when new or existing applications or processes are implemented or changed. We house most of our documentation on our internal Microsoft SharePoint site, capitalizing on SharePoint’s version control, document access, and other collaboration features.

We agree to all of the requirements of Section 16.4.2 and will provide any such documentation that would be needed by authorized DHH, FI, or enrollment broker users of our MIS and any documentation requiring review by DHH per Section 16.4.2.

We will configure our Microsoft SharePoint to offer DHH an online library of systems documentation that is relevant and germane to DHH use of our MIS, in the hope of making this documentation easy to access for DHH and other DHH designated users.

16.4.3 Systems Changes. We acknowledge and agree to DHH's requirements as stated in Section 16.4.3, including DHH testing requirements, as stated in the document CCN Prepaid RFP Questions and Answers, dated May 23, 2011, in response to question #261.

Today, Centene meets similar needs for a number of our state clients. We are able to meet the above requirements through our use of the following processes and tools:

- Our use of our Compliance/360 system, which will be used by our Centene Compliance Department, along with our Director of IT Security, and our LHC Compliance Officer, to track federal and state compliance regulations and contractual obligations, allowing us to systematically plan for upcoming mandates. See R.15 for more information.
- Our use of ServiceNow to systematically capture, classify by severity, track, communicate status, and manage to completion any incidents that materially impact the delivery of MIS services to our internal or external users
- Our suite of integrated software development and change management tools, including IBM Rational suite of development and testing tools, and Tigris SubVersion Version Control system
- Our adherence to the Agile Software Development Life Cycle process and the Information Technology Infrastructure Library (ITIL) process framework, realized through training curricula, organizational design, and policies and procedures

16.5. Systems Refresh Plan

16.5.1 Annual Systems Refresh Plan. As an architected platform comprised of numerous hardware, software, and networking components, our MIS is not a static utility, but instead, a *constantly evolving system*. Every year, we assess our clients' requirements for enhanced member engagement, provider collaboration, coordinated care, and state client service. We factor in the maturity, "implementation readiness," and interoperability of new technologies to identify when and how to incorporate those technologies in the continuously enhanced service of our constituents. As we plan the introduction of enhanced or new applications and systems, we also assess the need for updates to system and information management policies and procedures. We also compare all components in our integrated MIS portfolio (under our span of control) with the latest product versions from our vendors. The output of this effort is our **Annual Strategic Technology Refresh Plan (Refresh Plan)**, which serves as our roadmap for planned introduction of new or enhanced MIS capabilities. For example, in 2010 we successfully implemented (among other projects):

- a major upgrade of our core claims processing system, AMISYS Advance, from Release 1.0 to Release 4.0
- a conversion from our prior encounter processing system to our MDE Xpress Encounter Pro application
- the introduction of Teradata Extreme Data Appliance technology for data warehousing

Our investment in MIS continues to accelerate. Over the past year, we have committed significant levels of capital and development labor to new applications in member and provider services, data warehousing technology, health care informatics, predictive modeling, clinical profiling, and construction of a second major corporate datacenter, enabling new capacity for growth as well as "hot site" business continuity. We are phasing in these enhancements for our plans, including LHC, over the course of 2011 and early 2012.

We will supply a copy of our Refresh Plan to DHH each year.

16.5.2 Software Versions and Releases. As part of our Refresh Plan process, we maintain a *Technology Services Catalog* for all production, test and development services, and associated equipment. This includes information, such as software versions (application and operating systems), hardware model, capacity, and utilization information. In this process, we also consult with our vendors to ensure we are at the appropriate version and/or release level of each software and hardware component. As we add new systems or enhance existing systems, we update the catalog to reflect this change. We generate capacity and performance reports, which we review regularly to compare current utilization with capacity projections to determine if there is need for adjustments. Each year in October, we perform a complete audit review of all application, servers, software, storage, and infrastructure equipment to ensure that the

Technology Services Catalog contains the latest information. We then review that information to project and plan for any needed upgrades in the upcoming year.

16.6. Other Electronic Data Exchange

16.6.1 Indexed Electronic Image Support. Our MIS fully supports conversion of paper to indexed electronic images that are accessible by Internal Control Number or Claim Number, member, and/or provider identifier.

Our MIS includes integrated MACESS imaging software to index and scan paper correspondence, including:

- Paper claims and supporting claim documentation, such as Explanations of Payment (EOP) from third party payers, provider attestations, and/or other forms supporting claim submission
- Paper provider and member correspondence

Our trained, mailroom scanning staff use our Kodak scanners and MACESS software to index scanned claims documentation by an Internal Control Number (ICN), which links the paper claim documents to the unique ICN housed in our AMISYS Advance claims processing system. For both claims and other correspondence, the scanning staff index the claim documents or letter image by member and/or provider identifier (both if applicable), allowing our claims processors to access those images from AMISYS Advance; and our Member and Provider Services Representatives to access those scanned images via our member and provider services applications, MemberConnect and ProviderConnect (components of our Member Relationship Management (MRM) and Provider Relationship Management (PRM) systems, respectively).

We also receive fax through our integrated RightFax servers. Faxes are treated the same way as paper correspondence, with the exception that the "paper" is already in image form when we receive it. Faxes are indexed in the same manner by our mailroom, scanning staff and these indexed images are housed in our MACESS imaging system for subsequent retrieval by AMISYS Advance, MemberConnect, or ProviderConnect as needed.

In 2011, we will purchase a new data capture solution to *accelerate* the processing of paper and faxed authorization requests and health risk assessments. This solution will be integrated with RightFax on the receiving end and will leverage the workflow capabilities of our SharePoint Enterprise Content Management (ECM) solution to streamline and automate the capture and processing of these clinical documents, and integrate the data into our TruCare clinical care management platform.

Please see R.11 for more information about AMISYS Advance, MemberConnect, and ProviderConnect.

16.6.2 Use of OCR. Approximately 90% of all paper claims we receive can be indexed and converted into machine-readable data through the use of Optical Character Recognition (OCR). We use MACESS EXP Form Works OCR software to greatly enhance the speed at which our scanning staff index paper claims and the speed at which we produce machine readable data from the paper and fax claims we receive from providers. We encourage, train, and support our providers to move to electronic claims submission or to use standard "OCR friendly" red ink paper claim forms with typed or clearly written data, if a provider must use paper.

16.7 Electronic Messaging

Our electronic messaging standard is based on Microsoft products and will be fully compatible with existing DHH standards.

16.7.1 E-Mail with DHH. Centene's continuously available electronic mail system is based on Microsoft Exchange 2007, with secure gateway connection to the internet for email correspondence with any external party, such as DHH. Our current email client standard is Microsoft Outlook 2010, which is functionally compatible with Outlook 2007 (DHH's current standard). Because our office productivity standard is Microsoft Office 2010, Centene and LHC users will be able to exchange emails and attached documents with DHH that are compatible with DHH's Microsoft Office 2007 standard.

16.7.2 VPN As Needed. If needed, we will establish a Virtual Private Network with DHH or a DHH designated entity. We can and do support VPNs with our state clients or their intermediaries when necessary. We implement VPNs with Cisco ASA 5500 Series Adaptive Security Appliances for maximum authorized concurrent usage populations and hardware redundancy for VPN availability. We also use Symantec On-Demand Protection software for additional security with our VPN and secure web applications, to eliminate malware, clear cache history, and systematically enforce connection security policies.

16.7.3 Secure E-Mail. Centene supports several email encryption methods for secure communications, all of which are compliant with HIPAA and Sarbanes Oxley (SOX) rules and regulations. Centene's primary method for securing email communication between systems, sites, and/or domains is Transport Layer Security (TLS). TLS is an industry standard protocol for securing electronic communication and is designed to prevent eavesdropping, tampering, and message forgery. TLS also supports endpoint authentication and communications privacy using digital certificates.

Centene's messaging systems also support industry standard email and web encryption protocols, such as S/MIME and SSL. Centene has deployed Cisco's IronPort email security and encryption appliances at the network perimeter, which provide a seamless and integrated means to send encrypted emails to external parties. Centene also supports PGP Workgroup and third-party digital certificates for email encryption and HIPAA compliance where required.

16.8 Eligibility and Enrollment Data Exchange

16.8.1 Enrollment File Processing. Today we process inbound HIPAA 834 transactions on a daily, semi-monthly, and monthly basis from our state clients, their FI or enrollment broker (EB), and in accordance with companion guide specifications per state, FI, or EB. We can accommodate any 834 transaction schedules desired by DHH. We receive and transmit HIPAA 834 transaction files via our secure file exchange management system, Coviant Diplomat (Coviant). Our TIDAL job scheduling software manages member load processes for overall process integrity. Inbound 834 files are automatically processed through our EDIFECS EDI system for HIPAA 4010A and 5010 compliance validation and translation. EDIFECS, in conjunction with our TIBCO middleware, also edits for duplicate member records, date criteria validity, field data integrity, and valid date spans. Any member records, that trigger edits, default into an Exception Report where they are systematically corrected using data correction routines prior to subsequent processing.

We will process HIPAA 834 files from DHH's EB through our EDIFECS system using HIPAA 5010 compliance checks for go-live on January 1, 2012, and will load this data into our MRM member data management system through "Add, Delete, and Modify transactions" with accurate begin and end dates. MRM is our "system of record" and master data store for "all things member" related, including demographic (including identifiers, address and contact information, confirmed or potential family linkages, special needs, and numerous other attributes), administrative, and member preferences (e.g. communication options such as e-mail, phone, mail), along with history for these attributes. MRM houses our master member index (MMI), an internal global member identifier, similar to a master patient index, to tie together alternate or historic member identifiers, and allows us to systematically link information about the member across that member's relationships with us or DHH, or prior health coverage spans (where we have such history). Once member data populates MRM, it is systematically promulgated to our other systems, including (via TIBCO middleware) AMISYS Advance, our core claims processing system, our TruCare integrated health services management platform; our MACESS EXP paper scanning and MACESS FormWorks Optical Character Recognition (OCR) system; our Automatic Work Distribution (AWD) claims workflow engine; and our Enterprise Data Warehouse (EDW) data integration engine via our Informatica near real-time Extract, Transport, and Load (ETL) middleware. Through EDW, we also make member eligibility data securely accessible to our providers online via our Provider Portal.

We securely transmit member eligibility data to any subcontractors we are working with for a particular plan. For LHC, we will send this eligibility data to OptiCare Managed Vision® (OptiCare), LHC's affiliated vision benefits subsidiary and subcontractor. Our MRM can maintain LHC's member historical data indefinitely, subject to DHH retention requirements.

16.8.2 Database Update within 24 Hours. We process and update all eligibility and enrollment data we receive to our production databases within 24 hours or less of receipt. Our ability to meet this processing turnaround time is due to the automated workflow and interface capabilities we have designed and configured in our integrated Coviant, EDIFECS, TIBCO, MRM, and AMISYS Advance systems.

16.8.3 Member Information Changes to DHH. Today we support the ability to send member demographic changes, such as changes in address or telephone number, to any of our state clients who request this information. We support HIPAA 834 formats for this purpose and can also accommodate a state, FI, or EB proprietary format.

We efficiently capture member demographic changes via our MemberConnect contact relationship management (CRM) system. Our Member Services Representatives (MSRs) can enter new member contact information in fields that do not overwrite the information we have received from the state, FI or EB. This enables us to maintain data integrity, keeping data issued to us by the state logically separated from self-reported information from the member. Members can also record demographic changes via our secure Member Portal, and we can integrate this information with any updates recorded through MemberConnect into one consolidated member information change file for use by the state or the state's FI or EB.

In short, our Master Data Management (MDM) approach to member data integrity allows us to collect member data updates no matter how we become aware of that information: via phone call from the member, via secure messaging, via the web, via mail or fax, or, of course, via the HIPAA 834 from DHH's EB. Because we design our member data structures to ensure clear definitional attributes as to where member demographics originated (for example, the member or DHH's EB), we can maintain the integrity and auditability of member demographic information, along with history of these attribute changes.

16.8.4 Unique Member Identification. Based on Microsoft Dynamics and SQL/Server technology, MRM is our one integrated repository of "all things member" and has *three integrated components*:

- ***Member Demographics System:*** MDS is similar in design to a Master Patient Index application because it employs an MDM approach to member data. Our MDM design provides processes for collecting, aggregating, matching, consolidating, quality-assuring, persisting, and distributing member data throughout our organization to ensure consistency and control in the ongoing maintenance and application use of member data.
- ***MemberConnect:*** Our inbound member contact/query management application for use by our Member Services Representatives.
- ***MemberReach:*** Automates, manages, tracks, and reports on workflows for outbound and outreach member campaigns, as well as targeted outbound interventions.

MDS maintains a master member identifier that links information we have on a unique member across multiple populations we manage, with history of prior identifiers. MDS is the "source of truth" for member data across all of the applications in our span of control and for our downstream subcontractors. We also use MDS in some states to identify and "tie together" members in a family and we can use the case identification information in DHH's eligibility data for this purpose.

16.8.5 Identify Duplicate Records. During the initial load process referenced above, using EDIFECS and TIBCO, we identify duplicate eligibility and enrollment records in a particular HIPAA 834 load file. These duplicate records are output on a load report and are worked by our Eligibility Specialists. If we confirm that the records are duplicates, we report this fact back to the state, FI, or EB using the manner prescribed by the state.

Multiple Identifiers for Same Person. When we load processed member records into MDS, we identify any potential duplicate members "at the person level," meaning the system looks for members (perhaps with different identifiers) who potentially may be the same person. Our Eligibility Specialists work these records as well, and once we confirm the correct identifier and demographics for a member with the state, MDS distributes the information to all our internal systems so that we systematically link claim records, clinical case management records, member service records, etc. to the corrected member identifier.

For example, should our Eligibilty Specialist identify two records with two different eligibility spans and two different Medicaid ID numbers, but where it is possible that the two records apply to the same person (e.g. name, address, date of birth), our Eligibility Specialist will validate this fact by working with the EB and other records we may have on the member, as well as possibly contacting the member directly to confirm that the multiple records are, in fact, one person. If we confirm that the records are for one person, we link those records to our master member index for that member in MDS, allowing us to consolidate history (e.g. claims) at the person level. Please see R.6 for more information on our capabilities to process eligibility and enrollment data for DHH.

16.9 Provider Enrollment

As we similarly do for several other affiliate health plans, Centene and LHC will use the published list of Louisiana Medicaid provider types, specialty, and sub-specialty codes in all provider data communications with DHH and the EB through the use of the *Portico* component of our **PRM** system. PRM is our next generation provider services inquiry and provider data management application, powered by Microsoft Dynamics contact relationship management (aka "CRM") software and our *Portico* enterprise provider data management system, as well as our Emptoris enterprise contracting system. PRM is integrated with our Provider Portal, Amisys Advance, our MACESS image retrieval system, and our Automatic Workflow Distribution (AWD) system.

Portico contains "all things provider" related information and is the "system of record" for provider data in our MIS (similar to the manner in which MDS is the system of record for member data), systematically distributing provider data where needed to other systems (e.g. fee schedule information to AMISYS Advance, demographic information to TruCare, and MRM). Portico can maintain multiple identifiers, specialty and sub-specialty codes for individual providers, and we will configure Portico with the codes specified by DHH.

16.9.1 Provider Data, 16.9.2 Provider Ownership. We will convey the following in a transmission method, format, and frequency that DHH specifies:

- Provider name, address, licensing information, Tax ID Number, National Provider Identifier (NPI), taxonomy, and payment information
- All relevant provider ownership information as prescribed by DHH, federal, or state laws

We maintain the integrity of the above data in the Portico component of our PRM system. In Q4 2011, we are enhancing our provider data quality controls through Enclarity, Inc. (Enclarity). Enclarity is a recognized national leader in provider data quality services and we will use Enclarity's nationwide database of current and accurate provider data to regularly validate all aspects of our provider data related to demographics, licensure, and specialty. Please see Section R.6 for more information.

16.9.3 Provider Exclusion Checks. Centene's Provider Network Management Department, in conjunction with LHC staff, will perform all federal and state mandated exclusion background checks on provider owners and managers, as part of our normal credentialing and re-credentialing process.

Our credentialing process includes primary source verification as well as systematic scans for reported, sanctionable actions through our Enclarity service, as well as our use of data from the Council for Affordable Quality Healthcare® (CAQH), the US Department of Health and Human Services (including the National Practitioner Databank), the Center of Medicare and Medicaid Services (CMS) Office of Inspector General (OIG), and available state databases.

We maintain the results of these exclusion background checks in Portico, and we can include this information to DHH via a transmission method, format, and frequency that DHH specifies.

16.9.4 Provider Enrollment Functionality. Please refer to the table below for a description of how our PRM system, including Portico and our other PRM modules, support the requirements of Section 16.9.4.

Requirement	How We Support The Requirement
Audit trail and history of changes made to the master provider data	Portico supports full audit trail and history tracking by electronically stamping the effective date of provider data transactions, enabling full historic audit trail support.
Automated interfaces with all licensing and medical boards	Automated interfaces are supported via Enclarity's provider data service.
Automated alerts when provider licenses are nearing expiration	As part of our PRM system, Portico maintains licensure dates and alerts LHC staff when a provider's licensure is nearing expiration and via our ProviderConnect, provider services application, alerts our Provider Services Representative (PSR) for potential follow up or to remind the provider when they contact our provider call center
Retention of NPI requirements	The Portico data management subsystem of our PRM fully supports NPI capture, storage, and administration.
System generated letters to providers when their licenses are nearing expiration	As part of our PRM system, Portico maintains licensure dates and, leveraging these dates, we will deploy a monthly process whereby providers nearing a licensure expiration date will be notified via the ProviderReach integrated outbound provider campaign module of our PRM. ProviderReach will notify providers nearing licensure expiration via automated email, letter, or Predictive Auto Dialer (PAD) notification using our Avaya Voice Portal, depending on the provider's preference.
Linkages of individual providers to groups	Many-to- many linkages and affiliations between individual providers and provider groups are fully supported in Portico.
Credentialing information	We support a very wide variety of credentialing information in Portico, including support for all credentials obtained through primary source verification.
Provider office hours	Fully supported in Portico.
Provider languages spoken	Fully supported in Portico.

In addition to the above, our Portico system supports provider prospecting and recruitment processes, support for multiple provider locations and location contacts, and support for multiple individual level provider service locations.

16.10 Information Systems Availability

16.10.1 CCN Span Of Control. Centene and LHC will be responsible for the availability and performance of systems and IT infrastructure technologies in our span of control. This includes the hardware, software, and communication lines in and out of our MIS in all our installations, including our St. Louis datacenter, and all hardware and software in our LHC offices. Our span of control also includes our enterprise Wide Area Network (WAN) and the Local Area Networks (LANs) attached to our WAN and installed at LHC offices. Centene and LHC will not be responsible for the availability and performance of systems and IT infrastructure technologies outside of our span of control.

16.10.2 DHH Access. We will allow DHH personnel, agents of the Louisiana Attorney General's Office (AG), or individuals authorized by DHH or the AG direct access to its data for the purpose of data mining and review. We will provision secure accounts for these authorized personnel, and implement our two factor authentication controls for these users. Please see Section 16.14.10 below for a description of our two factor authentication controls, as well as Question R.16+. We will offer access for authorized DHH and AG personnel to our secure web based SAP BusinessObjects Enterprise Suite of business intelligence and reporting facilities.

16.10.3 Critical System Availability. Today our Avaya Voice Portal Interactive Voice Response Unit (IVR) and all of our external internet websites, including our secure Member and Provider portals, are available 24/7. We will maintain this level of service for LHC's CCN-P Program. Should we identify a need to schedule unavailability of these systems, we will consult with DHH and only implement scheduled unavailability with DHH's agreement.

16.10.4 Other System Availability. Outside of our IVR, internet websites, and email system, our other MIS functions are scheduled available for online use from 7AM to 7PM, Central Time, Monday through Friday. In fact, availability is typically well beyond these hours depending on night production batch cycle loads and system maintenance.

16.10.5 FI and Enrollment Broker Data Exchange Availability. All of our production systems, including our systems supporting data exchanges with our state clients and FI, as well as the LHC offices, are monitored 24/7/365 for service availability, system performance, and capacity utilization. We use Hewlett-Packards OpenView Operations®, Solarwinds, Cascade and Fluke's Visual Performance Monitor to systematically oversee system availability. Fluke Visual Probes monitor network performance and utilization of the connections to our corporate datacenters. If we experience a system or network service failure, *a notice is automatically sent to our central monitoring station and is reviewed by our Network Operations Center (NOC)*.

Applications and service-level monitoring is provided by our HP Business Availability Center (BAC) and CA Wily Introscope software. HP BAC software probes are strategically placed and emulate client access to business-critical applications. These probes provide metrics that assist in the prediction, isolation, and diagnosis of application events. In addition, the probes provide data that aid in capacity planning, performance measurement, and service level reporting activities. Introscope runs on our web application servers and enables visibility into complex transactions for our end-to-end application performance monitoring. For example, we use it today to monitor adherence to our performance Service Level Agreement (SLA) for another of Centene's state clients. These automated controls ensure that all of our systems, including the systems and processes within our span of control associated with our data exchanges with DHH's FI and/or EB and its contractors, will be available and operational. Please see R.3 for more information on the availability of our MIS and the controls in place we use to maintain availability.

16.10.6 Core Eligibility/Enrollment and Claims System. Centene has a complete, annually tested and refreshed Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to cover all aspects of production MIS applications, including our core eligibility, enrollment and claims system. Although these plans have a maximum timeframe of 72 hours for a return to online operations, our target is to restore all centralized MIS operations and applications, including core eligibility, enrollment and claims processing systems, to be back on line within 12 hours of a site or systems disabling event.

In Q4 2011, we will complete construction of our new, Tier 3, 19,000 square foot datacenter, with capacity for over 165 IT racks; 6,000 square feet of datacenter floor; and fully redundant environmental, power, and network connectivity systems. Our new datacenter has a seismic importance factor of 1.5 (fully operational following an earthquake) and is rated to withstand winds up to 165 MPH (an F3 tornado). *Beginning inQ1 2012*, we will operate our two datacenters as mutual "hot site" backups whereby each datacenter will be able to assume operation of critical production systems if the other datacenter becomes inoperable, within *seconds* of a site disabling outage. Please see M.1 and R.3 for a detailed description of our BCP and DRP.

16.10.7 Problem Identification. We will notify designated DHH staff via phone, fax, and/or electronic mail within 60 minutes upon discovery of a problem, within or outside our span of control, that may jeopardize or is jeopardizing availability and performance of critical systems functions and the availability of critical information, including any problems impacting scheduled exchanges of data

between LHC and DHH or DHH's FI. In our notification, we will explain in detail the impact to critical path processes, such as enrollment management and encounter submission processes.

Our Service Desk and Network Operations Center (NOC) uses our ServiceNow helpdesk ticketing management system to capture, track, and manage any reported MIS related incidents. In addition to the notices discussed above, our ServiceNow system will *systematically* notify designated, authorized DHH staff via automated e-mail incident acknowledgements, alerts, and updates. For example, any DHH user that calls in an incident will automatically receive notification that their incident has been logged, then another notification when the incident is being worked, then another when it is resolved, etc.

Service-Now also allows our ServiceDesk and NOC to send an email to any DHH email address from within the ticket. That information is saved within the ServiceNow's Activity Log for tracking, auditing, and continuous service monitoring purposes.

16.10.8 Problem Notification for DHH Users and Reports. We will notify designated DHH staff via phone, fax, and/or electronic mail within 15 minutes upon discovery of a problem that results in delays in report distribution or problems in online access to critical systems functions and information during a business day, in order for the applicable work activities to be rescheduled or handled based on our MIS unavailability protocol. As noted above, our ServiceNow system will support systematic notifications to DHH, in addition to phone and fax notifications.

16.10.9 System Unavailability Event Information. We will provide information on system unavailability events, as well as status updates on problem resolution, to appropriate DHH staff. At a minimum these updates will be provided on an hourly basis and made available via phone and/or electronic mail. As noted above, our ServiceNow system will support systematic notifications to DHH, in addition to phone notifications.

16.10.10 System Restoration. We will resolve and implement MIS restoration within 60 minutes of official declaration of unscheduled MIS unavailability of critical functions caused by the failure of any system and telecommunications technologies within the our span of control. Unscheduled system unavailability to all other MIS functions caused by system and telecommunications technologies within our span of control shall be resolved, and the restoration of services implemented, within eight hours of the official declaration of MIS unavailability.

Cumulative Systems unavailability caused by systems and/or MIS infrastructure technologies within our span of control will not exceed 12 hours during any continuous 20 business day period. In fact, in 2010, we experienced no instances of cumulative 12 hour unscheduled outages during any 20 business day period. Further, we experienced less than 28 hours of unscheduled outages during ***all*** of 2010.

16.10.11 Corrective Action Plan. Should we experience a problem with system availability, we will provide DHH with full written documentation that includes a corrective action plan describing how the CCN will prevent the problem from reoccurring. We use our ServiceNow helpdesk and incident management system to capture all aspects of problem identification, diagnosis, resolution, and follow up, which will serve as an important ingredient to any post incident documentation.

16.11 Contingency Plan

16.11.1 and 16.11.2- Contingency Plan, DRP, BCP. Centene and LHC will be jointly responsible for LHC's contingency plans to protect the availability, integrity, and security of data during unexpected failures or disasters and allow the continuance of critical application or systems functions during these events. These contingency plans are part of our integrated and coordinated BCP and DRP.

Every local plan in Centene's organization has a BCP and DRP, formulated and tested in coordination with Centene's Director of Business Continuity. From a data protection perspective, LHC's data availability, integrity, confidentiality, and security is protected and enforced by Centene-administered IT fault tolerant architecture, safeguards, controls, policies, as well as ongoing Centene and LHC testing, and employee training and certification. Depending on the situation, LHC's contingency plan may be invoked

by LHC's Business Continuity Planning and Emergency Coordinator (PCP/EC), LHC's Information Management and Systems Director, or Centene's Chief Information Security Officer or Chief Information Officer, or other qualified Centene or LHC senior management. Please see M.1and R.3 for more information on our contingency plans, BCP, and DR/DP.

Our MIS employs database clustering, server virtualization, RAID 5 storage, multiple path communications networking, hardware fault tolerance, automated system monitoring tools, and other technologies and controls to ensure data availability and security. Please see Section R.3 for more information on the availability and reliability aspects of our MIS. We use automated controls and safeguards to ensure data security, and validation edits, error correction routines, and industry standard database communication protocols to protect and assure data integrity. Please see Section R.4 for more information on our data integrity architecture and R.16 for more information on our security controls.

16.11.3 Contingency Plan Due Date. We will submit our LHC Contingency Plan to DHH for approval no later than 30 days from the date the CCN Contract is signed. We have honored similar ongoing commitments from our state clients throughout the nation since we began operations in 1984.

16.11.4 Contingency Plan Scenarios. Our BCP and DRP and associated policies and procedures cover these scenarios:

- **A site-disabling event** (including destruction) of our central computer installation in St. Louis, Missouri, including the recovery of all critical business systems within 72 hours. This recovery timeframe will be dramatically shortened in 2012. In Q4 2011, we will open our second enterprise datacenter and, beginning in Q1 2012, we will operate our two datacenters as mutual "hot site" backups whereby each datacenter will be able to assume, within *seconds* of a site disabling outage, operation of the critical production systems of the other datacenter.
- A system interruption or failure resulting from network, operating hardware, software, or operations errors that **compromises the integrity of transactions** that are active in a live system at the time of the outage. We document *database transaction* recovery policies and procedures for our MIS operations staff to follow depending on the specific situation. For example, depending on the nature of the interruption or failure, we can either roll back a transaction in the production database or roll forward using transaction journaling.
- A system interruption or failure resulting from network, operating hardware, software, or operations errors that **compromises the integrity of data** maintained in a live or archival system. Our *data recovery* procedures, which we test regularly, cover such scenarios. Through our Tivoli Storage Management (TSM) system, we can restore affected data rapidly and, if needed, retrieve backup data stored off-site from our vendor, Recall, via a secure web interface to quickly request that data.
- A system interruption or failure resulting from network, operating hardware, software, or operational errors that does not compromise the integrity of transactions or data maintained in a live or archival system, but does **prevent access to the system**. In these situations, our procedures document the appropriate near term actions, which include problem identification procedures and end user communications for ongoing status reports.

Our Service Desk and Network Operating Center (NOC) play a key role in all of the above scenarios. The NOC tracks the severity of the scenario incident and is the coordination point for all status and recovery activities - for the above and all other scenarios that might materially impact data availability, integrity, and security. Both our BCP and DRP include projected recovery times and potential data impacts, informed by our annual MIS Risk Assessment. Please see 16.4.11 above.

16.11.5 Contingency Plan Testing. All departments and Senior Management participate in an annual formal review of our entire BCP program, which includes a read through of current plans, an update of all materials, and a read through of the final plan after all changes have been made. We use every review and exercise as an opportunity to train and retrain Centene and LHC employees regarding roles and responsibilities. Under the guidance of our Centene BCP team (led by the Centene Director of Business

Continuity, LHC offices will also participate in annual desktop mock (or scenario) disaster exercises to further prepare for (and mitigate the impacts of) unforeseen events such as pandemic, or other natural or man-made disasters that might impact LHC and the delivery of care. Our program focuses on engaging management and employees in planning, as well as training, on pre-defined and pre-assigned responsibilities in emergency conditions. Additional BCP changes are made based on the scenario exercise to ensure the plan reflects the ideal response to an event. Crisis events, which include man-made, disaster or epidemic events, are used for annual scenario-based exercises.

In addition to the annual refresh and testing of our BCP, we conduct annual full-scale testing of our recovery capabilities by simulating the complete destruction of Centene's primary data center. As part of this exercise, we perform an annual "Hot-Site" information technology test, also known as a disaster recovery (DR) exercise. Historically, Centene has tested its ability to recover critical MIS capabilities by conducting a full-scale planned exercise using our third party vendor, SunGard. We make the results of our Disaster Recovery exercise available to each of our health plan compliance offers and to our state partners on request, and will offer the same to DHH. We look forward to sharing this information with DHH and answer any questions DHH may have. Please see M.2 for more information on our BCP and DRP annual tests.

16.11.6 Contingency Plan Corrective Action Plan. As mentioned above, both Centene and LHC view our annual contingency plan reviews, refresh, updates, tests, and training as an ongoing opportunity to improve and enhance our ability to ensure continuous operations, including the safeguarding of data integrity, availability, and security. In the event that we fail to demonstrate through our BCP and DRP tests that we can restore MIS functions, we will submit a corrective action plan to DHH describing how the failure shall be resolved within ten business days of the conclusion of the test.

16.12 Off Site Storage and Remote Back-up

16.12.1 Information To Back Up. We perform backups nightly of relatively static data, such as network file shares. More volatile data, such as database logs, are backed up at a greater frequency dictated by the speed in which the data is changing. With the completion of Centene’s second datacenter in Q4 20ll, backup service levels will be enhanced such that all changes to data on Centene systems will be replicated near real-time to the second datacenter. We use Tivoli Storage Manager (TSM for both Enterprise backup and recovery operations. As part of these backup services, all production systems are backed up daily and replicated to an off-site storage facility through our vendor, Recall, in addition to a disaster recovery site hosted for us by SunGard Availability Services. In the event of a disaster, Centene can recover data and operate production systems from the off-site storage facility and disaster recovery site. Even though data is replicated to an offsite disaster recovery site, Centene stores backup tapes with historical data in an off-site storage facility. Access to these tapes is restricted to individuals authorized by management. Data recoverability is tested on a regular basis by fulfilling restore requests. Full system recovery is tested yearly during an annual Disaster Recovery test.

We also store in our off-site facility current versions off all system operating instructions, procedures, reference files, system documentation, and, as noted above, operational files. Using Recall's secure ReQuest Web service, authorized Centene and LHC staff have complete visibility into where our stored documents are at any time. We can also request storage services (e.g. pick/up), check status, and even retrieve an electronic copy of our physical documents via image via Recall's ReQuest service.

16.12.2 Data Back-Up Policy and Procedures. Our data backup policies and procedures are reviewed annually by our Chief Information Security Officer and are published on Centene's intranet, CNET. Our policies and procedures include documentation on controls for backup processing, including how frequently backups occur; backup procedures; the location of data that has been backed up off-site; the identification and description of what is being backed up as part of our backup plan; and any changes in backup procedures in relation to the enhancements to our MIS or the addition of new backup services or

facilities. For example, in Q4 2011, we will go live with a second major datacenter installation and will modify our backup policies and procedures documentation to reflect this major enhancement.

16.12.3 Back-up File List. We maintain a current list of all files that we backup to remote sites, which we will provide to DHH, including the frequency with which these files are updated.

16.13 Records Retention

16.13.1 Document Retention Periods and Retrieval Requirements. Centene and LHC can fully support DHH's requirements for document retention. Any and all records, whether originated as electronic data (e.g. EDI or data entry) or paper and subsequently scanned to image by Centene and LHC, will be kept in accordance to DHH's specific retention schedule. As with all Centene plans, LHC will designate a records coordinator who will manage the retention schedule for LHC's CCN Program, in conjunction with our Centene IT Security Department and Compliance Officer.

We will keep LHC data online for six years, with the exception of claims data related to DHH specified "once in a life-time," per DHH's procedure formulary file, which we will not archive or purge from online storage. All of our production applications are capable of housing data for six years or beyond this timeframe if needed, including our AMISYS Advance claims processing system; our TruCare clinical care management system; our MRM and PRM system for member and provider service support and centralized member and provider data management, respectively; and our Centelligence™ data warehouse, health informatics and reporting system.

Today we also scan and index paper records, including paper claims, as well as member and provider correspondence related to those claims or to provider authorization requests, through our MACESS EXP Imaging and FormWorks system. LHC and Centene staff can then access scanned documents online, which can be accessed by internal claim control number (ICN) or member or provider identifier search arguments.

In addition, our Zasio Versatile Enterprise™ system will enable LHC to electronically scan, store, and manage other day-to-day paper records, such as legal and confidential documents. As with all our online imaged documents, we house Zasio stored images in our secure corporate datacenter; and as with all our local health plan offices, Centene will partner with an offsite records management vendor in Louisiana (such as Recall or Iron Mountain) for offsite storage of paper when originals are required to be kept for any period of time. All data and scanned paper images records are kept in archive indefinitely, unless LHC needs to have them destroyed, per specific DHH compliance guidelines.

Centene’s Corporate Ethics and Compliance Department will train LHC's records coordinators, per specific DHH requirements, and Centene’s Corporate Records Coordinator will conduct periodic reviews of LHC's internal practices.

Responsive Records Retrieval. Authorized LHC staff will have instantaneous access to six years of data online, including scanned paper images. We will archive data records older than six years to secure offsite locations. When an audit is in progress or audit findings are unresolved, records shall be kept until the audit is closed or until all issues are finally resolved, whichever is later. We will retrieve any LHC records or data requested by authorized agencies from our LHC offices in Louisiana. Alternatively, we will promptly respond to any authorized written or telephonic requests for information, once we verify that the requester is authorized to receive the information. Centene and LHC will provide a dedicated telephone number for DHH to use to directly contact LHC offices in Louisiana, to help ensure our responsiveness to DHH record requests. We will track and manage all records requests (written or oral) in our Compliance 360 corporate governance, risk management and compliance system. Compliance 360 allows us to organize and manage any type of audit related project, including record requests, across our organization, so that Centene and LHC can support record retrieval requests in a timely, efficient, and compliant manner. If requested records are available online in our MIS, we can retrieve the information instantly through our Centelligence™ Enterprise Data Warehouse (EDW), which houses all of our core transactional service records and our online imaging applications that contain indexed images of scanned

paper records, including claims, contracts, and other LHC information. We can retrieve archived records (e.g. 6 to 10 years old) within 72 hours or less. LHC will provide requested records in electronic format, on paper, or by fax to a secure location, at DHH's direction.

16.13.2 Encounter Data Retention. Our MDE Xpress Encounter Pro (Encounter Pro) system is integrated with our MIS, including our AMISYS Advance claims system and EDW data warehouse, and provides the automated production and ongoing management tools needed for our encounter submission process. We can and will retain online access to LHC encounter data in Encounter Pro for six years, as we do with other Centene health plans today.

16.13.3 Audit Trail Retention. We can, and do, retain audit trails for all of our production systems, including AMISYS Advance, MRM, PRM, Centelligence™ (including EDW), and TruCare. Archived audit trails, which are initially kept in online storage for 6 years, can be retrieved within 48 hours upon request.

16.14 Information Security and Access Management

16.14.1 Access Management.

Role Based Access Controls. Centene enforces strict control over global application and systems access via a series of interconnected technical and administrative controls. In particular, we implement Role Based Access Controls (RBACs) throughout our MIS so data can only be accessed, created, or changed by those who have the authority to do so, and in compliance with HIPAA Minimum Necessary rules. Our RBAC provides auditing support and serves as a strong basis for separation of duties while simplifying security administration by assigning privileges to a role (as opposed to a user) and then assigning role(s) to users. In addition, RBAC addresses security risks by defining employee access rights based on the employee's job functions or responsibilities and eliminates problems inherent with assigning access rights on an individual basis.

On the **technical** side, we have implemented RBAC such that the individuals responsible for *provisioning* application access, to AMISYS Advance (our enrollment, eligibility, and claims processing application) for example, are not themselves members of roles that have rights to *perform transactions* within those applications. Furthermore, our monitoring regimen mitigates the risk of security personnel modifying their own roles, or provisioning new roles for themselves, by logging all changes to access, issuing privileged access reports for periodic review by application owners, and by notifying oversight personnel when there are any changes to highly privileged administrative roles.

On the **administrative** side, we enforce separation of duties such that the individuals that provision front-end access to the network and core applications do not have rights to provision access to crucial *back-end* components such as our Business Objects reporting application and our Enterprise Data Warehouse (EDW); and the reverse is also true. Likewise, individuals provisioning access to our network do *not* have rights to provision physical access to the areas where systems are housed (e.g. to physical servers). In addition, we document and enforce access control policy that explicitly defines role limitations and access review requirements for applications in our environment. For example, our access control policy for AMISYS Advance requires that the system be audited monthly to ensure that no single role, or no combination of roles granted to a single user, has rights to setup a member or provider and process a claim.

We administer RBAC by tasking department managers to define the functions and access rights (roles) their employees need to accomplish their jobs. We then map each job function or position to a set of responsibilities associated with that job function and to a collection of work roles and security RBAC profiles. Centene's IT Security Department conducts Role Based Access Control (RBAC) tests and audits to ensure application access has been appropriately provisioned. Our MIS security staff may, depending upon an employee’s job responsibilities, expand, limit, or eliminate that employee's access to Protected Health Information (PHI) or other information at any time. In addition, a Centene Security Officer must

approve an employee's access to information if that access request is not part of a standard security profile commensurate with the normal responsibilities of the employee's position. Depending on the type of access being requested, the Centene Security Officer or LHC Information Management and Systems Director must obtain the approval and sign-off from the appropriate functional vice president.
RBAC controls are present in all of our core business systems, including AMISYS Advance (claims processing), TruCare (clinical care management), Centelligence (reporting, business intelligence, and healthcare informatics), and our member and provider service management applications, MRM and PRM. With respect to user logins, password length, complexity, and lifetime are systematically controlled to ensure they cannot be easily compromised, and users are forced to change passwords every 42 days. Inactive PC workstations are automatically locked and after three failed login attempts, users are locked out and these attempts are logged. Our IT system administrators maintain an incident reporting and follow-up file providing the date, time, and comments regarding any unauthorized attempts.

16.14.2 System Information Access by DHH. We will enable access for duly authorized representatives of DHH and other state and federal agencies to evaluate, through inspections or other means, the quality, appropriateness, and timeliness of services LHC performs, which we can accommodate through site visits to any of our LHC field offices or Centene's corporate datacenter in St. Louis, Missouri; secure WebEx; or secure remote access to authorized DHH personnel, depending on the need.

16.14.3 Integrity Controls. Our MIS incorporates several types of controls to maintain information integrity, depending on the data processing, transmission, receipt, or storage application. Our controls are tested both via ongoing processes (such as edit enforcement routines for data load processes), via our own internal spot audits, and via several external audits, including our annual SAS/70 Type II and Sarbanes-Oxley Section 404 Management Controls audits.

For data exchanges with external entities (e.g. our state clients, their FIs or EBs), we use Public Key Infrastructure (PKI) based protocols with public/private key exchanges to ensure data is not altered "in flight" and that sender and receiver are assured of each other's respective identity.

All of our online, transactional, and batch data interfaces and load processes have appropriate data validation logic to enforce data integrity properties such as:

- Codeset compliance with HIPAA, HL7, US Postal Service, and other standard code sets, for example. We also use check digit algorithms, such as with the National Provider Identifier's tenth digit, where available.
- Data validation through the comparison of key indices of inbound data with values we have stored, such as member and provider identifiers.
- Information completeness, which includes the enforcement of required, situational, and conditional fields on inbound or outbound data transmissions

All of our core and critical business systems are based on relational database management system (RDBMS) technology from Oracle, Microsoft (SQL/Server) and Teradata - and in all cases we enforce referential integrity, field types, and missing data edits.

Using Symantec's Control Compliance Suite (CCS), we monitor access to secured LAN folders and sub-folders containing critical data, identify changes made to documents stored in these folders, and enforce privacy and security policies on documents containing PHI.

16.14.4 Audit Trails. All core business applications in our MIS, including our applications for MRM and PRM, HIPAA transaction processing (EDIFECS and TIBCO), claims and encounter processing (AMISYS Advance and MDE Xpress Encounter Pro), case and utilization management (TruCare) and informatics (Centelligence™ Enterprise Data Warehouse and supporting applications) support audit logging and audit trails for data changes, allowing us to track activity in each of these business applications. In addition, our Informatica data integration middleware captures every data change in each of these core data systems in audit logs. We also use master data management (MDM) methodologies and controls with common "cross application" primary and foreign keys, allowing information on source data

files and documents to be traced through the processing stages to the point where the information is finally recorded. In particular:

- All online application interfaces for our core business systems capture and log unique log-on IDs and/or the device used to access the application ("terminal ID"), along with date and time of create/modify/delete actions. These audit capabilities are within the applications themselves, for example, our AMISYS Advance online application captures for our audit trails the log-on ID, date, time, and edit activity of the online user. AMISYS Advance also displays the last change date for claims data, on all online screens related to claims viewing by the online AMISYS Advance user. Similar capabilities exist in our other core applications, allowing the online user of these systems (e.g. MRM, PRM) to see when the last time transaction data was updated. Our core applications also capture and display batch process change activity, where those activities alter data. Our batch routines also produce audit trail data during the particular processing cycle.
- All core health plan data, including member, provider, claims, encounter, authorization, and health risk assessment data, can be traced throughout our MIS from the point of entry through the final information product and/or outbound transmission. We use appropriate indices to enable this capability. For example, we use member, provider, and ICN indices to associate a stored image of a paper claim - through our EDIFECS EDI system, through MACESS EXP (image storage), into AMISYS Advance (claims processing), through Centelligence™ (reporting), and MRM and PRM (member and provider services and data management), and Xpress Encounter Pro (encounter processing).
- All core business systems mentioned above produce listings, transaction reports, update reports, transaction logs, or error logs that serve as an audit trail of online, database transaction, batch file processing, and/or inbound or outbound transmission. For example, we have multiple batch processes that update our Centelligence™ Enterprise Data Warehouse (EDW). If an update process detects incomplete records or other data problems, this is written to an audit report and investigated by an EDW specialist in Centene's IT Department.

16.14.5 Prevent Alteration of Finalized Records. All of our core business applications, including TruCare (clinical care management), AMISYS Advance (enrollment, eligibility, claims processing), Member and Provider Relationship Management (MRM and PRM, for member and provider service management respectively), Xpress Encounter Pro (encounter processing) and Centelligence™ (business intelligence, reporting, and health informatics) do not allow the alteration of finalized records. For example, our TruCare system does not allow chronological clinical notes to be edited once those notes are written to the TruCare database. A TruCare user can add to historical notes (and these additions are time stamped and ID stamped) - but no TruCare user can "go back" and edit previously entered notes. Similarly, no AMISYS Advance user can alter finalized claims data. Adjustments and voids against finalized claims are possible, but no alteration is possible on the original, finalized claim record itself.

16.14.6 Physical Safeguards and 16.14.7 Perimeter Access Controls. The Centene corporate datacenter in St. Louis, Missouri, houses core data and voice communications systems securely connected via our internal WAN to our information technology assets located throughout local field offices, including LHC. Centene physically protects all core business application and telecommunications systems in our corporate datacenter with limited and strictly controlled access. We secure our Centene datacenter and all Centene corporate and health plan facilities, including LHC, via proximity card access by authorized personnel, on all external doors, elevators, and the internal entry doors on each floor. The Centene datacenter contains an additional layer of proximity card access restricting access to authorized personnel only. The local LHC server and network room will have a similar control. Additional physical security controls at our Centene datacenter include digital security cameras, multiple security guards who are on duty at all times, and panic switches installed at each reception desk.

We will provide DHH with access to our data facilities upon request. We require that every visitor to the Centene datacenter sign into the log book indicating the time, employee escort, and purpose of their

presence in the network room. We also require that visitors sign out when leaving the datacenter. Our card access system records all access attempts/card swipes whether successful or not. We also monitor and record access and movement using multiple cameras throughout the Datacenter, including all entry points into the Datacenter room. The Centene Director of Systems Services must authorize Centene Datacenter access requests and grants authorization on a need basis *only*. Our MIS staff require vendors performing services within the Centene Datacenter to sign in and be escorted into the facility by authorized personnel only. Each month, the Manager of Centene Datacenter Operations reviews the sign in log to ensure that physical access requests are approved only if appropriate. In addition, onsite security guards are on duty at all times at our Datacenter facility. The physical security provisions we have in place today will be in effect for the life of our Contract with DHH.

16.14.8 Physical Security Features.

Enterprise Class Physical Datacenters To Protect Data & Operations. The Centene datacenter houses all the hardware, systems, and application software furnished to our local health plan offices, including LHC's offices, field staff, providers, and members. The datacenter is equipped with redundant environmental systems for power, cooling, and humidity control. We execute a full power load test quarterly on our backup generators, switching all power loads to the generator to validate the generator's effectiveness. Less than 15 seconds is required to automatically switch to backup generator power resulting in no downtime for the IT infrastructure. A redundant chiller plant controls temperature and humidity levels and uses a highly efficient water-cooled system backed up by an air-cooled system in the event of loss of water to the facility. Our environmental systems are implemented as an N+1 design ensuring that the loss of any one unit does not affect our ability to maintain safe temperatures. All environmental systems are tied into Centene’s security system and send an audible remote alarm to our datacenter and security staff when temperature or humidity falls outside of predefined ranges or water is detected. A Very Early Smoke Detection System (VESDA) provides our datacenter with fire alert capabilities. Our VESDA takes air samples throughout the datacenter, sensing particulates that are present in the air prior to actual combustion. Our fire suppression system is an Ecaro-25 Clean Agent Fire Suppression System. A pre-action water sprinkler system provides a second level of protection. Safeguards are in place to minimize the risk of accidental discharge of both the clean-agent and sprinkler suppression systems.

Centene's Second Datacenter. In the 4th Quarter of 2011, we will complete construction of our new, Tier 3, 19,000 square foot datacenter, with capacity for over 165 IT racks; 6,000 square feet of datacenter floor; and fully redundant environmental, power, and network connectivity systems. Our new datacenter has a seismic importance factor of 1.5 (fully operational following an earthquake); is rated to withstand winds up to 165 MPH (an F3 tornado); and has all HIPAA compliant state of the art security measures. In the 1st Quarter of 2012, we will operate our two fully-redundant enterprise datacenters as mutual "*hot site*" backups. Each datacenter will have the capacity to assume operation of all **business critical** production systems if the other datacenter is rendered inoperable-within *seconds* of a site disabling outage:

- Fully redundant **networking infrastructure and circuits** between the two datacenter facilities will ensure that an outage by one of our telecommunications providers will not result in our systems being rendered unavailable.
- **Utility power** will flow into each datacenter facility via redundant, geographically diverse routes enabling continuous service even if one power feed is severed.
- **Battery backup systems** will be available to keep systems operational in the event of a wide-spread utility power outage.
- Each facility will be equipped with an on-premise **diesel generator** for prolonged power outages.

Please see R.16 for more information.

16.14.9 Network Access Controls.

Protecting Our Internal Network. Centene will provide LHC offices and field personnel users with internet access through our OC-3 circuit. The 155Mbps internet service is transported and terminated on a Cisco access router; connected to redundant corporate firewalls (Cisco 6500s with Firewall Switch Modules). Intrusion Detection Systems (IDS) are located in strategic locations within our trusted and untrusted segments to assist in the detection of security violation attempts. Centene uses Cisco IDS for network monitoring. IT staff monitor IDS logs daily and act on any unusual activity immediately. We use Rapid 7's Nexpose system to continuously assess our systems, software, devices, and processes against both a library of existing exploits and signatures for new or emerging exploits. Once a vulnerability is identified, it is categorized by risk and addressed accordingly using approaches such as vendor update, administrative control, custom development, or a compensating control, such as a new firewall rule.

We also have De-Militarized Zones (DMZs) to provide semi-trusted segments for Web Servers, Domain Name System (DNS) Servers, and Secure Access Gateways, thus isolating our internal applications from the internet. We provide remote access to Centene Corporation's network through a VPN using Cisco's VPN 3000 Concentrator and also through encrypted web access sessions using Citrix Secure Gateways.

Enhancing Security with IPS. In June 2011, we are further hardening our perimeter security with the deployment of Intrusion Prevention Security (IPS) technology from Sourcefire, Inc. Our Sourcefire Next-Generation IPS integrates real-time contextual awareness into the IPS' inspection. This IPS gathers information about our network and host configurations, applications and operating systems, user identity, and network behavior and traffic baselines. The utmost visibility of what is running on our network allows our Sourcefire system to offer event impact assessment, automated IPS tuning, and user identification. The emphasis is on shifting from intrusion *detection*, to intrusion **prevention.** Please see R.16 for more information.

16.14.10 Two Factor Authentication. ***Secure Remote Access.*** As a part of our commitment to the comprehensive implementation of information security best-practices, Centene and LHC will utilize award winning SecureAuth® *Identity Enforcement Platform (IEP)* software to provide secure multifactor authentication for LHC employees and partners, including DHH designated users that require remote access to Centene information systems.

IEP will be one of the core components on our defense-in-depth strategy ensuring that only authorized individuals are allowed remote access into our Cisco VPN, Microsoft Outlook Web Access, and Citrix published applications. In addition, the extensible and flexible nature of the IEP software allows it to be quickly integrated to protect any other applications that might be deployed in the service of LHC's Coordinated Care Network. Centene and LHC recognize that DHH must approve our approach to 2-factor authentication no later than 15 calendar days after the Contract award.

16.14.11 Security Risk Assessment. Centene conducts in-depth risk assessments and penetration tests of our MIS and key business processes on a regular basis; four such assessments were executed in 2010. Our security risk assessment activities include a mix of regularly scheduled assessments as well as periodic, on-demand, assessments necessitated by significant changes in the threat environment or specific requests by customers or business partners. These assessment activities are further augmented by our vulnerability management program, which includes the regular scanning of our MIS against both new and existing exploits and to verify continued regulatory compliance. In all cases, should material defects or weaknesses be discovered, they are prioritized based on risk, mitigated, and retested to validate resolution. Testing is performed using both internal resources and reputable third-party providers such as Ernst &Young, LLP, and ViaForensics. Centene's well-established Internal Audit Team, with independent validation from our third-party audit partner, Ernst and Young, oversee risk mitigation and management.

Centene and LHC will conduct a security risk assessment and communicate the results in an information security plan to be provided no later than 15 calendar days after the Contract award, with the risk assessment made available to appropriate federal agencies.

16.15 Audit Requirements

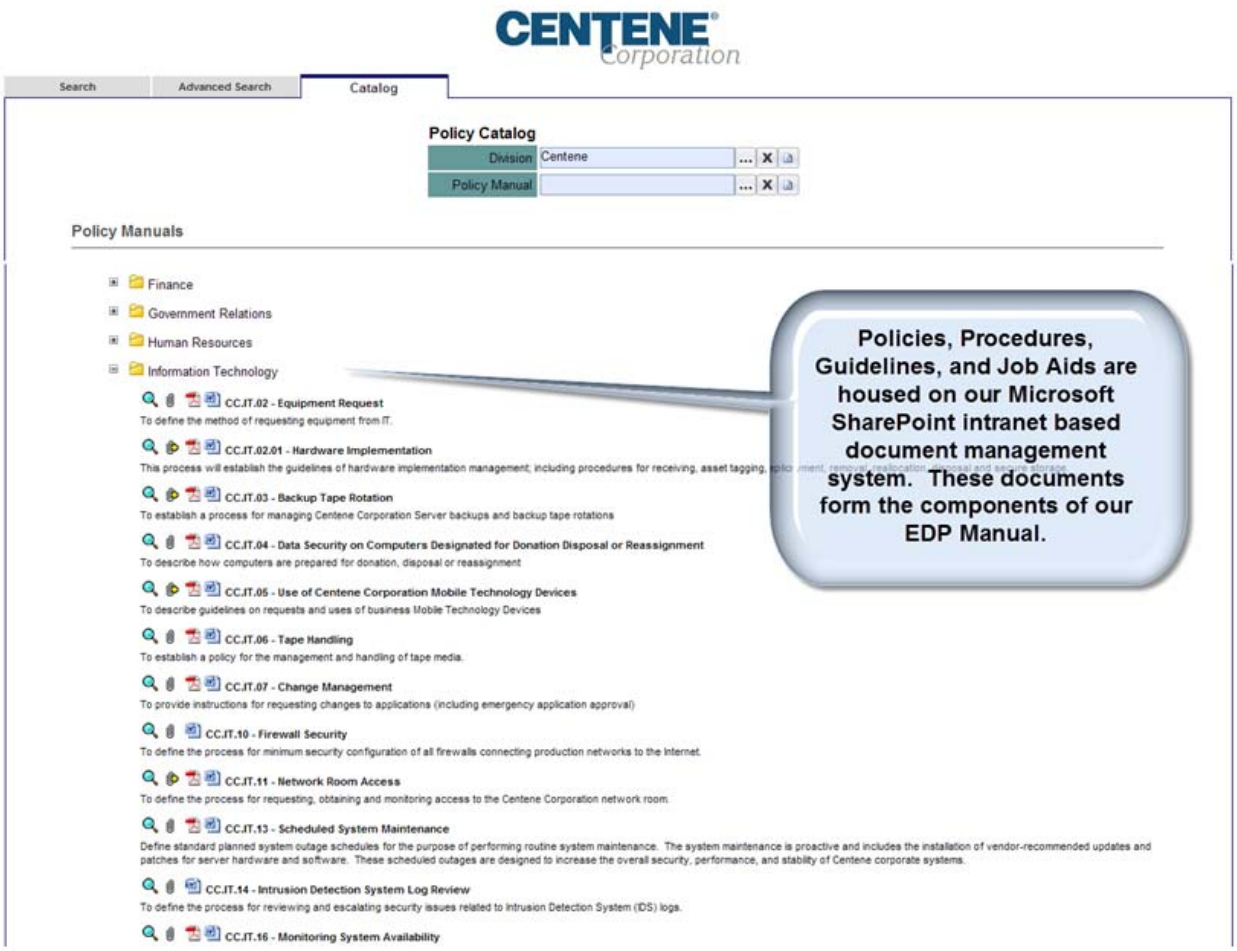
16.15.1 Audit Trail for Claims. Our core claims processing system, AMISYS Advance, provides a comprehensive audit function with definable parameters to track all changes to any individual claim. AMISYS Advance creates a unique auditing record for every modification, including adjustments, to create a complete historical account of all changes. The system retains associated audit records for a claim or service for 90 days after resolution and may be readily accessed and used for auditing, tracking, and reporting. We use unique claim identifiers to track claims from original submission through to payment and encounter reporting. AMISYS Advance, along with our EDIFECS EDI system, and MACESS OCR imaging system, follow the objectives of the American Institute of Certified Public Accountants (AICPA) Audit and Account Guide and The Auditor's Study and Evaluation of Internal Control in Electronic Data Processing (EDP) Systems. Our SAS/70 Type II auditor, KPMG, LLC, audits our claims processing and data center operations annually in accordance with standards established by the American Institute of Certified Public Accountants.

16.15.2 EDP Policy and Procedures Manual. The components of our EDP Policy and Procedures manual materials (EDP manual) are housed on our internal Microsoft SharePoint system, and incorporates our disciplined approach to application development and maintenance; user interface standards; security standards and policies; change and release management; and unit, system, user acceptance, and post production testing.

Both the Agile Software Development Life Cycle process and the Information Technology Infrastructure Library (ITIL) process framework inform our EDP documentation. Centene follows an Agile process to deliver higher quality software faster, while maintaining effective business controls. Agile is an industry best practice development and deployment cycle that has a collaborative and evolutionary approach with consistent outcomes in both quality and customer satisfaction. We have integrated the ITIL process framework into our IT organization and documentation. ITIL is a process based, best practice framework for delivering and managing MIS services. Centene requires MIS management to obtain certification in ITIL v3 and incorporate these practices into their service areas.

We house EDP documentation on our intranet and use Microsoft's SharePoint document management and library system to organize our documentation. We use SharePoint's library, version control, searching functionality, and other features to make our documentation easy to access and up to date. Please see ***Figure R.7-A: IT Documentation*** for an example screenshot of our SharePoint system.

Figure R.7-A: IT Documentation



16.16 State Audits

16.16.1 State Auditor Access. We are able to support state auditor written requests for files covering a specified accounting period during our Contract with DHH, in a wide variety of formats and media, including magnetic tapes, CD, or other media compatible with DHH and/or state auditor facilities, including secure email or secure FTP. Our LHC Compliance Officer will ensure that DHH and/or the state auditor is supplied with the information they need.

16.16.2 Correction Action Plan. Should the state audit result uncover material discrepancies or errors, we will provide a written corrective action plan to DHH within ten business days of our receipt of the audit report.

16.16.3 Integration of Audit Results into EDP. We will integrate any findings from a state audit into our EDP manual, documenting the date of these inclusions in the revision history of our EDP manual.

16.17 Independent Audit

Centene undergoes regular external audits related to our MIS and we agree to all requirements in Section 16.17.

16.17.1 Independent Auditor. We can, and currently do, support independent audits of our MIS and will be happy to review our existing audit plan with DHH. For example, in 2010, Centene engaged Ernst & Young for our annual Information Technology Risk Assessment to review Centene's IT risk profile/risk

universe and ensure that we had identified appropriate risks, the potential severity of those risks, and the likelihood of their occurrence and impact. Our IT risk profile is used in Centene's Enterprise Risk Management (ERM) process, which includes an ongoing review and assessment of Centene's risk environment with senior management.

We also engage external auditors for our annual Sarbanes Oxley Section 404 management control and SAS/70 Type II audits (see below).

Our Centene Director of IT Security works with our Centene Corporate Compliance Officers and local health plan Compliance Officer (e.g. LHC) to ensure that our auditors have full access to our operations, documentation, and systems for these audits.

16.17.2 Independent Audit Report. We will ensure that our auditing firm delivers to DHH the auditor's report of findings and recommendations within 30 calendar days of the close of each audit. As we do today, this report will be prepared in accordance with generally accepted auditing standards for EDP application reviews.

16.17.3 DHH Use of Audit Report. We recognize that DHH will use the findings and recommendations of each report as part of its monitoring process.

16.17.4 Audit Report Corrective Action Plan. Should an MIS audit result in a corrective action plan to address any deficiencies, we will deliver that action plan to DHH within ten business days of our receipt of the audit report, and will include the corresponding audit findings in our EDP manual, noting the date of these additions in the revision history of our EDP manual.

16.17.5 SAS 70. As a public company, Centene undergoes annual Sarbanes Oxley (SOX) Section 404 management control audits and an annual SAS/70 Type II audit, both performed by independent auditors. Ernst & Young, LLP performs our SOX audit and KPMG, LLP performs our SAS/70 Type II audits. Our SAS/70 audit is conducted according to American Institute of Certified Public Accountants (AICPA) Professional Standards for Reporting on the Processing of Transactions by Service Organizations. KPMG, LLP issued an unqualified opinion in Centene's most recent SAS 70 Type II audit, completed in 2010; and Ernst & Young, LLP also issued an unqualified opinion in our most recent SOX Section 404 audit (no material findings in either SAS/70 or SOX 404 audits).

Question R.8

Change Management and Version Control Processes

R.8 Describe your information systems change management and version control processes. In your description address your production control operations.

Managing Information System Changes and Modifications through Disciplined Processes and Automation

Louisiana Healthcare Connections (LHC), will use a Management Information System (MIS) designed to provide a comprehensive breadth of application functionality. Operating such an MIS demands self-documenting, auditable, yet efficient change order and software modification processes. We will be *responsive* to MIS change requests in **quick fashion**, yet *manage* these requests appropriately in terms of business need priority. Coordinating the timing of all changes via our software release strategy and impact on MIS performance is critical, keeping in mind the overall imperative of excellent service to DHH, our members, and providers.

In order for LHC to ensure that we have developed and continually maintain effective information systems controls (including effective system change controls), we utilize both internal audit (Ernst & Young) and external audit (KPMG) professionals to conduct a SAS 70 Type II audit. Statement on Auditing Standards No.70 (SAS 70) is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) in 1992. It is used to report on the "processing of transactions by service organizations," which can be accomplished by completing either a Type I or a Type II audit. A SAS 70 Type I is known as "reporting on controls placed in operation," while a SAS 70 Type II is known as "reporting on controls placed in operation" and "tests of operating effectiveness." Centene participates in the Type II audit the 4th quarter of each year. This ensures that we maintain the highest quality while enforcing the lowest risk to our production systems. In addition to the above formal audit, we utilize our own Internal Audit department to review our controls each quarter to validate both the quality of the control as well as the activities related to our controls.

We achieve a judicious balance of MIS change alacrity and careful change management control through:

- *Disciplined* identification and validation of required changes
- Industry *best practice* standards in:
  - Six Sigma Continuous Quality Improvement (CQI)
  - Software Development Life Cycle (SDLC) approach and controls
  - Agile rapid application development
  - Information Technology Infrastructure Library (ITIL) process framework
  - Our Enterprise Business Implementation (EBI) Project Management Methodology (please see our response to Question R.1 for more detail on our Project Management approach)
- *Standardized* ServiceNow enterprise software change and release management workflow system

All three aspects of our change management approach will be facilitated, continuously refined, and promulgated throughout LHC and Centene by our Information Technology (IT) Strategy and Service Continuity Team (IT Service Management Team), which reports directly to our Chief Information Officer (CIO). Through the IT Service Management Team, our local LHC staff, and our ServiceNow system, we will be able to communicate and collaborate effectively with DHH and/or our providers for MIS modifications affecting any of our constituents, including providing DHH and/or the fiscal intermediary with appropriate system access to allow testing of system changes.

We will keep all parties informed of project progress and adjust activities in light of any new circumstances that surface during a change or modification project. LHC will also notify DHH of major changes, upgrades, modifications, or updates to core applications or operating software (including, but not limited to, those listed in Section 16.4.3.4) at least 90 calendar days prior to the projected change date. For any system changes that are necessary, LHC/Centene will incorporate revisions into our documentation and manuals as appropriate and provide a copy to DHH for review and approval 30 days prior to the implementation of the change. All documentation and subsequent revisions will be maintained

in an electronic format and be made easily available to DHH. Any such revisions in printed documentation will be completed within ten days of the actual revision made.

Best Practices to Effect Changes and Software Modifications

Agile Software Development Life Cycle. Centene and LHC will use an Agile Software Development Life Cycle (SDLC) process to deliver higher quality software faster, while maintaining effective business controls. Agile is an industry best practice development discipline that has a collaborative and evolutionary approach with consistent outcomes in both quality and customer satisfaction. We implement MIS changes as part of an integrated release management process. Each Centene application team (e.g. claims, reporting, case management) works with their business partners to capture requirements and define priorities, and then establishes and publishes a release calendar with controlled releases typically every two to four weeks. This frequency mitigates operational risk by reducing emergency changes. Our SDLC includes the following stages facilitated by our IT Service Management Team and the Change Review Board (CRB):

- Stakeholder Input on Release/Change
- Development and Unit Testing
- Review of Release/Change and Deployment to Test
- Integration Testing/User Acceptance Testing
- Management Validation
- Change Review
- Move to Production
- Validation of Production

Each stage has defined tasks and responsibilities to ensure a successful development and change release process.

Information Technology Process Improvement. Our IT Service Management Team drives our efforts to continuously enhance IT processes throughout the organization. We have integrated the Information Technology Infrastructure Library (ITIL) process framework into our IT organization. ITIL is a process-based, best practice framework for delivering and managing day-to-day IT services. Centene requires MIS management to obtain certification in ITIL v3 and incorporate these practices into their service areas. We will establish communication channels between LHC and our IT organization by assigning an IT Executive Sponsor who ensures bi-directional communication and coordination at the highest levels between the health plan (e.g. LHC) and Centene IT. This will enable a close alignment between LHC priorities and our systems development. In addition to this role, each functional area of LHC, such as claims, medical management, quality management, encounters, operations, and compliance, will have designated IT contacts and liaisons at Centene for immediate tactical and planning support.

Automation to Power Change Management: ServiceNow. To further enable and leverage ITIL methodology, Centene augmented their toolset in 2010 with ServiceNow, an ITIL-based workflow application for integrating multiple aspects of MIS service delivery. Centene's initial implementation of ServiceNow has leveraged the tool to provide Request Fulfillment (i.e. server request, password reset request, new user request, storage request, etc.), Incident/Issue Resolution, Problem/Root Cause Analysis, Change Management, Asset/Lifecycle Management, and Configuration Management. ServiceNow's comprehensive approach to service management provides us with the technological toolset to ensure that IT change order and software modification processes can be effectively and consistently managed with higher quality results, in auditable fashion. ServiceNow has already provided Centene enhanced management oversight of change activities, improved release management control, and a streamlined approach to overall service management administration.

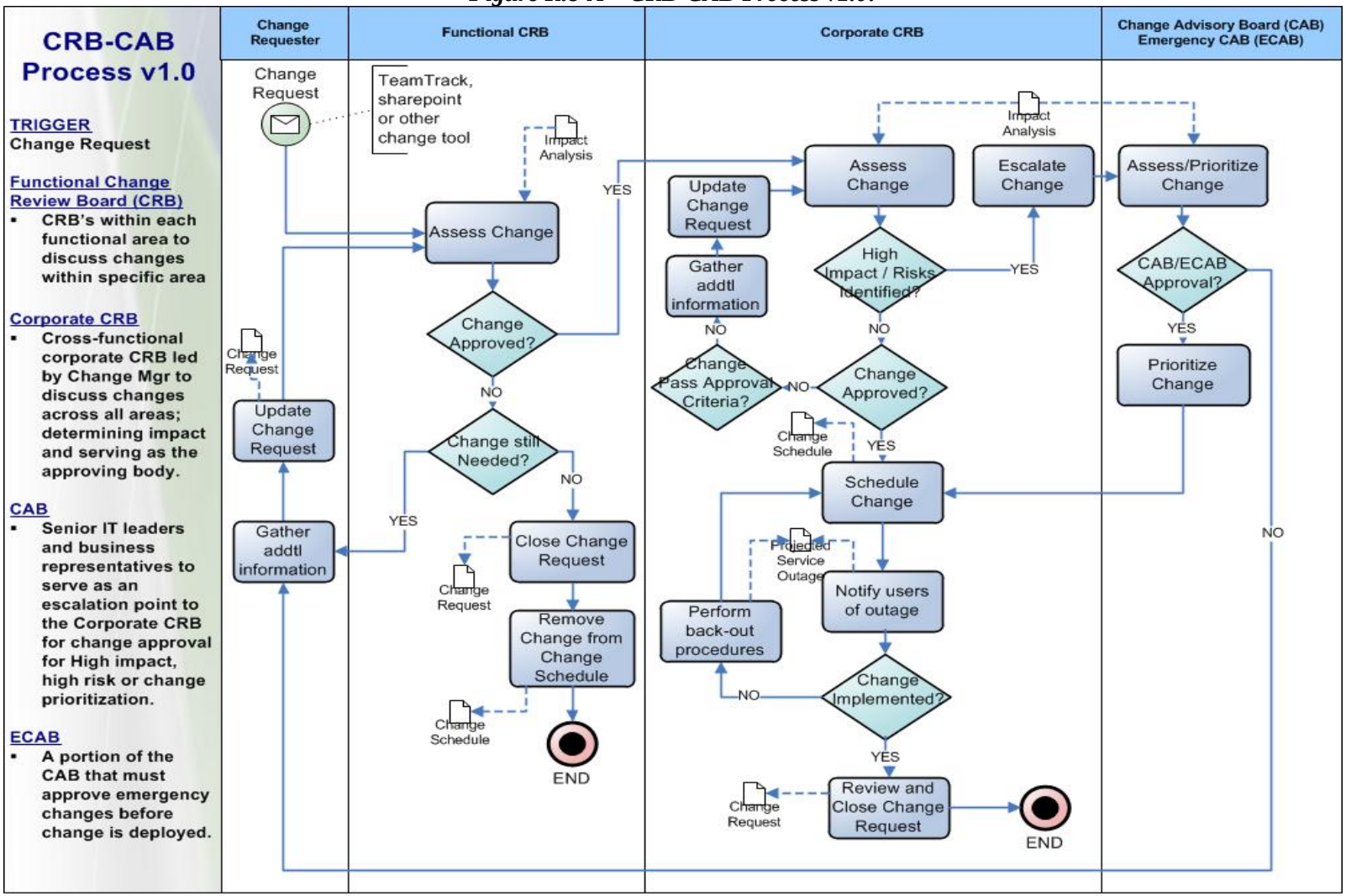
A Standardized and Disciplined Process for Change and Production Control

LHC will follow a structured and disciplined change management process throughout the DHH contract. Centene manages change requests according to a pre-established hierarchy that establishes the priority and protocol that must be followed to implement the change, and LHC will follow this same protocol.

- **Standard change.** These changes are typically pre-approved, low risk, and relatively common changes that are routine and do not significantly alter the production environment. For example, provisioning a PC to a new employee and providing regular, role-based network or application access would be considered a standard change. Standard changes do not require CRB approval as long as they follow established policies and procedures governing the particular request (i.e. application requests must be in compliance with role-based security access protocols).
- **Normal change**. These are planned changes to a service or infrastructure that are assessed and authorized based on financial implications, impact, and risk. Normal changes *require* CRB approval prior to deployment. Those changes determined to be High Impact and/or High Risk will be escalated to the Change Advisory Board (CAB) for additional review when appropriate.
- **Emergency change**. These changes reflect unplanned Severity 1 (Sev1) or Severity (Sev2) Break/Fix changes that must be implemented with minimal notice in order to protect a service from an unacceptable risk of failure, service degradation, or a lack/loss of functionality. Emergency changes are automatically approved for deployment (due to the nature of the issue causing the emergency); however, notification still goes out to the CRB to maintain communication protocols. Emergency changes, although rare, may be made directly in production first, then made back into test environments for post-deployment assessment and testing.

For a visual representation of our production change control process, please reference ***Figure R.8-A – CRB-CAB Process v1.0*** below.

Figure R.8-A – CRB-CAB Process v1.0:



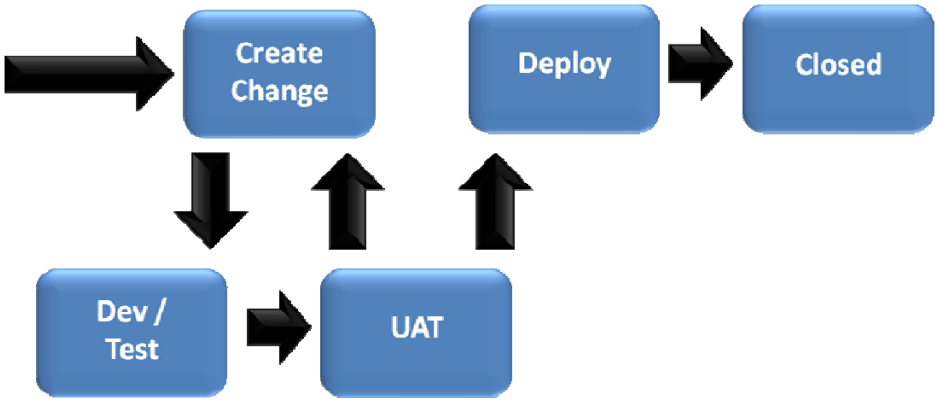
▪

Identifying and Validating Changes and Software Modifications

Centene follows a standard process to implement changes in a structured and controlled manner. This process, in place now for *all* Centene health plans, establishes the roles and responsibilities necessary to identify, document, and deploy changes. MIS software changes always originate from a "Key Business Stakeholder" (KBS) within our organization who identifies a change or software modification for one of three reasons:

- To implement new contractual requirements from state agencies, such as DHH, or other regulatory agencies
- To infuse new capabilities that enhance services to members and providers in an innovative fashion
- To enhance or reengineer an existing process to improve overall efficiency and service

In terms of *contractual/compliance driven changes*, the KBS will usually be LHC's Compliance Officer or Centene's Legal Department that will work together to identify needed changes in line with DHH and/or federal mandates, using our Compliance 360 corporate governance and compliance system. A KBS at LHC, in consultation and with the support of an appropriate Centene IT liaison, will champion change orders or software modifications to introduce innovative solutions for our LHC members and providers. All change and software modification requests are documented and signed off on in our ServiceNow system, with appropriate management approval, and are reviewed weekly by the IT Service Management Team's interdisciplinary CRB. The CRB ensures that changes and software modifications are implemented in coordinated release fashion, and that adequate time and resources are assigned for unit, system integration, user acceptance, and regression testing. The flowchart below graphically illustrates our disciplined process and further detail is provided in the narrative below.



- **Create Change**. The initial step in our Change Management process is to initiate the change process. To do this, the KBS, Change Owner and Development Team participate in an initial Release Planning Meeting to review "user stories", which reflect the business requirements comprising our change releases. A key output of this meeting is to identify and prioritize changes to be included in the next system release. Within this step, business requirements are developed for each user story and targeted analyses conducted to answer open questions and establish a common understanding of the change that is necessary. Once completed, resources are assigned to perform specific tasks (e.g., architecture design, business rules) as appropriate for the change. All user stories are documented as part of this step.
- **Development and Testing.** Once the change is approved and resources assigned, development activity can begin. Throughout the development effort, testing is completed and may be completed simultaneously with development to ensure that the desired functionality works accurately and as expected based on established requirements. The team holds daily "scrums," or meetings, to discuss

development status and how user stories are being met. Both IT and business owners attend the daily meetings. Extensive peer review and engineer review processes are performed in this stage as required to ensure the changes are consistent with overall strategy and design.

- **User Acceptance Testing (UAT)**. Once developed, changes are moved to a test environment for UAT. Although this is a formal step within the testing process, the KBS and IT teams conduct testing activities throughout the development process. UAT serves as a final checkpoint for user acceptance prior to promoting the change to production. Prior to the actual promotion of the change to production, the release must be submitted to the CRB for approval. The CRB reviews all changes that have been submitted for deployment in the next week. Each change is discussed to ensure the timing does not present any conflicts or unanticipated impacts on production.
- **Deployment**. Once the CRB has reviewed and approved the change release, IT management must *also* validate the release and provide their approval for the release to be deployed. IT management approval consists of validating that all requirements are included in the release and all documentation has been obtained and approved. Once approval is obtained, the release is ready for deployment to production. Key Business Stakeholders are auto-notified and requested to provide production approval within three business days. Once the release is in production, an audit trail is documented to track the release in ServiceNow.

Business Process Optimization (BPO)

In addition to more typical change requests identified by our business owners, our Centene BPO Team (BPO Team), which reports directly to the CIO, identifies reengineering opportunities to drive improvement in overall efficiency and service delivery. The BPO team will work jointly with LHC, using a Six Sigma approach to continuously measure and analyze operational Key Performance Indicator (KPI) information and seek areas for improvement, often using external benchmarks as a guide. Once we identify a process area for focus, the BPO Team applies root cause analysis to identify underlying problems and a resolution. The BPO Team then identifies key process metrics that allow us to measure the impact of our improvement strategies and ensure the resolution is effective in enhancing the target process. Along the way, the BPO Team (working with LHC staff) may formulate a change order or software modification, and the appropriate KBS sponsors the change in ServiceNow for appropriate sign-offs and release scheduling through the CRB. For example, our BPO Team recently uncovered an opportunity for more efficient distribution of member care gap information derived from our predictive modeling software. The BPO Team led a cross functional team with representation from Medical Management, Case Management, Member and Provider services, and our IT organization. This ultimately led to a software modification: the secure search and display of care gaps via our Online Care Gap Notification Please see our response in Section R.10 for more information on this feature.

Production System Version Control – A History of Success. Centene regularly upgrades core systems to take advantage of new technologies or to meet new compliancy requirements. Although the majority of our system upgrades are routine and pose minimal risk to operational processing, **all** upgrades and conversions are closely tracked and managed utilizing the tools and methodologies described above. In those instances during which a major system upgrade or conversion is necessary to leverage highly-desirable system capabilities, stay current on vendor system versions, or meet external requirements, Centene and LHC will further augment these methodologies with additional management oversight, extended stakeholder communication, and comprehensive planning which includes extensive testing and contingency planning.

Centene's ability to achieve successful system conversion implementations is a recognized strength, with accomplishments demonstrated throughout our public sector contracts. LHC will follow appropriate DHH notification guidelines and submit a proposed project plan for review, including a timeline, milestones, and adequate testing before implementation. Additionally, we follow any required monthly update communication schedule requirements for our state clients and provide frequent updates during the course of the conversion. Since conversions can impact the provider community, we will take a proactive

approach by mailing notices informing providers of the conversion and asking providers to be aware and to notify us with any issues. During major system conversions, Centene's objective is to make the *right* decision, at the *right* time and to maintain an open, honest communication protocol with all stakeholders.

Maintaining Production Control While Introducing Meaningful Innovation

Through Centene's 27 years supporting Medicaid managed health programs, we have *carefully* but *continuously enhanced* the individual components and integration of our software architecture.

We balance the demand for software reliability, data integrity, and availability with the need to *carefully* infuse relevant new software versions and innovations, deploying new software and updated software versions through well-documented SDLC and MIS operation techniques. Our use of the AGILE method for SDLC allows us to formulate, develop, test, and introduce new software versions quickly, yet within the confines of auditable change management, and allowing for total project risk mitigation procedures.

Every year, we review and compare all hardware and software components in our integrated MIS portfolio with the latest product versions from our vendors, and overlay the projected needs of our business for the following year. The output of this effort is our Strategic Technology Refresh Plan, which serves as our annual roadmap for planned introduction of new software versions for both Centene proprietary and vendor supported software components. Centene will provide DHH a copy of our Strategic Technology Refresh Plan (Refresh Plan) in accordance with the requirements specified in the RFP. Please see Section R.7 for more information on our Refresh Plan. Additional documentation supporting original equipment manufacturer (OEM), software development firm (SDF), or third party authorization requirements will also be incorporated into the plan and provided to DHH as appropriate.

A Hardware Architecture That Easily Accommodates Change

Centene engineers the hardware, software, communications, and processes in our MIS to ensure that our applications are available for our internal staff, providers, members and state partners, such as DHH, with the least possible disruption, even during software upgrades and release changes. We maintain and continually enhance the availability of our MIS-related capabilities through the design of redundancy we factor into the hardware, software, and networking components of our MIS architecture. All of the MIS infrastructure technologies, MIS service management strategies, Incident Management, Business Continuity and Disaster Recovery policies, procedures and processes supporting our MIS offering to DHH are in place *today*. We have successfully implemented – and currently operate – these solutions for our plans in Illinois and Mississippi, and these are the same solutions that support all our operations in 11 plans across the United States.

Our MIS architecture is based on the four key principles of:

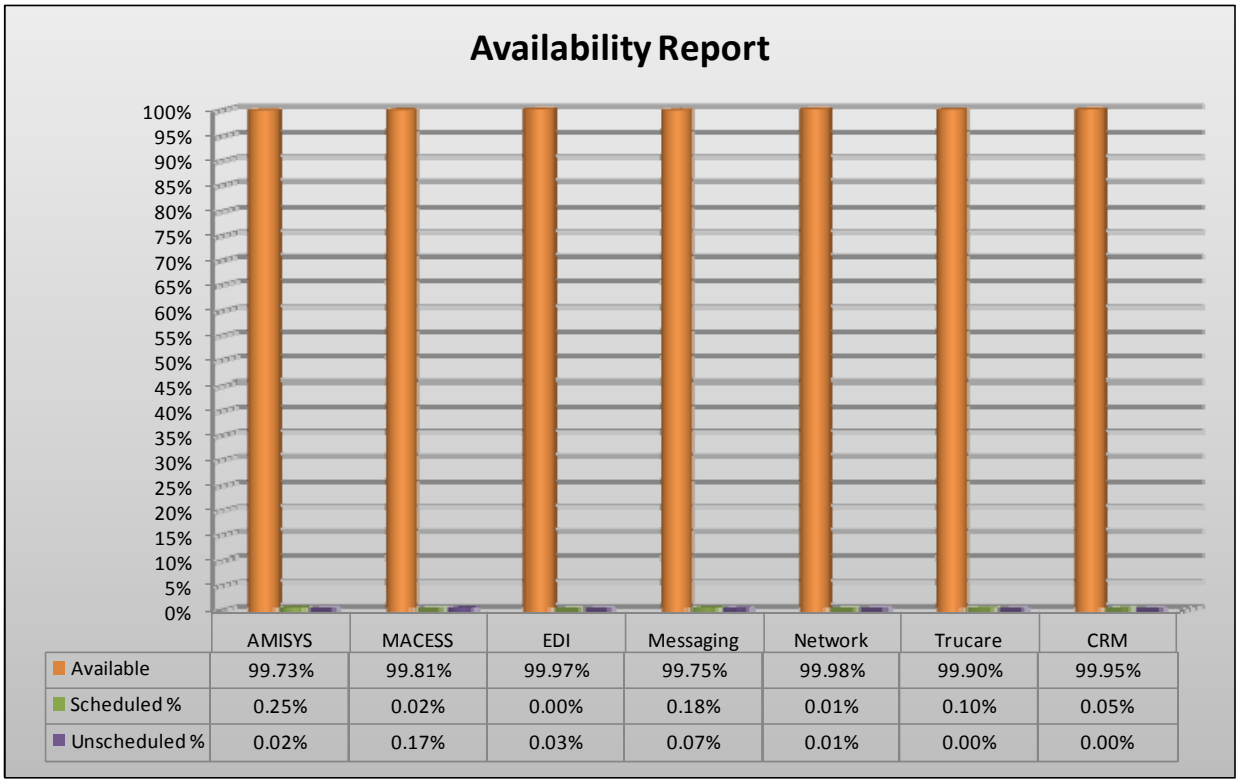
1. High Availability;
2. Industry Standard and Best-In-Claims Systems;
3. Scalability & Flexibility and
4. Monitoring & Service.

Each principle guides the identification, deployment, monitoring and delivery of IT services in an effective and consistent manner.

We manage hardware changes and upgrades with the same methodology that we deploy for software version upgrades and changes (discussed above). In addition, our hardware and system software changes are also informed by our ongoing capacity monitoring and planning processes (see question R.1 for more information). The highly redundant and fault tolerant aspects of this architecture (e.g. through the use of clustering, virtualized blade servers, multi-path Storage Area Networks and RAID storage) allows us to often switch to new software versions or upgrades with minimum downtime.

Our rigid adherence to these principles leads to solid performance results as illustrated in the systems availability graph below for the preceding 12 months of service:

System Availability Report June 1, 2010 Through June 1 2011.



	AMISYS	MACESS	EDI	Messaging	Network	Trucare	CRM
Available	99.73%	99.81%	99.97%	99.75%	99.98%	99.90%	99.95%
Scheduled %	0.25%	0.02%	0.00%	0.18%	0.01%	0.10%	0.05%
Unscheduled %	0.02%	0.17%	0.03%	0.07%	0.01%	0.00%	0.00%

In the unlikely event LHC experiences system problems, LHC will comply with all requirements specified in Section 16 of the RFP including, but not limited to:

- Responding within five calendar days of receiving DHH notification of system problems
- Correcting system problems and/or submitting a solutions document to DHH within 15 calendar days
- Implementing a solution to correct the system problem effective by a DHH-determined date

In addition, LHC will not schedule system downtime or unavailability to conduct any upgrades or maintenance during a time which will adversely impact critical business operations. LHC and Centene are committed to establishing and maintaining an effective MIS solution that will meet or exceed the needs and requirements of DHH, our members, providers, and other DHH-designated entities. For more detailed information on our systems availability, please refer to our response in Section R.3.

Experience in Supporting Federal Mandates

As a publicly held entity subject to federal SOX regulations, Centene has continuously refined our processes for the systematic and early identification of federal mandates germane to our health plans. To ensure the coordinated, phased transitioning of mandates to meet compliance effective dates, we expeditiously assess the impact of mandates on our IT infrastructure and operations, develop and implement remediation plans resulting from those assessments, and formulate and execute Level I (internal) and Level II (external) testing plans, working collaboratively with our state clients and providers. Centene and LHC will conform to future federal and DHH standards required for encounter data exchanges within 120 calendar days prior to the effective date as required by DHH and/or CMS. Please see Section R.15 for more information on our support of federal mandates.

Question R.9

Demonstrating Information System Readiness Prior to Operational Start

R.9 Describe your approach to demonstrating the readiness of your information systems to DHH prior to the start date of operations. At a minimum your description must address:

- provider contract loads and associated business rules;
- eligibility/enrollment data loads and associated business rules;
- claims processing and adjudication logic; and
- encounter generation and validation prior to submission to DHH.

LHC Approach to Readiness

LHC's Management Information Systems (MIS), managed by our parent company Centene, supports the goals of responsive, accountable, and coordinated care for almost 1.6 million Americans in our affiliated public sector, full risk, managed care plans in 11 states. In each of these states, we are accountable to our state partners for the readiness of our operations at contract implementation, as well as each change we implement into our MIS environment through the duration of each contract. In fact, we begin the readiness review process well before contract implementation with our well-defined MIS processes, procedures, and documentation when we design and build our systems. The process continues as we analyze, in detail, and document the specific contract implementation requirements, then configure, thoroughly test, and implement those requirements into our systems. Centene is well practiced in demonstrating our systems, protocols, and supporting documentation for readiness reviews prior to operational start date(s) and is able to accommodate nearly any preferred review format, structure, and venue.

We will prepare for readiness reviews by first compiling documentation for a desk review that illustrates our MIS, including system and enterprise architecture documents, technical reference documents, IT policies and procedures, user manuals, etc. We provide this information both electronically and in hard copy via binders in a well-organized manner, by each functional area of system operations. These documents allow for an upfront and detailed understanding of our MIS. Ideally, we would meet with the state to review these documents to answer any questions DHH might have about our MIS environment or terminology.

Following this presentation, and closer to the operational start date of the program, we typically provide more *targeted* and *customized* information at an onsite review, related specifically to the needs of the state and the health care program we are implementing. This onsite review for DHH and the Coordinated Care Network Prepaid (CCN-P) program would be our opportunity to demonstrate our systems with a live "walk through" or presentation of key functionality. In addition, we would provide further program documentation, such as our configuration documents, user stories, testing results from internal integrated testing, and our testing results illustrating our ability to successfully process all required transactions with DHH's enrollment broker (EB) and fiscal intermediary (FI). The live demonstration typically covers, but is not limited to, our Provider Relationship Management (PRM) System (provider contract loads and associated business rules), our Member Relationship Management (MRM) System (eligibility/enrollment data loads and associated business rules), AMISYS Advance (claims processing), MemberConnect and ProviderConnect (call center operations), TruCare (health services management), LHC Member and Provider portals, MDE Xpress Encounter Pro (encounter processing), and finally our Centelligence™ informatics platform. We will focus on any particular process as required by DHH. Below is a brief description of the demonstrated functionality DHH should expect to see:

Provider Relationship Management

Centene will provide the specifications, basic design, and user documentation for our PRM system, including: **Emptoris**, our provider contracting system; **Portico,** our provider data management solution; and ProviderReach and ProviderConnect functionality provided by our **Customer Relationship Management (CRM)** system, powered by Microsoft Dynamics.

Emptoris. We will demonstrate to DHH how contract templates are generated using standardized language formats that are electronically available to our Network Management Contractors in Emptoris, and how customizable language is available, allowing for contracting variations, while maintaining structure and comprehensive documentation retention. We will generate and load both typical and atypical provider contracts for illustration.

Centelligence Negotiator. Within our Centelligence™ Negotiator system, we configure the pricing structure behind each contract. Centelligence™ Negotiator is an all inclusive documentation system, allowing our Provider Network team to effectively transition the details of a provider agreement to a Contract Implementation Manager and Configuration Engineer, who ensures the proper code configuration within **AMISYS Advance**, our core claims processing system. We will demonstrate how we do this in Centelligence Negotiator as well as share with the state our configuration and testing documentation that goes hand in hand with contract loads.

Portico. We will also demonstrate our Portico provider data management system, which holds all demographic data for our providers and is fully integrated with AMISYS Advance and our ProviderConnect and MemberConnect service inquiry applications. We will specifically highlight the credentialing process and documentation; how we know if a provider license is nearing expiration; financial affiliation information; demographics and the unique data fields for the CCN-P Program, such as the flag for Memorandum of Understanding for emergency events; and how we update provider records and provider directory management.

ProviderConnect and ProviderReach. Integrated with Portico, and AMISYS Advance, ProviderConnect and ProviderReach comprise the CRM components of our PRM. ProviderConnect allows Provider Service Representatives (PSRs) to view all relevant provider data so that they are able to respond to most provider inquiries, without the need to refer to other systems or route the call to another party. We will demonstrate to DHH how the PSR records the nature of the provider inquiry, where the PSR documents the discussion and outcomes, and the reference screens they access to obtain information at their fingertips. When the PSR is not able to directly answer a provider question, we will show how the PSR can route that call to a specific call queue and how they can track the call through to completion.

Our ProviderReach functionality enables us to create and manage *outbound* call campaigns via email, automated Predictive Auto Dialing (PAD) services, or call queues to be placed manually by LHC outreach staff. We will demonstrate how this is done in ProviderReach and discuss how we will use this functionality, for example, to send a letter to specific providers when their licenses are nearing expiration or to capture and record the availability of provider services following an emergency event so that we can refer members to offices that are in service, and provide this information to the relevant Emergency Operations Center.

Finally, we will demonstrate the reporting capability of ProviderConnect to assist LHC management in identifying opportunities for outreach and provider education. For example, if we see multiple inquiries for the same type of question or concern, we will analyze this to determine if there is a better way to disseminate information to avoid confusion or calls to our call center in the first place.

Eligibility/Enrollment

Once we receive the 834 Companion Guide from DHH or DHH's EB, we will create our functional specification and business rule documentation for the enrollment process. These are largely internal mapping documents, but we would be happy to review these with DHH to demonstrate how these documents are utilized to map and structure enrollment data in our systems.

Testing with the EB and FI. We consider testing with DHH's EB one of the most critical components in preparing us to serve our CCN-P members. Early and successful completion of testing with the EB during the transition phase will better position us to serve CCN-P at go-live with few or no issues. Utilizing sufficient data provided by the EB, we anticipate thorough and comprehensive testing to test multiple scenarios with the **daily** 834 enrollment file, and the **weekly** and the **monthly** enrollment reconciliation

files. Throughout the testing process we will document progress, issues, and the resolution of those issues; take screen shots, where appropriate; update our documentation; record the results of our testing; and share the results of our testing with DHH.

Demonstrating the Enrollment Process. We will demonstrate a mock enrollment using data provided by DHH's EB, if available, or test data mocked up from one of our affiliate health plans. To complement our demonstration of the systematic processes, we will tie in evidence of our reconciliation and error reporting processes, as well as any needed manual intervention to correct and load fallout records, or those with conflicts, such as a single member with multiple identification numbers. We will further demonstrate the creation and delivery of eligibility files to our affiliated vision subcontractor, OptiCare Managed Vision® (OptiCare), followed by a review of our service level agreements with OptiCare.

Member Data Management. Once loaded, we will be able to show the data in our Member Relationship Management (MRM) system. MRM is our "system of record" and master data store for "all things member related". We will be able to show DHH a member record, how MRM stores member identifiers, address and contact information, confirmed or potential family linkages, special needs, and numerous other attributes, as well as member preferences, including communication options such as e-mail, phone, or mail. We will demonstrate the direct update abilities we have within MRM to exemplify both the data quality controls and the flexibility and responsiveness we are able to offer to handle emergency enrollment changes, updates, and member requests.

MemberConnect and MemberReach. Our MRM is designed on the same CRM platform that enables our ProviderConnect and ProviderReach functionality described above. Like PRM, we are able to track and manage *inbound* member calls to our LHC Member Service Representatives (MSR). We will show the state how the MSR navigates MRM to obtain information integrated into MRM from our other core systems, such as claims from AMISYS Advance and provider information from PRM, so that in most cases the MSR can address member concerns easily and efficiently without the need to go into other systems, or route the call to another department. We will show DHH how MRM links family records together based on pre-determined criteria and how our MSR navigates between those records to see if there is an opportunity to address something related to another family member during the call. Finally, we will demonstrate how care gap alerts generated from our Centelligence™ Foresight tool are integrated into MRM and how alerts can be manually entered into the system to alert the MSR that there is something an LHC Case Manager wants to cover with the member while they are on the phone. For example, a Case Manager can put an alert in MRM when trying to reach a member. If the member calls LHC, the MSR will see that alert, and after addressing the member question or concern, can warm transfer the call to the Case Management Team and route the call within CRM to the appropriate queue. We will also demonstrate how email from our Member Portal is integrated with CRM and our response and tracking procedures for email communications.

MemberReach. Finally, similar to the outbound call campaigns we conduct to our provider community, we will demonstrate how we can create and manage outbound call campaigns to our members and discuss with DHH how we might use this functionality. For example, during our Hurricane Awareness month, we will pull a report of Special Needs members and send an outbound message to them by mail, email, PAD, or an in person phone call, reminding the member to review and update their Emergency Preparedness Plan (EPP). As always, we will provide our member services dial-in number on the DHH approved outbound message to assist any member who contacts LHC for help with completing or updating their personal EPP. Finally, we will demonstrate the reporting capability of CRM and how this helps LHC manage and track, for example, attempts to contact members for their LHC welcome call, whether or not the member has completed a Health Risk Screen, if a member is Special Needs, etc.

Claims Processing and Adjudication Logic

In preparation for the CCN-P Program, we will hold a "configuration summit", which includes representation from our Claims, Configuration, and Network Contracting Departments. During this week

of intense focused activity, we request that senior staff from the health plan and a representative from the state be accessible to facilitate decision-making to ensure the process moves forward quickly. Out of this summit and activity, we produce a detailed benefit grid and detailed payment guidelines. These documents are the foundation of our configuration requirements and will be shared with the state during readiness. We attach this documentation to "change requests" to initiate configuration within AMISYS Advance, our core claims processing system. The configuration process includes multiple phases, all of which are documented in our workload management tool. We will show DHH how we document configuration changes and how these requests move through the process of Development, Integrated Testing, User Acceptance Testing, and finally to Production. We will also share with the state the results of our 100% quality review audit that verifies if the configuration in the system is true to the intent of the actual configuration request.

AMISYS Advance. We will demonstrate the functionality of AMISYS Advance, our core claims processing system. We will walk DHH through our pre-adjudication designs, including values edited; and accept, reject, and denial coding.

We will follow a claim through the process of adjudication within AMISYS Advance. We will highlight areas of interest, such as how we know when a claim was received; the pricing of the claim; how we know what denial or payment codes were applied; if there was an authorization requirement and if the requirement was met (AMISYS Advance matched the authorization on record to the claim); and if the claim contained a trauma code so that we can route the claim to Health Management Systems, Inc. (HMS), our partner for post payment recovery services, for further investigation. We will also show a corrected claim, how we treat a provider's request for reconsideration, how our pend queues are configured, how claims can be routed to specific, experienced processors for review through our Automatic Work Distributor (AWD) system, and how the information is updated in AMISYS Advance. We will also explain our relationships with the multiple EDI claims clearinghouses with whom we partner.

Encounter Submissions

In addition to testing enrollment with DHH's FI prior to go-live, we anticipate testing the submission of encounter data with sufficient quantity and type of claims to address the greatest number of scenarios possible. A critical component in our approach to encounter processing is Centene's effective testing, validation, and operational processes. We look forward to iterative end-to-end testing cycles with DHH and the DHH's FI and will share the results of our testing with DHH.

We use Medical Data Express's (MDE) Xpress Encounter Pro (Encounter Pro) to process Encounter information to the state. During an onsite demonstration, we will visually explain and demonstrate the acquisition of encounter data that originates in AMISYS Advance and is integrated into our Encounter Pro system via our Enterprise Data Warehouse (EDW). Directly in Encounter Pro, we will show how encounter data is viewed, processed, and audited, in accordance with both federal and DHH requirements to ensure complete and accurate representation of encountered services. We will show DHH how we are able to capture the same line item detail as the submitted claim, regardless of the claim type, disposition (e.g., paid or denied), third party liability indicators, or capitation arrangements. We also will show how we can process encounters to include all rendered services, original and adjusted claims, the application of retroactive fee or member changes, etc., according to the size and file format required by DHH and DHH's fiscal intermediary. We will demonstrate how our data adheres to NCQA, AMA coding, UB-04 editor, NCCI, and DHH standards, use of standard codes (including CPT Category I and II, HCPCS Level II and ICD-9-CM), counting methods, units, etc. Finally, we will show how the 837 file is generated in Encounter Pro and how we intake and process response files.

In addition to demonstrating readiness in the above four key areas, LHC and Centene will be prepared to demonstrate readiness related to the areas below.

Call Center Operations

In addition to our MRM and PRM features above, we will also review with DHH our telecommunications functionality supporting our call centers, including our call scripts, call flows, and emergency response procedures.

We will review the reporting made available *real time* through our Avaya Voice Portal (AVP), which allows us to track call wait and hold times, total call times, call volumes, call types, as well as listen in on MSRs and PSRs handling a specific member or provider inquiry. We will demonstrate our ability to quickly adjust call queue staffing ratios to ensure we are able to meet and exceed DHH service level expectations.

Interactive Voice Response (IVR) Systems. We will walk through mock member and provider phone calls with the DHH readiness review team, using a variety of scenarios, some which will be handled via our fully automated IVR system and others which will fall into live call center queues in our CRM. Through these demonstrations, DHH reviewers will experience first hand the options for assistance and support that we offer to our members and providers. We will spend significant time walking through the IVR phone call flows, which we have carefully architected to provide expedient and considerate care of our members' and providers' needs.

Medical Management

LHC and Centene staff will walk through all elements of TruCare, our member-centric health services management solution that enables LHC to coordinate care for our members across the health care services that they receive, and provide case and utilization management for the CCN-P Program. We will start with member demographics, showing our ability to store multiple addresses and indicators for special needs or language/cultural considerations, allergies, treating providers, etc. We will also review within TruCare, the member benefits/eligibility file. We will walk through the Case Management process from receipt of a task through full Health Risk Assessment, condition specific assessment, and creation of a service plan, including identification of problems, goals, interventions and barriers, which may be medical, behavioral, or social in nature. We will show how Case Managers can generate reminder tasks to follow up with a member for reassessment or create a task for one of our MCRs to research alternate phone numbers, conduct a home visit, or contact the member to remind them of an upcoming appointment.

We will demonstrate how our case managers and medical reviewers see specific work tasks queued in TruCare for follow up and how TruCare creates alerts so that these are managed in a timely manner. We will also demonstrate how we queue tasks for follow up by our Member Connections Staff or for our triage nurse, to determine priority of work for members in need of outreach by our MemberConnections or clinical staff. Finally, we will walk through the process for entering an authorization including clinical review; the application of our online InterQual medical necessity criteria, which is imbedded within TruCare; and our process for advisor (MD) review, determination and provider notification.

Provider and Member Portals

We will provide a full demonstration of all facets of our public and secure Member and Provider Portals. On the public Portal, we will highlight all the required elements specified by DHH, including the Member Handbook and Provider Manual; member privacy and other member rights and responsibilities; grievance and appeals procedures; contact information; and frequently asked questions and answers. We will show where our 800 number is posted and the contact number for the Telecommunications Device for the Deaf (TDD), where the link to EB's website can be found, and the toll free number where current or potential enrollees can call with their questions. We also will demonstrate our provider directory search feature,

and how our members can search for providers by geography, gender, or language, and how a member can access and complete a Health Risk Screen online.

Provider Portal. We will provide a full demonstration of all facets of our public and secure Provider Portal. Providers can register for access to our secure Provider Portal where multiple administrative and clinical features are available to streamline processes and enhance quality care to our members. We will demonstrate the Provider Portal registration process and the various administrative capabilities we offer to our providers on the secure Portal, including our online Direct Data Entry (DDE) claim submission process, claim adjustments, ability to view claim status, submit authorization requests, how providers can add supporting attachments and documentation, view explanations of payment (EOP), register for electronic payment (EFT), and a variety of other functions.

We will also demonstrate our clinical functionality beginning with the eligibility search, which returns not only a member's eligibility status with LHC, but also Online Care Gap Notifications (OCGN) powered by our Centelligence™ Foresight capability. OCGNs are available to providers when checking eligibility for an individual member and when PCPs view their Member Panel Roster, a display of all LHC members in their care. We will further demonstrate the rich integration of our portal with our Centelligence™ platform and our Enterprise Data Warehouse (EDW), which delivers our Member Health Record, which includes a view of the member's history such as medical, behavioral, and pharmacy claims data; health risk assessment information; lab test results; and other information housed in our EDW. We will also show the evidence-based *Clinical Practice Guidelines,* and provider online access to HEDIS reports, and the Emergency Care Record. Finally, we will demonstrate the more robust functionality CenTraCare will provide to our PCPs and FQHCs who have achieved NCQA or JCAHO recognition as Medical Homes. For more information on our Clinical Portal and CenTraCare, see our response in Section R.15.

Member Portal. Following the demonstration of our public site and Provider Portal, we will demonstrate the secure login capability of our Member Portal and the rich content and features available to our members in a secure environment. We will walk through the administrative features of the portal to demonstrate where members can update their portal security information; how members can use the Contact Us feature to send emails and use their secure inbox to retrieve them; how to use the change PCP function; how to view claims information; and how the Portal presents care gap alerts to the member.

Reporting

We will dedicate time to demonstrate to DHH our integrated reporting tools including our EDW, Centelligence™ Insight, and Centelligence™ Foresight capabilities. Through the demonstration of these reporting tools, DHH will gain a solid understanding of how we architected not only our core systems, but also the data modeling and warehousing structures that support them and enable us to report and extract information for the benefit of our members and providers. Centene's goal is to always progress and our key to ensuring we do so is by carefully analyzing our data, trends, systemic protocols, and operating patterns. The breadth of our reporting tools and our ability to create meaningful and actionable reports and metrics keeps us continually enhancing and developing our business from both technology and operations perspectives.

Enterprise Data Warehouse. Our EDW integrates medical, behavioral, vision, dental, and pharmacy claims; lab test data; member and provider demographics; and Health Risk Assessments (HRAs) into a centralized repository powered by Teradata® Extreme Data Appliance. Teradata® significantly improves our ability to handle truly large amounts of data in much shorter timeframes, resulting in more timely reports, Care Alerts, Dashboards, and other informatics. We will demonstrate our BusinessObjects reporting capability, which accesses the EDW; show DHH some of the many reports we are able to generate; and discuss with DHH how the information is operationalized. We will review the levels and types of data available and the flow of data through our core systems to our reporting tools.

Centelligence™ Insight. Centelligence™ Insight provides desktop, client, and provider profiling reporting in addition to internal management KPI Dashboards and our Catalyst QSI HEDIS application. We look

forward to showing DHH our award-winning desktop executive dashboard, which provides real-time operations intelligence to our management, updated daily to provide early warning of adverse trends; claims drill-down for a quick analysis of clinical, financial, or operating issues; and predictive modeling. We will also demonstrate and share with DHH how using our proprietary software integrated with OptumInsight's Impact Intelligence provider profiling system and clinical data (medical, behavioral, and pharmacy claims and other data) housed in our Teradata EDW, we are able to produce practice level clinical quality and reporting information for our NCQA and JCAHO recognized Medical Home providers.

Centelligence™ Foresight. Centelligence™ Foresight incorporates our Ingenix Impact Pro and Centene proprietary predictive modeling and Care Gap/Health Risk identification applications so that we can identify and report preventive service gaps and potentially significant health risks at various population, provider, and member levels *beforehand* so we can initiate appropriate care management activities. This is the technology that supports our OCGN assisting our medical management team, our Member and Provider Services Team, and our member and providers via the portal described above. We will demonstrate the reporting capability of **Centelligence™ Foresight, if possible, using the historical data provided to LHC from the state.**

Following the review of our system documentation and this onsite demonstration of our systems, we will look forward to moving to CCN-P "go live" with DHH.

Question R.10

Reporting and Data Analytic Capabilities

REDACTED

R.10 Describe your reporting and data analytic capabilities including:

- generation and provision to the State of the management reports prescribed in the RFP;
- generation and provision to the State of reports on request;
- the ability in a secure, inquiry-only environment for authorized DHH staff to create and/or generate reports out of your systems on an ad-hoc basis; and
- Reporting back to providers within the network.

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Question R.11

Profile of Key Information Systems

R.11 Provide a detailed profile of the key information systems within your span of control.

Nationwide HIT Expertise Focused on Local Plan Public Sector Programs

Louisiana Healthcare Connection's (LHC) key Management Information Systems (MIS) resources will be managed by LHC's parent company, Centene Corporation (Centene) and Centene's over 275 experienced MIS professionals working in conjunction with LHC's MIS, Operations, and Managerial staff. Since its inception in 1984, Centene has focused exclusively on Medicaid, CHIP, and other public sector managed care programs, and has successfully addressed the unique functionality, connectivity and data exchange needs that our local plans, state clients and public sector providers need for effective, results-driven health plan administration. Today Centene's HIT resources support our local plans in eleven states, and over 100,000 public sector medical - all serving the care needs of 1.6 million Americans. We propose the MIS infrastructure and applications described below in service of the Department of Health and Hospitals (DHH).

We have reviewed all information technology requirements in the Department's Request for Proposal (RFP) and are able to fully support or exceed all information technology aspects of the CCN. Please see Question R.7 for details on how we meet or exceed each requirement in Section 16. Please see Questions R.2, R.5, and R.6 for information on our support for requirements stemming from the CCN-P Systems Companion Guide, Question R.3 and Section M, Questions M.1 and M.2 for our support for business continuity planning, contingencies, and availability requirements, Section K, Question K.5 for our support for members via the internet, Section Q, Questions Q.1, Q.2, and Q.3 for our support of RFP Section 17 claim processing requirements, and Section P, Question P.1 for our support of Third

Deploying MIS Resources at the Plan Level

In our response to Question R.11 below, we have outlined the functionalities and capabilities of the MIS resources and components that are within our span of control and are in place today that we plan for deployment at LHC by the time of contract implementation. Table R.11-A below offers a summary of the material *detailed* in the rest of this section.

An important aspect of our entire MIS Resource portfolio is that all our systems and applications support our clinical and administrative operations - facilitating coordinated care critical in the CCN.

Table R.11-A

HIT Resources	Timing
MIS Infrastructure - Redundant, highly available application, relational database, and data storage servers for core applications (enrollment, eligibility, claims and encounter processing, clinical management, websites, reporting) - and *supporting* applications (EDI, image scanning, middleware, data integration subsystems, e-mail and secure e-mail, office automation and support).	In place now.

HIT Resources	Timing
Redundant, highly available **Wide Area Network** (WAN) for data and voice communications.	In place now. Local connections, pre-configured local thin client, secure desktop workstations, and telephone system (including Interactive Voice Response) for LHC office will be put in place prior to contract implementation by our Centene MIS department.
HIPAA compliant transaction and codeset translation software, HIPAA compliance checking software, and HIPAA compliant security controls.	Full HIPAA transaction support available now via our EDIFECS EDI system. All HIPAA Security controls in place now (see Question R.16). Physical controls based on Centene security standards for LHC office will be put in place prior to contract implementation by our Centene facilities manager and staff.
Integrated core processing applications: including AMISYS Advance claims processing, Centelligence™ Enterprise Data Warehouse (EDW) and Centelligence™ integrated SAP BusinessObjects reporting software and Impact Pro Predictive modeling system, MACESS document management and Member and Provider Services and master data management support (via our Member Relationship Management (MRM) and Provider Relationship Management (PRM)) systems.	In place now.
Secure web based Member Portal and Provider Portal (with advanced clinical support).	Our Member Portals are in place now. We will customize versions of both our Member and Provider Portal for LHC operations prior to contract implementation. Please see Section K.5 for specifics on our Member Portal and Question R.15 for more on our Provider Portal.
CaseNet TruCare (TruCare) clinical management system, MDE xPress Encounter Pro (encounter processing), and MedAssurant Catalyst (HEDIS and clinical quality reporting).	In place now.

Our MIS Resources Include Technology, Security, Applications, Processes, and People

Centene and LHC view our MIS resources as significantly more than hardware and software. Our MIS capabilities stem from a confluence of organization, computing infrastructure and applications, and vendor and subcontractor alliances all focused on delivering reliable, scalable, responsive and innovative system solutions - with the ultimate goal of addressing the needs of our state clients and the health of our members, their families and our shared communities.

Thus, delivering MIS resources that address accountable, integrated care means more to LHC and Centene than acquiring, developing, and running hardware and software, although a smoothly operating information technology (IT) infrastructure is certainly critical. Grounded in Centene's 27 years' experience of supporting the MIS needs of Medicaid and other public sector and individual health care programs we meet and surpass our state clients' needs, maintaining our system capabilities through:

1. **Technology Infrastructure:** We continually **architect** an integrated IT base engineered for reliability, growth, and interoperability; while continuously evolving that base to exploit new technologies and business imperatives in a carefully controlled manner through our business requirements driven *refresh plan*. Our architecture allows us to easily support multiple and secure data receipt, transmission, and data integration protocols for information exchanges with providers, our state clients, or other data sharing collaboratives that may be initiated by our state clients (e.g. in DHH's case, potential Health Information Exchange (HIE) projects) .
2. **Information Security:** Today, Centene employs rigorous safeguards, policies, monitoring tools, and automated business processes to ensure adherence to HIPAA Security, Privacy, and Transactions and Code Set Standards. We employ administrative, technical and physical security safeguards under the guidance of Centene's Compliance Officer, Chief Information Security Officer (CISO), and General Counsel. We have Business Associate Agreements in place for all subcontractors and vendors we employ who have access to Protected Health Information (PHI). We support HIPAA transactions and codeset exchanges directly and through clearinghouses.
3. **Best of Breed Applications:** We deliver LHC MIS functionality to our plans by sourcing the best functional applications and integrating into our overall MIS architecture and business process workflows via our Service Oriented Architecture (SOA). Our applications are functionally rich for the job they are designed for, yet integrated where they need to be to assure efficient, quality care operations. Please see Question R.4 for more information.

   Supporting the computing assets listed above, we have two other major ingredients to our MIS resources supporting our plans (such as LHC):
4. **Processes:** We **implement changes** and new functionalities in our MIS through the disciplined use of proven Agile Software Development Life Cycle (SDLC) procedures and Project Management methodologies. Our Agile approach assures DHH of an effective readiness review and implementation and our Project Management methodology effectively communicates at appropriate project junctures to all our subcontractors, Providers, DHH and all other constituents needed for the CCN program.
5. **People:** We organize our MIS professionals at the plan and Centene Corporate level so that we consistently maintain excellent service, while investing in the ongoing professional development and training of our IT staff and MIS end users (including our provider, member and state client users). Our attention to training for our IT staff, along with our automated processes and controls, ensures reliable data receipt, transmission and integration operations, along with best practice MIS management approaches. Our business and technical analysts are trained and experienced in all aspects of our MIS, as well as our rigid approach to requirements analysis. We also team effectively with our critical *extended organization* – our subcontractors. We carefully oversee the MIS operations and data integration activities of our subcontractors, through the clear contractual delineation and obligations of our subcontractors to exchange data with us on formal schedules, in specified formats, and by our regular operational oversight we perform on our subcontractors.

Technology Infrastructure. All of the functions and supporting information technology (IT) infrastructure that we describe in this section is in place *today* (unless otherwise noted) and ready for deployment in service of LHC and the CCN.

A Hardware Architecture Engineered for Dependability and Growth. We maintain and continually enhance our MIS related capabilities through the meticulous design and technology refresh we incorporate in all the hardware, software, and networking components of our IT architecture.

Our MIS architecture is based on these principal design points:

- ***Reliability*** – for sustained availability through redundancy in our entire computing infrastructure.

- ***Scalability*** – to expand the capacity of our operations without affecting current business operations.
- ***Data Integration*** – allowing us to use common data across processes to power our unified care model.
- ***Flexibility*** – to maintain agility in our MIS, allowing for quick changes based on business imperatives.

Delivering the Right Processing Power**.** We use proven, industry standard hardware and software components for our core processing applications, summarized in five categories in Table R.11-B below, to deliver computing power to our local plans:

Table R.11-B

Key Component	Description
Database Layer	All core data is stored on our fully redundant Storage Area Network (SAN) which supports access to two highly available arrays: a NetApp SAN attached Storage Array with Independent Disk (RAID) 5 and RAID 6 configuration; and an HP StorageWorks XP24000 configured for RAID 5 storage. The XP24000 can scale up to 1.13 PB and is currently configured at 146.5 TB. Our Centelligence™ family of reporting and decision support applications is powered by our Teradata® Extreme Data Appliance.
Business System Layer	Five HP 9000 servers running HP/UX Unix power AMISYS Advance. Three *application* servers operate as a cluster using Veritas technology and are configured with 4 CPUs and 64 GB of main memory, each scalable to 8 CPUs and 192 GB of memory. Two *database* servers use Oracle 10g Real Application Clustering (RAC) for high availability and are configured with 4 CPU's and 48 GB of main memory, each scalable to 8 CPU's and 192 GB of memory. For our Clinical Applications (such as our TruCare clinical system), we use rack mounted Windows/Intel ("WinTel") blade servers operating in a virtual environment using EMC's VMware virtualization software technology.
Presentation Layer	We deploy virtual desktop and remote application support using Citrix XenDesktop, XenServer, and XenApp products. Centene was selected as a finalist in the 2010 Citrix Innovation Award for our rapid deployment of virtual desktops. All LHC programs, applications, processes and data are maintained and run centrally at our datacenter and our virtual desk-tops connect to our centralized IT resources via our high-speed network. We configure, provision, and use a standardized desktop environment for all Centene and LHC staff. The desktop operating systems include Desktop Windows Server 2003, SP2 with Citrix XenApp 4.5 for thin clients, and Windows XP and SP for desktops and laptops. We use IBM WebSphere technology web and portal platforms operating on Red Hat Enterprise Linux. WebSphere Portal Server (WPS) is used to integrate our electronic business applications across multiple computing platforms, using Java-based Web technologies.
Network Layer	LHC staff connect to our core applications via Centene's Wide Area Network (WAN), consisting of a virtual full-mesh, private IP Multiprotocol Layer Switching (MPLS) network. We have a standard LAN configuration using 100 Mbps T100 Network Interface Cards and Cat5 dual port wiring. Internet access is provided through our OC-3 circuit, and 155Mbps Internet service is supported through a Cisco router; connected to redundant corporate firewalls (Cisco 6500s). Intrusion

Key Component	Description
	Detection Systems (IDS) are located within our trusted and untrusted segments. We also have De-Militarized Zones (DMZs) to provide segments for Web Servers, Domain Name System (DNS) Servers, and Secure Access Gateways. We provide remote access to our internal network through a Virtual Private Network (VPN) using Cisco's VPN 3000 Concentrator and also through encrypted sessions using Citrix Secure Gateways.
Telecommunications Layer	We use the Avaya IP Telephony platform with Dual S8730 Media Servers in our datacenter; capable of failing over to a redundant pair of Avaya S8730 Enterprise Survivable Servers (ESS) for back up and disaster recovery. Avaya G450 Media Gateways provide local connectivity at remote offices for analog, digital, and IP endpoints, and has a Local Survivable Processor (LSP) which can process calls in the event that connectivity is lost to the Enterprise network. Avaya Call Manager (CM) provides automatic call distribution (ACD) and advanced vectoring technology. CM provides the ability to support remote IP agents. Our managed private IP MPLS backbone is deployed in a fully meshed topology with vendor diversity, connecting our field offices and specialty company telephone systems using Voice Over IP (VOIP) technology, and providing multiple routing paths for high volume conditions. The voice network consists of dedicated local Primary Rate Interfaces (PRIs) and analog lines provided by the Local Exchange Carriers (LECs) and long distance PRIs that carry outbound toll and incoming toll free calls provided by Verizon. Call center prompts on the toll-free numbers for Member, Provider, and medical management services are designed using the Avaya Voice Portal.

Engineering Performance and Availability in Servers and Storage. Our multi-tiered hardware platform delivers highly available application services using Clustering, Server Virtualization and Blade Servers. For example, Hewlett-Packard's ServiceGuard® Server Clustering software allows us to deliver application services across a group of server nodes configured so that any one of the nodes can provide appropriate end-user access. In the event that one of the nodes is lost, the surviving nodes pick up the work load, averting a prolonged outage. With the use of VMware's Server Virtualization Infrastructure and High Availability Services, we deliver a fully redundant server farm capable of running a number of different application services.

Virtualization reduces our power consumption and air conditioning needs, and optimizes the amount of CPU power and data storage that we can house in our building space. Virtualization also provides high availability for our applications, and streamlines application deployment and migrations. The servers are automatically load balanced to provide the best performance. If one of the physical nodes were to fail, be taken out of service for maintenance, or experience higher than expected utilization, the application service automatically moves to another node in the server farm without any interruption to the application service (i.e. no impact to the user). All core LHC data (claims, Member, Provider, etc.) will be stored on an HP XP24000 SAN-attached Storage Array, with multiple paths to RAID 5 storage devices facilitating high performance and fault tolerant data access, and supporting extensive growth.

<u>The bottom line</u>: as Centene and LHC take on transactions for LHC members, DHH can be assured that we have the IT infrastructure in place today to reliably and quickly service those transactions. Please see Question R.1 for more information on our Capacity Planning methodology.

<u>An Open Standards, Secure and Highly Available Network Infrastructure.</u> Today, our local plan field offices connect to our core applications via Centene's Wide Area Network (WAN): a secure, high-performance, fault-tolerant network architecture designed for stability, interoperability and growth through a mesh design that provides multiple paths to and from each point. If one path is down, or not performing optimally, the request is rerouted through another branch.

Today, Centene provides a secure access medium for mission-critical applications including voice, video, and time-sensitive data. Our data and voice services are provided through a Dedicated OC-12 (622Mbps) SONET Ring Service (DSRS). The OC-12 provides a resilient ring topology that connects Centene headquarters with geographically diverse Local Exchange Carrier (LEC) Central Offices. All Centene Corporate data circuits use this Dedicated SONET Ring Service. Carrier diversity is established by using dual SONET ring service from two independent, inter-exchange carriers. Each SONET connection consists of a resilient ring topology that connects the corporate office to the service Provider's telecommunications infrastructure. Additional physical link protection is provided by establishing geographic diversity through physical separation of fiber routes.

Our primary WAN infrastructure consists of a high-speed, virtual full-mesh, Private IP Multiprotocol Label Switching (MPLS) network. Centene's corporate campus is linked to this MPLS infrastructure via an OC-3 (155Mbps) circuit transported within the OC-12 DSRS. Field offices are connected to the MPLS infrastructure using aggregated T1s bonded via Multilink PPP (MLPPP). Remote office connections range in bandwidth from 3 Mbps for smaller offices to 12Mbps for large regional offices such as will be the case with LHC's office.

Our local field offices have a Centene standard Local Area Network (LAN) configuration using 100 Mbps T100 or 1GB Network Interface Cards (we will install 1GB NIC's for the LHC offices) and Category 5 (Cat5) dual port wiring to each work area. The LANs are connected to our WAN using Cisco 2600/3600 switches which allow for extensive expansion and fast data transfer. Redundant WAN connectivity is established through a secondary Service Provider to enable *carrier-diversity*. This redundant network consists of multiple point-to-point T3 (45Mbps) and T1 (1.5Mbps) leased lines. LHC's office will be connected to this backup network through direct circuits to Centene headquarters. Multiple T3s enter our Centene headquarters location, with two of these T3s delivering remote T1 circuits to/from the LEC. A 45Mbps connection is provided for our dedicated business-continuity and disaster recovery site.

All Centene field locations are independent so that high-utilization in one location will not impact system performance in another. In the event an office loses its direct connection with Centene corporate headquarters, alternate route paths are available for redirecting traffic through backup connections on the secondary network. In addition, all network equipment used for primary and secondary service delivery is designed for high-availability using redundant component configurations.

In the event of complete system failure or environmental catastrophe, our Business Continuity Plan (BCP) provides direction for sustaining operations during any site disabling event. Network performance is monitored 24/7 from our Network Operations Center (NOC). Using Citrix and Avaya Voice-Over IP (VOIP) Phone Systems, our staff can access all of Centene's systems remotely to address issues. Staff can resolve issues any time, any place, and from any Centene-registered IP node to fully support the delivery of services.

Enabling Data Exchanges with Providers. Our data networking and server architectures allow us to provide several ways Providers can send and receive data from us. We have securely connected our network to several EDI clearinghouses. Providers are also able to submit HIPAA EDI claims, or enter claims online using our HIPAA Direct Data Entry (DDE) support via our Secure Sockets Layer (SSL) secured Provider Portal, as well as perform a number of other query and entry transactions such as eligibility inquiry, claim status inquiry, authorization submission.

Secure, High Capacity Internet Connectivity. Today, Centene provides field offices with Internet access through Centene's OC-3 circuit. The 155Mbps Internet service is transported and terminated on a Cisco access router. The access router is connected to redundant corporate firewalls (Cisco 6500s with Firewall Switch Modules). The Cisco 6500 Internet Access switches are connected to the internal network using Gigabit Ethernet over fiber. Centene's Internet infrastructure defines trusted and untrusted segments. Intrusion Detection Systems (IDS) are located in strategic locations within the trusted and untrusted segments to assist in the detection and prevention of security violation attempts, including unauthorized access attempts, denial-of-service attacks, or other malicious attempts to disrupt normal business activities. In addition to the trusted and untrusted zones, we have established De-militarized Zones (DMZs) to provide semi-trusted segments for Web Servers, Domain Name System (DNS) Servers, and Secure Access Gateways. We provide remote access to Centene Corporation's network through a Virtual Private Network (VPN) using Cisco's VPN 3000 Concentrator and also through encrypted web access sessions using Citrix Secure Gateways.

Using Industry Standard Desktop Operating Systems. For all of our staff at Centene and our field offices, we configure, provision, maintain and use a standardized desktop environment, and each desktop is maintained in compliance with our software upgrade policies. Please see Question R.7 for details on the desktop hardware and software we use today and that we will deploy for LHC.

Data Center Facilities: Designed for Dependable, Reliable Operations. Centene's Data Center is located in St. Louis, Missouri and is home to all of the core application services that will be furnished to LHC. Our Data Center is equipped with four Uninterruptible Power Supplies (UPS) providing redundant, battery back-up power to all IT equipment. In addition, the building is also equipped with a three Megawatt, 6,600 gallon diesel generator capable of supporting all IT services in the event of a prolonged power outage. We execute a full load test annually, switching all power loads to the generator, to validate the generator's effectiveness. Less than 15 seconds is required to automatically switch to backup generator power resulting in *zero* downtime for the IT infrastructure.

Environmental Safeguards. Temperature and humidity levels in the Data Center are controlled through three Liebert high capacity precision air conditioning systems. The loss of any one unit does not affect our ability to maintain safe temperatures. All environmental systems are tied into Centene's security system and send an audible remote alarm when temperature or humidity falls outside of predefined ranges or water is detected. We have environmental monitoring sensors located within the server racks and wireless temperature sensors placed throughout our Data Center that send out automated alerts when temperatures and/or humidity levels exceed defined thresholds. These alerts are sent to Centene's Network Operations Center (NOC) and key IT management staff so that we can respond promptly.

Fire Protection. Centene Data Center facilities are protected by an advanced fire suppression system, which includes a VESDA (Very Early Smoke Detection Alarm) system. This system takes air samples throughout the Data Center sensing particulates that are present in the air prior to actual combustion. The alarm system is integrated with the building alarm system which is connected to the local fire authorities. The fire suppression system is an Ecaro-25 Clean Agent Fire Suppression System. A pre-action water sprinkler system provides a second level of protection. Safeguards are in place to minimize the risk of accidental discharge of both the clean-agent and sprinkler suppression systems.

A Telecommunications Architecture Designed for 24 by 7 by 365 Operation. Centene's telecommunications hardware is the Avaya IP Telephony platform with an S8500 Media Server. Two

G650 Media Gateways provide redundancy and host the analog, digital, IP, and trunk modules for the system. Networking the S8500/G650s to our corporate facility S8720 Media Servers and G650 Media Gateways allows for multiple call path redundancy, both at a public ISDN trunk(s) and at the backbone Private IP circuit level. Active, redundant systems are installed at our SunGard facility for back up and disaster recovery. Avaya Communication Manager (CM) Version 3.1.4 delivers world class call routing and feature rich applications. For implementation of our CCN plan, LHC will be supported (as our other local plan offices are today) by automatic call distribution (ACD) and advanced vectoring technology. Avaya's CM 3.1.4 provides the ability to support remote IP agents, allowing maximum flexibility for distributing call agent workload as well as supporting disaster contingencies. Our managed private IP Multiprotocol Layer Switching (MPLS) backbone is deployed in a fully meshed topology with vendor diversity, connecting our field offices and specialty company telephone systems using Voice Over IP (VOIP) technology, and providing multiple routing paths for high volume and emergency conditions. The voice network consists of dedicated local Primary Rate Interfaces (PRIs) and analog lines provided by the Local Exchange Carriers (LECs) and long distance PRIs that carry outbound toll and incoming toll free calls provided by Verizon Business. Call center prompts on the toll-free numbers for Member, Provider, and medical management services are designed using Verizon's Enhanced Call Routing platform.

Automated Systems Monitoring to Support MIS Management. Our architecture includes integrated automated management and monitoring at key points in our overall MIS. Please refer to R.3 for details on the software and systems we use to monitor our MIS in real time.

An Integrated Software Infrastructure. While our hardware, systems software, data and voice architecture will supply the requisite computing platform for LHC operations, it is through our *integrated business applications* that Centene delivers the functionality in service of our health plans, including LHC, and our State clients. Please also see our response to Section R.4 for more information on our integrated system software that supports an accountable, integrated care model. Our software applications integrate tightly via underlying standards based transactions, file interfaces, and a data storage array that retains pertinent information such as Member, Provider, encounter, and clinical case management activity. Our front-end clinical case management system (TruCare), claims processing system (AMISYS Advance), our Member data management and Member service system (Member Relationship Management), our secure Member Portal and Provider Portal, and our Centelligence™ reporting, business intelligence and decision support applications, access data from this array to provide our staff, providers, and members with comprehensive information to effectively manage the member's and provider's needs.

Centene's relational database design provides the flexibility and extensibility needed to quickly develop new methods for collecting data to meet the DHH's changing requirements. For example, AMISYS Advance, while having its own "built in" capabilities, is built with open application programming interfaces (API's) that allow our skilled MIS Application Developers to customize AMISYS Advance to meet the contractual requirements of DHH.

Please refer to Question R.14 for an itemized list of our software componentry. Continually Updating Our Architecture: Technology Refresh**.** Since the information technology industry and our businesses are in a state of constant change, Centene and LHC continuously search for new technologies that can lead to improving care for our members, and continually enhance service to our providers and state clients. Each year, we review all of our computing related equipment; our current hardware and software deployment compared with the latest product versions from our vendors; and the projected needs of our business for the following year. The output of this effort is our *Technology Refresh Plan* which serves as the basis of our overall IT Refresh Plan. Please see Question R.7 for more information.

State of the Art Data and Systems Integration. Today, our middleware software layer integrates and supports our local plan's business applications and data**.** Centene uses a Service Oriented Architecture (SOA) based on TIBCO and Informatica products to fully integrate all systems in a secure environment, from internal systems, including our MRM and PRM member and provider data systems, our AMISYS

Advance claims processing, our TruCare clinical care management system; to our front-end components such as our web portals and secure EDI gateways. TIBCO and Informatica are industry leading middleware software vendor and an early adopter of the Service Oriented Architecture (SOA) paradigm.

Centene's SOA strategy builds in these MIS advantages:

- **Reliability**: Our middleware layer performs complete data interchange handling routines both within the Centene and LHC enterprise and with external partners. Our middleware layer handles both regularly scheduled and unscheduled data exchanges, and can respond to unexpected circumstances to maintain data integrity. An example of this latter situation is support for assured delivery and two-phase commit.
- **Security:** Ensuring secure, encrypted, data exchange between systems.
- **Availability:** Enables operational continuity of systems, by systematically shifting resources in the event of a component failure in our MIS.
- **Automation:** Eliminates tedious and error-prone manual tasks, such as scheduled file loads, back/ups, and data transmissions or receipts.
- **Scalability:** Supports increased workloads through either vertical or horizontal systems growth.
- **Adaptability:** Enables systems to communicate easily with each other using open, standard transaction messaging protocols.

Please see Question R.4 for more information.

An Enterprise EDI Architecture Supporting HIPAA Transactions & Code Set Standards. Nationwide, all Centene affiliate health plans support all HIPAA X12 Version 4010 transactions and code sets requested by our state clients, their subcontractors, and our provider communities. We are also well along in our HIPAA 5010 and ICD-10 planning and implementation projects, and will be ready to move to these versions in time for the US Department of Health & Human Services (HHS) compliance effective dates (per HHS Final Rule), and upon approval by the DHH, on 1/1/2012. Please see Question R.15 for more information on our plans for HIPAA 5010 and ICD-10.

Information Security

Centene uses a combination of rigorous safeguards, policies, monitoring tools, and automated business processes to ensure systematic, ongoing, and auditable adherence to HIPAA regulations, mandates, rules and standards per HIPAA Security (45 CFR 164), HIPAA Privacy (45 CFR 160 and 164), and HIPAA Transaction & Code Set (TCS) (45 CFR 164). We *are* and *have been* compliant with HIPAA on or before the respective effective dates of each HIPAA rule, including the HIPAA Security Rule. In short, our plan to continue meeting and exceeding HIPAA mandates centers on our existing, comprehensive, and constantly updated controls, policies and processes described below. Please see Question R.16 for more information.

Business Continuity Program (BCP). Centene's Information Technology (IT) Department will be responsible (with LHC) for LHC's emergency response continuity of operations plan, which we refer to as our Business Continuity Plan (BCP). Please see Question R.3, and Section M, Questions M.1 and M.2 for more information.

Applications for LHC: Functionally Rich - Integrated Where Needed

Member Eligibility. We receive Member enrollment, disenrollment, and eligibility files from our State clients or their Fiscal Agents using our CoViant software. Virtually all of our clients (as would the DHH Enrollment Broker (EB)) send us eligibility data via the HIPAA 834 enrollment and disenrollment transaction file. Our CoViant Diplomat Transaction Manager handles our automated, scheduled production file exchanges. Today we exchange data with many of our State clients (or their intermediaries) using Secure FTP, but we can support virtually all industry standard secure file exchange protocols. CoViant protects our file exchanges with access control, authentication, and secure

configuration features, and allows us to support our contractual requirements with our State clients (such as the Department) as they pertain to data exchanges.

Our EDIFECS EDI and TIBCO software suite in conjunction with Coviant – supports a wide range of file transmission acknowledgement protocols, including ANSI standard 997 and 999 (for HIPAA 5010), TA1, 831, 824, or state and/or Fiscal Agent proprietary formats if needed.

We encourage the use of acknowledgements for both file transmission and receipts - as a control for assured delivery, data integrity, and record balancing. Once we receive eligibility files, TIBCO automates the steps in eligibility processing, while providing visibility into the status at any process step for our local plan (e.g. LHC) and Centene operations management. We automate eligibility processing scheduling runs (daily, weekly, monthly or other frequency) thru our TIDAL Enterprise Scheduler (TIDAL) job scheduling software - for example: we will automate the electronic retrieval from the EB and the processing of the DHH's daily output 834 and weekly and monthly roster 834; as well as our transmission to the DHH EB of updated member demographics.

Our EDIFECS HIPAA compliance software and TIBCO middleware programs will receive the 834 enrollment and eligibility files from the EB, validate and map each data item to the membership input file format of our MRM system, which immediately will make this data available to AMISYS Advance.

TIBCO also applies edits such as those for duplicate Member records, date criteria validity, field data integrity, and valid date spans - all prior to load into MRM. Any Member records that trigger edits will default into an Exception Report where they are systematically corrected using data correction routines. Corrected and clean original records will be loaded into MRM Member tables through Add, Delete and Modify transactions with accurate begin and end dates.

Our MRM is a master data management and contact management system specifically designed for member related data and processing workflow needs in health care administration. MRM will allow LHC to view and interact with our CCN members in the context of that member's *total* relationship with us - demographic, administrative, wellness, and clinical. In addition, MRM will enable us to identify and establish linkages amongst members in a family - in the case of DHH, by using the Responsible Person field in loop 2100 G of the EB's 834 and weekly and monthly Roster 834. TIBCO will feed eligibility data into MRM for systematic processing and dissemination to our other MIS components (including AMISYS Advance) and our subcontractors. Please see our discussion below in for details on MRM. Once eligibility data is loaded and processed in MRM, that data will be systematically promulgated to our TruCare utilization and care management system , our MACESS.exp (MACESS) our claims pre-processing, document workflow, and customer service platform, and our Centelligence™ Enterprise Data Warehouse (EDW) data integration engine.

Through EDW, we also make Member eligibility data securely accessible to our providers online via our secure Provider Portal.

Finally, today we transmit member eligibility data to our subcontractors (and in the case of the LHC CCN, our sole claims paying subcontractor is OptiCare Managed Vision® (OptiCare) – LHCs affiliated vision benefits subsidiary and subcontractor.

Imaging. MACESS provides us with an imaging and Optical Character Recognition (OCR), and scanning. Please see Question R.7 for more information, as well as Question R.5 and R.6.

Member Services: The Member Relationship Management System. We provide a *powerful* automated Member services functionality - through our **Member Relationship Manager** system to support all aspects of our Members' relationship with our plans (including LHC). Please refer to Figure R.11-A for the following discussion. The three concentric circles in Figure R.11-A represent multiple types of interactions among:

- MRM (item 1 in Figure R.11-J),
- LHC Member services staff and outward facing applications (item 2), such as our secure LHC Member Portal, and
- Our Members (item 3)

Centene's MRM will enable LHC to identify, engage, and serve our members in a holistic and coordinated fashion – across the breadth of their wellness, clinical care, administrative and financial matters related to DHH's Coordinated Care Network (CCN)

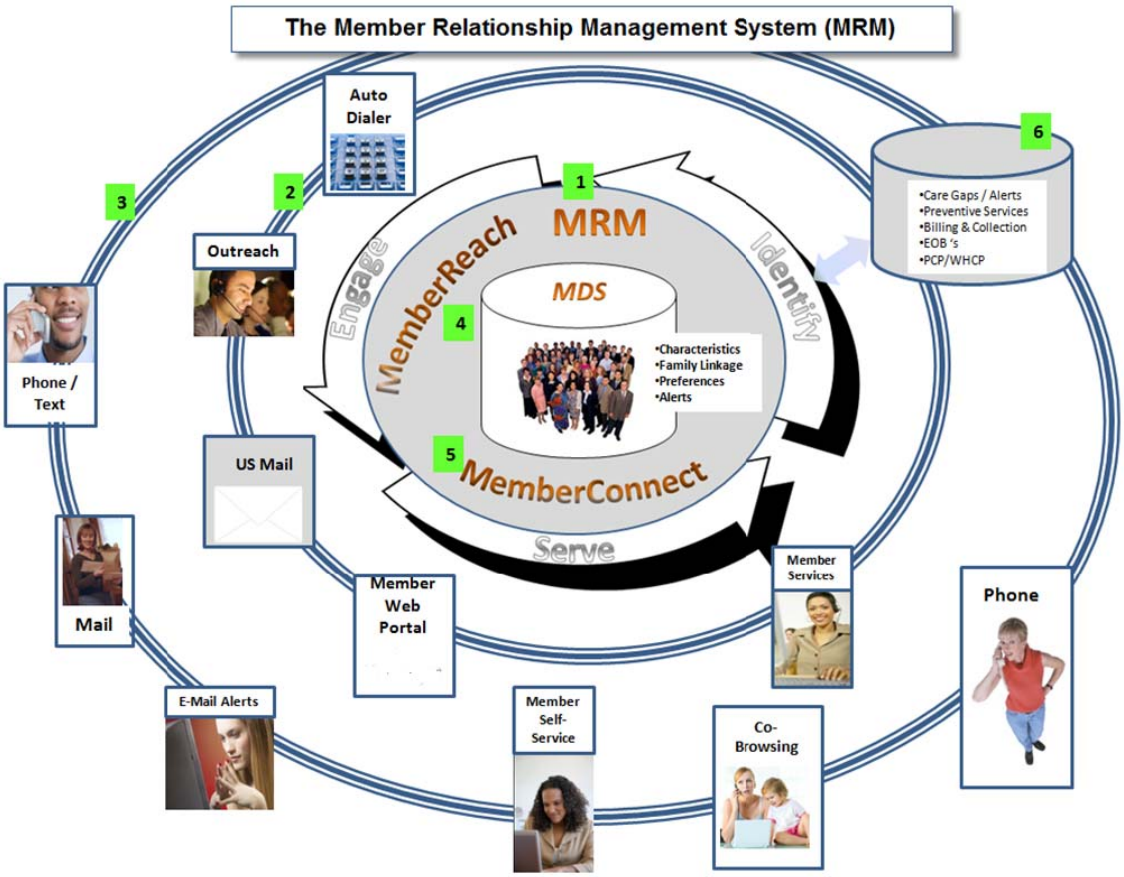
MRM will be our one integrated repository of "all things member" and will have 3 core integrated components:

- ***Member Demographics System*** (MDS - item 1). MDS is similar in design to a Master Patient Index application in that it employs a Master Data Management (MDM) approach to member data. Our MDM design provides processes for collecting, aggregating, matching, consolidating, quality-assuring, persisting and distributing member data throughout our organization to ensure consistency and control in the ongoing maintenance and application use of member data.
- ***MemberReach.*** (Item 4) will automate, manage, track and report on our workflows for *outbound and outreach* Member campaigns as well as targeted outbound interventions (such as engaging high risk members in disease management programs).
- Through MRM's third component, the ***MemberConnect*** module (item 5), MRM expands the efficiency and extent of member (and member family linkage) information that we can collect, transmit and display.
  - For example, MRM will support *inbound campaign management*: situations where, if a member who we have been trying to reach (but have been unable to contact for whatever reason - e.g. incorrect phone number in our records) – calls us for any reason – our LHC Member Support Representatives (MSRs) will be able to address the member's immediate issue – and address the issue(s) that we have been trying to communicate to that member. By way of illustration, suppose a CCN member were to call us with a general question concerning their benefits. Independently, suppose we had been trying to contact that member thru MemberReach because our Centelligence™ Predictive Modelling system (powered in part by Ingenix Impact Pro) had detected an important gap in care for that member, but we could not contact the member due to incorrect phone number and/or e-mail that we had on record for that member. In this situation, when our MSR pulls up the calling member's record, the MSR will see that we need to connect the member with one of our care or disease managers or other staff on our Integrated Care Team (ICT). The MSR will address the caller's question - and then offer to "warm transfer" the member to our clinical staff. A "warm transfer" is a phone transfer where the MSR stays on the phone line with the member while connecting to our clinical staff - to ensure a smooth conversational transition from member-MSR to member-ICT professional. The MSR then hangs up to allow the Member and ICT staff to continue talking.
- Item 6 represents the data interfaces MRM will have with our data integration engine, Centelligence™ EDW (please refer to R.10 for more information on Centelligence™ and EDW). Through these two way interfaces:
  - EDW can post outreach *alerts* - automated flags set in MDS that will instruct MemberReach to contact the member in the most appropriate manner, and in ways that the member prefers. For example, if a member registers to use our LHC Member Portal, the member will be able to set up user preferences on what and how they would like to be reached, including phone and/or e-mail. Depending on the severity of the outreach alert, MemberReach may issue an e-mail to the

member. No Protected Health Information (PHI) is conveyed; the e-mail will provide a link back to the LHC Member Portal to allow the member to log in to the Portal and retrieve their message.

- Conversely MRM can *send* data from or about the member to the appropriate business application.

Figure R.11-A



MemberReach. MemberReach will enable **outreach campaigns and targeted messages or interventions**.

<u>Campaigns</u> will include:

- Automated Predictive Auto Dialing (PAD) using our Avaya Voice Portal (AVP) as well as outbound calls queued up by MemberReach to be placed manually by LHC outreach staff for a particular reason (e.g. administration of Health Risk Assessment). Our outreach staff will work outbound call queues displayed by MemberReach.
- General US Mail mailings on new or existing LHC programs or information on specific programs - sent to members who may be interested based on Centelligence™ Foresight analysis or other aspects of their profiles in the MRM database (MDS).

<u>Targeted Messages or Interventions include</u>:

- Initiating PAD calls to members where we have important medical information specifically for them and optional e-mail alert (where the Member has "opted in" that they would like to be notified of such matters via e-mail in their LHC Member Portal profile. Examples:
- A member has not received a wellness examination within acceptable timeframes.
- A new member has not chosen a PCP and/or has not yet completed a Health Risk Assessment

- Depending on severity - calls from our Integrated Care Team (ICT) concerning an identified care gap (either identified thru Centelligence™ Foresight - or by the CCN Care Manager via any other means and documented in our TruCare system).

MemberConnect. MemberConnect will support and enhance our call center Member Services functions in several ways:

- Basic **Contact Relationship Management** (CRM) functions including call inquiry entry, categorization, routing, follow/up tracking, management and reporting.
- Support for **PCP information:**
  - Our MSR's will have the ability to update PCP assignment for a member upon member's request. As an alternative, the member him/herself will be able to update their PCP choice via the secure LHC Member Portal.
  - MemberConnect will also have the ability to display the PCP assignment of the member - for viewing by our MSR's.
  - Our PRM Provider Data Management system will electronically feed LHC Provider information to MRM's MDS, where it will be accessible by an MSR using MemberConnect or a member via our Member Portal, enabling the member (either via the web or by phone with our MSR's) to change their PCP assignment based on characteristics such as location, ethnicity, language spoken, and specialty.
- Support for "**Inbound Campaign Management"** (as discussed above)
- **Co-browsing**: that is, the ability of our Member Services Rep (MSR) to view (with the consent of the Member on the phone) what the member is viewing on the Member Portal.
  - **EXAMPLE:** suppose a member calls LHC Member Services while the caller is online, for example: *"I am on the web and I have a question on how I can order a replacement CentAccount Card?"* With MemberConnect's co-browsing capability, the MSR can see what the Member is seeing and to explain the situation: *"Yes, I see what you are talking about. Here is where you need to click and this is how you can order a replacement CentAccount Card..."*

Member Demographics System. The Member Demographics System (MDS) represents the data storage and data integration component of MRM and will store, maintain, manage, and interface with our other business applications, all key attributes concerning our Members - including:

- **Demographics:** Including information we receive via DHH's 834 enrollment and eligibility files; as well as Family Linkage data (see discussion below)
- **Claims Payment Information:** Information on claims paid on behalf of the Member by LHC as well as pharmacy information (obtained through DHH).
- **Wellness and Care Gap Alerts:** Preventive Services alerts/reminders; information comes to MRM via our Centelligence™ Foresight application and our EDW data integration engine
- **Member Preferences:** This includes items such as:
  - PCP assignments (as discussed above)
  - "My Web Account" information for the member's access to the Member Portal. Specifically: the member's sign/on information, e-mail address, and other preferences.

Member Services: The LHC Member Portal. Another key component of our MIS support for Member service is our secure LHC Member Portal, offering a number of self-service, wellness and care features that we will specifically tailor for CCN Members.

Our secure LHC Member Portal will offer LHC members the "informational tools" they need to help them take personal accountability for their health care by providing important basic information (such as eligibility and benefit information); helping them understand what they have to do (care gap alerts, wellness reminders, and other health information); and providing self-service support tools (such as the ability of the member to choose or change their PCP online, print a temporary ID card, exchange secure

messages with our staff, and manage their Member Portal web account information and preferences). Our web based portals access secured content supplied through our Enterprise Data Warehouse (EDW) and supporting business applications. For further information on our LHC Member Portal services please see Section K, Question K.5.

Provider Data Management: PRM

Our integrated Provider Relationship Management system (PRM) enables our health plans (including LHC), and their operational departments and call centers to: (a) handle *more* inquiries *more* efficiently and accurately, while supporting the local nuances and emphasis particular to each plan; (b) systematically reach out to providers when needed; and (c) manage a broader range of member & provider data and provider contracts in more holistic and integrated fashion.

Provider Relationship Management (PRM) is our next generation ***provider services inquiry & provider data management*** application, powered by Microsoft Dynamics contact relationship management (aka "CRM") software, *and* our Portico enterprise provider data management system, as well as our Emptoris enterprise contracting system. PRM is integrated with our Provider Portal, Amisys Advance, our Automatic Workflow Distribution (AWD) claims workflow system, and Avaya Voice Portal (AVP - for voice recognition enabled IVR and outbound campaigns).

PRM has <u>four components:</u>

- **<u>ProviderConnect</u>** is our application for creating, routing, tracking, managing, and reporting (via Centelligence™ Insight reporting - see R.10 for more information) provider inquiries. The main users of ProviderConnect are Provider Service Representatives (PSR's) - but PSR's can send and receive work items (provider inquiries) to any other operations department (including Member Services Representatives), using ProviderConnect.
- **<u>ProviderReach</u>** is our automated outbound Provider campaign management application; allowing the efficient and coordinated launch of broad based (plan level) provider communiqués, notices, and recruitment across multiple communication channels including telephone, e-mail, fax and web.
- **<u>Portico</u>** is our provider data management system which contains "all things provider" related information. Please see Question R.4 for more information.
- **<u>Emptoris</u>** is our comprehensive provider contract management software, enabling powerful and efficient contract administration, management visibility, and proven controls to reduce healthcare procurement and IT costs, improve the management of LHC and provider agreements, and ensure regulatory compliance.

<u>Managing Provider Contracts.</u> **Emptoris** complements Portico by providing full electronic storage of Provider contract information. We will use Emptoris to manage provider contracts, and to issue relevant reminders to our local LHC contracting staff when documentation, approvals, and other such contract updates are needed. Our data management processes support the HIPAA NPI, from provider set up, through Provider Directory updating, to claims and encounter processing.

TruCare - Service Authorization and Medical Necessity Review. TruCare is our member-centric health management platform for collaborative care coordination; and case, disease, and utilization management. All clinical staff at LHC - TruCare which is integrated with McKesson's industry leading InterQual evidence based medical necessity criteria (MNC) software to automate all workflows related to clinical decision support criteria, prior authorization and medical necessity review. Together the integration of TruCare and InterQual afford us **evidence-based criteria** to give us a consistent, detailed guideline approach to help our medical and behavioral utilization managers on the CCN to determine medical necessity and the appropriateness of covered services requiring prior authorization. McKesson updates their evidence-based clinical guidelines regularly through a development team of over 60 clinical specialists, and a recurring vetting process which includes a multi-specialty medical and behavioral panel

of over 800 clinicians. Today, the InterQual software is grounded in more than 16,000 citations from the medical literature, and from a variety of acknowledged and accepted sources.

Unlike many clinical care and prior authorization systems, TruCare's technical design centers on the member and not clinical cases. This allows our clinical care and utilization managers to focus on the member's care holistically and not in terms of fragmented services - particularly important for our members with behavioral and medical conditions requiring a coordinated case management approach.

Clinical workflows are integrated into TruCare and are task and queue driven - allowing staff to rapidly respond to caseload and authorization request demands in the most efficient manner possible. In addition, TruCare automatically generates a care plan and allows case managers to assign health outcomes. We also configure TruCare for authorization "auto approvals" when conditions merit: for example, we can configure the system to auto approve maternity admissions. Prior authorization data is fed systematically from TruCare to AMISYS Advance for consistent, efficient claims adjudication. TruCare also accommodates the documentation of key metrics directly by our CCN users which allows our case management staff to track services for *hybrid* HEDIS reporting.

As with all our PHI handling applications, TruCare is only accessible to appropriate clinical operations staff, and even then, TruCare uses Role Based Access Control to ensure a finer granularity of *who* can see what data for *which* Members and perform *what* operations on that data.

Claims Processing Centered on AMISYS Advance. Centene accepts HIPAA 837 EDI electronic claims directly from providers or their authorized intermediaries via our HIPAA compliant EDI architecture and for CCN Providers, via leading clearinghouses. We also offer HIPAA compliant Direct Data Entry (DDE) of claims via our secure Provider Portal. Please see Question R.13 for more information on our offerings and assists to providers, encouraging them to submit claims electronically and receive electronic payments from us.

HIPAA EDI format adherence is verified real-time using our **EDIFECS** compliance software which improves our claim auto-adjudication rate and the quality of the downstream encounter data we process and submit to our State clients.

Providers can also submit paper claims, which are scanned using Optical Character Recognition (OCR), indexed and converted to machine readable data through MACESS. EDI and paper claims data are processed through our EDIFECS and TIBCO software to map, translate, and validate the data, ensuring that common edits are consistently applied to both paper and electronic claim submissions. AMISYS Advance, our claims processing system, is one of the health care industry's premier health plan administrative systems, providing HIPAA-compliant eligibility and claims processing. We will configure AMISYS Advance to comply with DHH and federal claims processing requirements and timeframes. AMISYS Advance delivers accurate claims payment with configuration capabilities to price according to fee schedules, per diem rates, capitation scenarios and many other complex pricing arrangements.

ClaimsXten® reviews adjudicated claims *prior to payment* for such items as bundling and unbundling of services, incidental services, mutually exclusive codes, global surgery follow-up days, duplicate claims, invalid procedures, bilateral services, and incorrect age/gender validation. When an edit is warranted, the software recommends the most likely clinical situation or replaces codes that were inappropriately billed. When changes are made, the claim is re-priced, based on the new codes. ClaimsXten provides LHC with nationally recognized guidelines and practices, and is flexible, allowing us to modify rules to local practice patterns and DHH regulations. We also employ the services of HCI (a unit of Verisk, Inc.) for systematic and high speed analysis of claims prior to payment - for potential fraud, waste, and abuse (see Section Q, Question Q.1 for more information).

As mentioned above, Centene offers a variety of payment options for providers, including Electronic Funds Transfer (EFT) and/or Electronic Remittance Advice (ERA) directly to our Providers, through a clearinghouse, or through our, provider-friendly **PayFormance** and EMDEON ePayment capabilities.

Explanation of Payment (EOP) information is also available to Providers through our secure Provider Portal.

Encounter Processing. Once claims are adjudicated to a finalized status, they will be prepared for submission to the DHH as encounters through our Medical Data Express (MDE) Xpress Encounter Pro - system (Encounter Pro). Encounter Pro provides encounter tracking, history and resubmission functionality, and is based on years of Centene and MDE's experience processing Medicaid encounters. Through Encounter Pro, the entire encounter submissions process comes together: starting with inbound claims submissions from providers; ***through*** accuracy and completeness checks performed by LHC; to submissions to the DHH and receipt of DHH's acknowledgement and process results files; and subsequent reconciliation on each encounter.

In April, 2010, Centene was awarded the 2010 Gateway Business Innovation Award for our Desktop Executive

Quality and utilization management. TruCare, integrated with our Centelligence™ informatics tools, allows LHC clinical staff to proactively identify persons with high needs through analysis of utilization data.

Centelligence™. Centene and LHC will utilize a state-of-the-art business intelligence platform to monitor a wealth of operational and quality metrics. Several distinct applications comprise our Centelligence™ business intelligence environment including our Enterprise Data Warehouse, our Ingenix® Impact Pro™ and Centene proprietary Predictive Modeling system, MedAssurant Catalyst QSI HEDIS reporting application, our SAP Business Objects decision support and reporting suite, and our Informatica Power Exchange and Change Data Capture software. Informatica extracts transactions in near real time from our core applications (AMISYS Advance, TruCare, MRM, PRM, and Encounter Pro.) and populates these transactions into the EDW in near real-time. We produce ad hoc and standard reporting through the use of SAP BusinessObjects Web Intelligence.

Our BusinessObjects software, in conjunction with EDW and our Informatica software, form the components of our Desktop Executive Dashboard which provides real-time intelligence for our local plan management (e.g. LHC) and is updated daily to provide early warning of adverse trends, claims drill-down for a quick analysis of clinical, financial or operating issues, and predictive modeling. All metrics are calculated and stored for historical analysis and trending. Reports can be produced in various formats, such as Microsoft Excel, Microsoft Word, and Adobe Acrobat PDF.

Centelligence™ EDW. This Centene proprietary business intelligence and data management platform, powered by Teradata's Extreme Data Appliance relational database technology, serves as the foundation of LHC's data integration and reporting strategy. In addition to the reporting capabilities of the EDW, a data integration engine enables seamless incorporation of external data such as pharmacy data, lab test results, etc.

Centelligence ™ Foresight: Centene has significantly augmented our existing predictive modeling capabilities with the integration of Impact Pro with our Centelligence Foresight system. Impact Pro is a multi-dimensional, episode-based predictive modeling and care management analytics tool that will allow LHC to utilize clinical, risk, and administrative profile information, and provide more targeted health care services to our CCN members. Impact Pro identifies care intervention opportunities which are electronically fed back into EDW for import into our TruCare clinical management system, as well as our MRM system, triggering subsequent action by relevant case or disease managers, and / or automated actions in our MRM system.

Centelligence ™ HEDIS Reporting via Catalyst .A key component in managing better health outcomes at lower costs is our ability to continually evaluate performance against specific, measurable outcomes. LHC's Quality Improvement (QI) Department will work closely with DHH to in DHH's HEDIS quality measuring efforts. To evaluate and report on our performance, LHC QI staff will work with Centene's

Health Economics and IT Department using MedAssurant's NCQA Certified Catalyst QSI Software in conjunction with our EDW and BusinessObjects software for analysis and reporting. A combination of these tools will provide LHC and DHH comprehensive metrics for HEDIS, Provider profiling, and LHC and DHH specific quality improvement projects.

See Question R.10 for more information on Centelligence™ and its integrated data management and decision support analytics modules.

Question R.12

Profile of Current and Proposed Information System Organization

R.12 Provide a profile of your current and proposed Information Systems (IS) organization.

Centene Corporation (Centene), will manage MIS and claims operations for LHC and support our local IS, operations, and managerial staff with over 275 experienced Information Technology (IT) professionals and 450 claims staff. Since its inception in 1984, Centene has focused exclusively on Medicaid and other public sector managed care programs and has successfully addressed the MIS needs of our affiliate plans, state clients, and public sector providers for effective, results-driven health plan administration. Today, Centene's MIS organization supports coordinated care for 1.6 million Americans enrolled with our affiliates in 11 states and over 85,000 public sector medical and behavioral providers.

MIS Support. IT staff supporting LHC's MIS are located primarily in Centene's corporate headquarters in St. Louis, Missouri. In our experience, MIS functions are best centralized to take advantage of the synergies created through combining technical expertise with multi-state/multi-product operations. LHC's members, providers, and DHH will benefit from best practices in information technology and data reporting from across the country. LHC will have *business owners in all key functional areas in Louisiana* who will work closely with the corresponding Centene MIS staff, enabling LHC's members, providers, and DHH to benefit from *both* centralized IT best practices and data reporting *and* the knowledge, expertise, and quality of care provided through a strong local presence in Louisiana.

Centene's Chief Technology Officer will serve as LHC's ***Information Management and Systems Director*** to oversee all CCN information system functions, including interfaces with DHH and DHH's enrollment broker and fiscal intermediary, as well as all other MIS functions serving LHC and the CCN Program, including our network providers. Centene's Director of Business Continuity, who will serve as LHC's ***Business Continuity Planning and Emergency Coordinator***, will work closely with LHC, and specifically with the Louisiana based IS Liaison, to create, manage, maintain, oversee, and exercise with all Louisiana staff emergency management, response, and disaster recovery plans. Each leader's qualifications are described below, with a brief description of the experience of all our IT senior leadership team. LHC's ***IS Liaison*** will be located at the LHC office in Baton Rouge and will ensure local MIS Security, provide support to end users, and provide local computing resources such as, network equipment, computer servers, and desktop systems.The IS Liaison will also monitor change requests with the Service and EDI Help Desks and assist the Centene Network Operations Center (NOC) and Systems Administrators with any technical issues at any of our Louisiana locations.

MIS functions based in St. Louis are divided into six major areas, described in the narrative below the included charts.

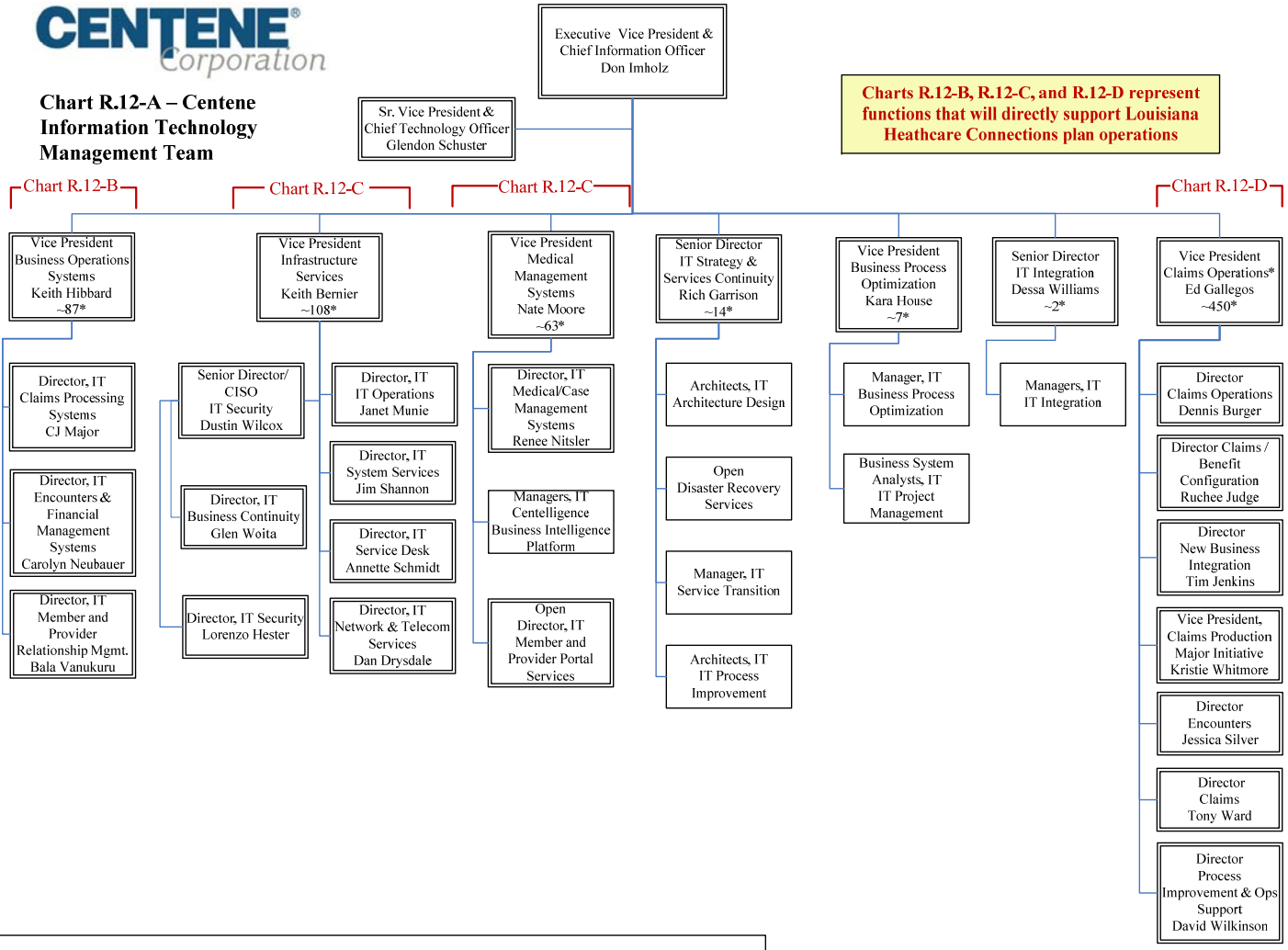
Claims Department Staffing. Centene's Vice President of Claims and Encounters will serve as LHC's ***Claims Administrator*** and will oversee all major claims processing functions and systems used to pay claims in accordance with DHH and federal requirements; claims quality and timeliness standards; and third party liability and recoupment processes. Please refer to our response for sections Q.1, Q.2, and Q.3 for a detailed description of our claims processes. Two local claims professionals will support LHC. The ***Claims Liaison*** will trend performance issues; develop and update policies and procedures; issue related bulletins when work processes change; and ensure correct implementation of any process improvement changes. The Claims Liaison will also analyze root causes and recommend changes to workflows and system configuration to improve performance and productivity. The LHC ***Provider Claims Educator*** will be our hands-on leader on all provider education opportunities related to claims. They will work directly with our provider community to ensure understanding of claims submission requirements; assist the Provider Services Call Center and Electronic Data Interchange (EDI) help desk in identifying training opportunities; measure provider satisfaction and address issues through outreach and training to increase EDI claims submission and Electronic Funds Transfer.

An IT Organization To Enhance Integration. Please see Charts R.12-A through R.12-D and related narrative below for a graphical depiction of Centene's current IT and Claims organizational structure, staffing, and qualifications, including the functions performed at a local level. Please refer to Question B9 for a description of our overall LHC organization and an organizational chart showing the integration of our MIS and Claims Operations staff with the LHC team.

LOUISIANA HEALTHCARE CONNECTIONS

CENTENE Corporation

Chart R.12-A – Centene Information Technology Management Team

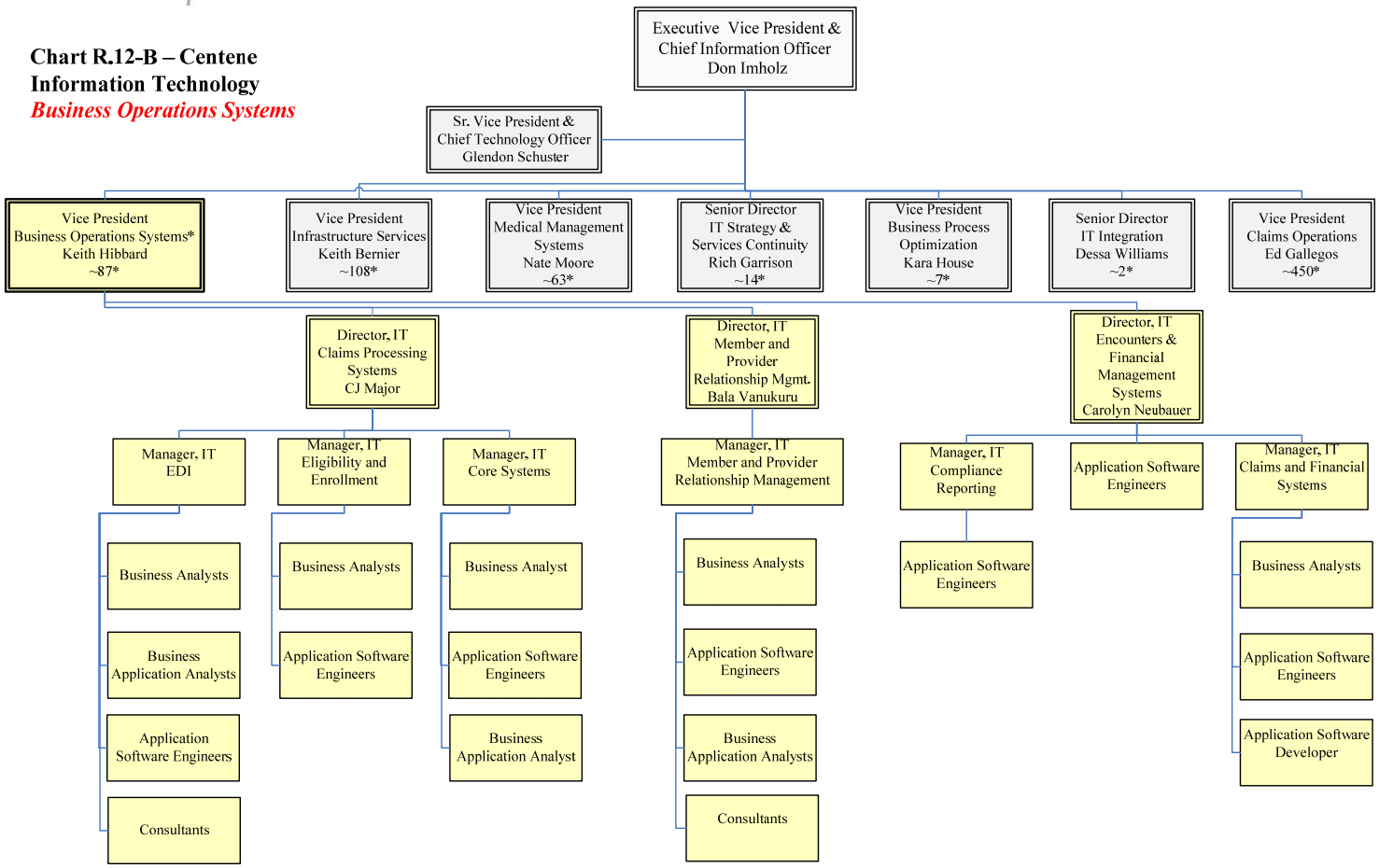


* Indicates the number of Full Time Equivalents (FTE) in the corresponding department as of June, 2011.

LOUISIANA HEALTHCARE CONNECTIONS

CENTENE Corporation

Chart R.12-B – Centene Information Technology
Business Operations Systems



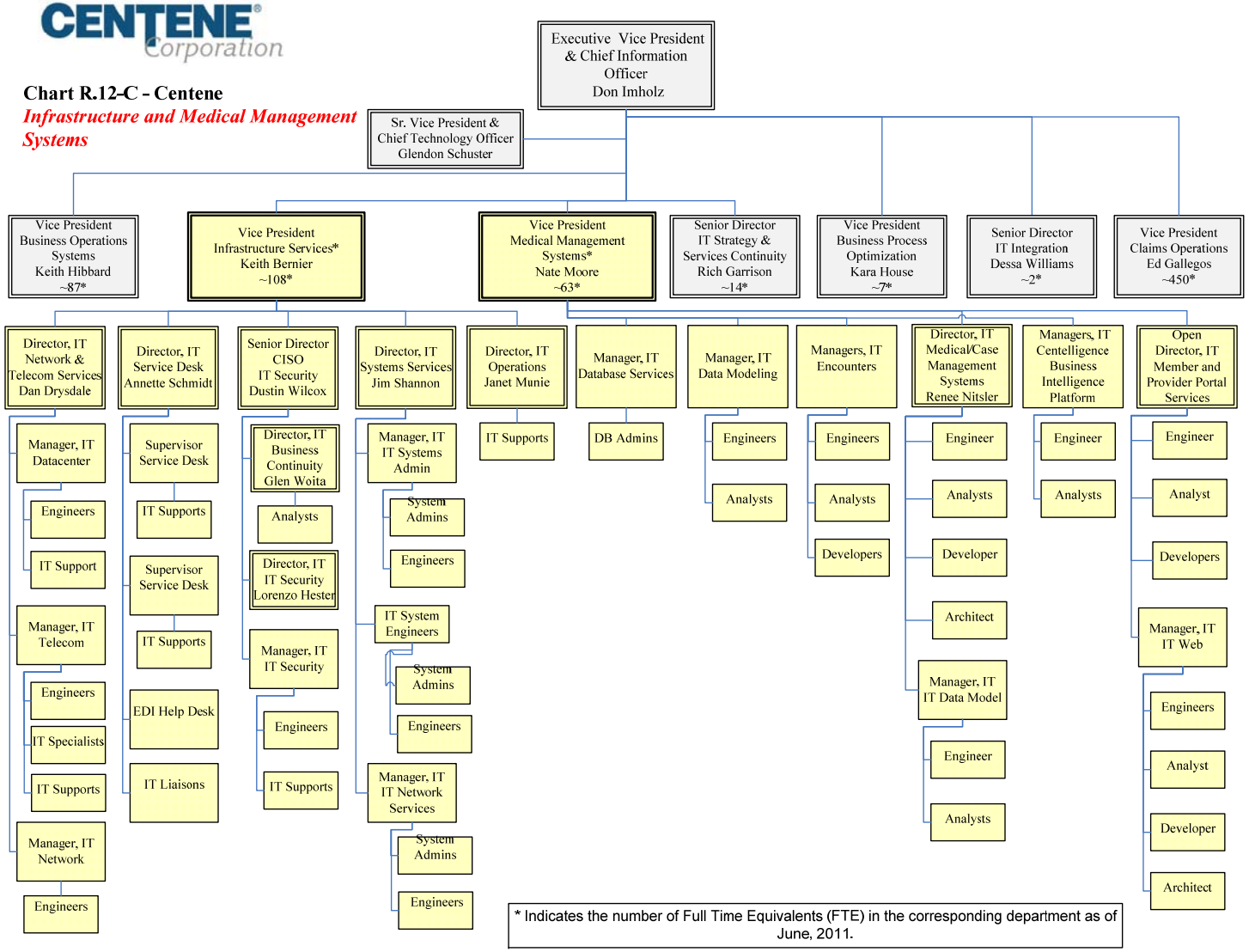
* Indicates the number of Full Time Equivalents (FTE) in the corresponding department as of June, 2011.

LOUISIANA HEALTHCARE CONNECTIONS

CENTENE Corporation

Chart R.12-C - Centene

Infrastructure and Medical Management Systems

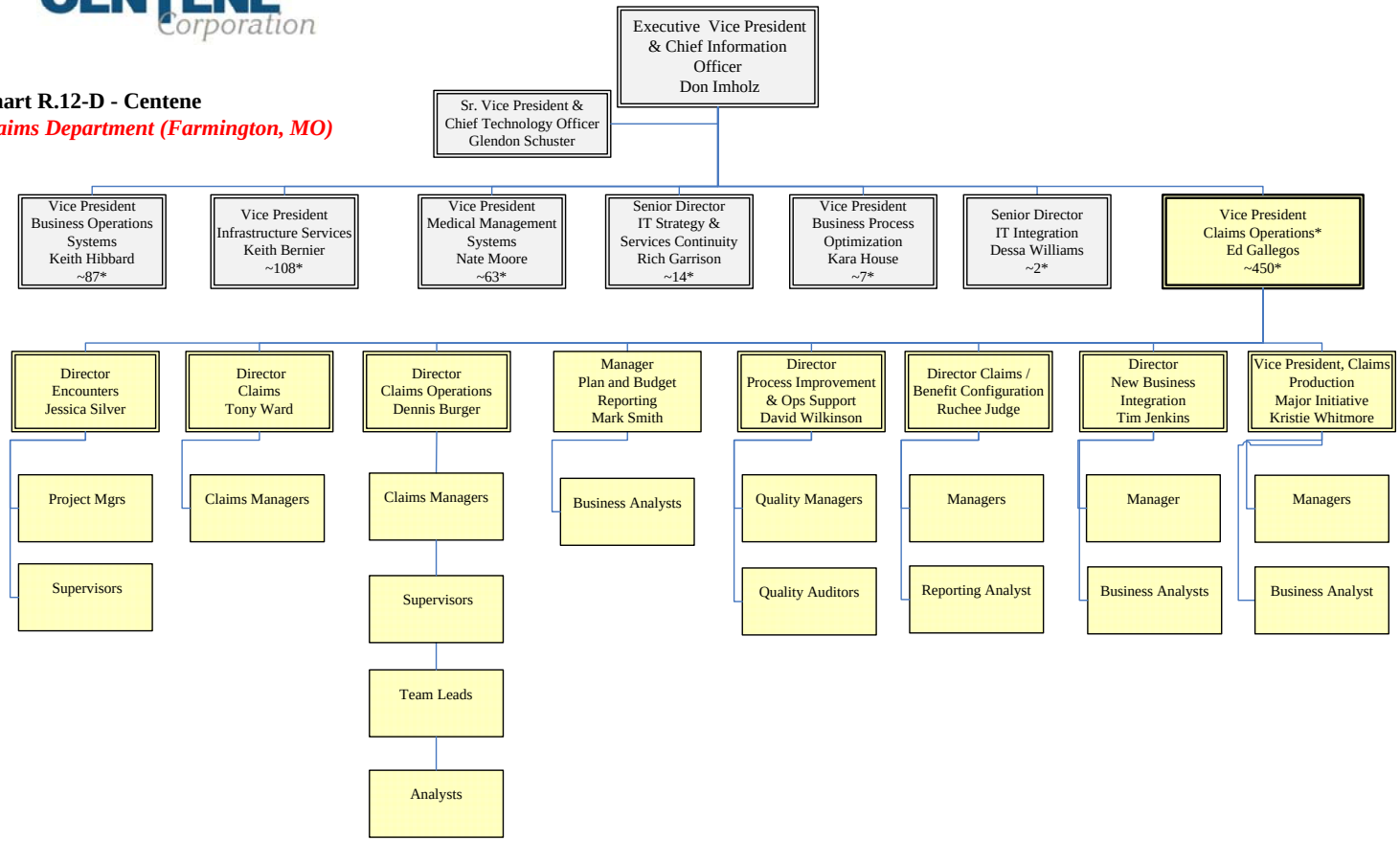


* Indicates the number of Full Time Equivalents (FTE) in the corresponding department as of June, 2011.

LOUISIANA HEALTHCARE CONNECTIONS

CENTENE Corporation

Chart R.12-D - Centene
Claims Department (Farmington, MO)



* Indicates the number of Full Time Equivalents (FTE) in the corresponding department as of June, 2011.

Executive Vice President & Chief Information Officer, Chief Technology Officer, and the Vice Presidents are located in St. Louis, MO

The majority of the claims staff who will support LHC are in Farmington, MO

Chart R.12-A: MIS functions are divided into *six major areas* reporting directly to the ***Chief Information Officer (CIO)*.** The four areas that directly involve health plan operations are depicted in **Charts R.12-B** through **R.12-D**. The other two areas, depicted in Chart R.12-A, include IT Strategy and Service Continuity and Business Process Optimization, which also will benefit our LHC operations and include:

IT Strategy and Service Continuity. This group reports to the Senior Director of IT Strategy & Services Continuity and provides architecture design services to address business goals, direction, and growth. They provide architecture design expertise for new business implementations, as well as researching and recommending new and emerging technology solutions that have meaningful application in support of our health plans. To ensure effective and compliant service delivery, this team is also responsible for capacity management, to evaluate current use of IT services and projecting future needs; and release and change management, to ensure the smooth and controlled release of business services into production. The IT Strategy and Service Continuity team, along with the Infrastructure Services team, is responsible for the implementation of new facilities, such as our new data center and all our local LHC offices; and the Information Systems Disaster Recovery processes for Centene.

Business Process Optimization (BPO). By using the Six Sigma and Lean Six Sigma methodologies, the BPO team works across all functional areas of the organization, evaluating the interaction of processes to ensure proper alignment with business objectives, performance, and financial outcomes. The BPO team proposes, develops, and implements continuous process improvements and best practice solutions to ensure delivery of quality services and adoption and smooth transition of new and existing business requirements. For example, our BPO Team recently uncovered an opportunity for more efficient distribution of member care gap information derived from our predictive modeling software. The BPO Team led a cross-functional team with representation from medical management, case management, member and provider services, and our IT organization. This ultimately led to a software modification: the secure search and display of care gaps via Centene's Online Care Gap Notification feature. Please see section R.7, R.11 and R.15 for more information on the Care Gap feature. Where their analysis leads to technology solutions or change, they are an integral part of the development team, facilitating requirements gathering, documentation and developing training materials.

IT Integration. This team focuses on new health plan *implementations*, integrating new business within existing health plans and aligning critical health plan priorities with on-going IT development activities and release schedules to ensure on-time delivery of new features and enhancements. The IT Integration team ensures repeating "Best in Class" performance from previous implementations and integration projects, strengthening Centene's response to challenges, collaborating efficiently and effectively with business partners, providing consistent and repeatable reporting metrics and eliminating waste and duplication in order to ensure speed to market.

Chart R.12-B: Business Operations Systems. Led by the VP of Business Operations Systems, this team maintains our *primary business operations systems,* providing systems leadership and expertise during new program implementations to ensure accurate, complete, and secure flow of data with our business partners, and to ensure that the unique requirements for our state clients' programs are configured and managed comprehensively within our core administrative systems. The Business Operations Systems group includes the following teams:

AMISYS Advance Support. This team directly supports EDI, Eligibility and Claims Payable/Reporting teams. The AMISYS Advance Support team coordinates work between Centene and DST Health Systems, Inc. (the creators of AMISYS Advance), as well as the applications we have integrated with AMISYS Advance, such as ClaimsXten (clinical claim editing software from McKesson, Inc.).

Claims Payable/Finance and Claims Reporting. This team customizes the claims payable, finance, and reporting components of AMISYS Advance according to the requirements of the state and state

compliance officers. They also work on programming interfaces with vendors/banks for Electronic Funds Transfers (EFT).

Compliance Reporting. Using a variety of tools and data from the Enterprise Data Warehouse (EDW), the compliance business intelligence team develops standard and ad-hoc reports for state agencies per state contracts (as interpreted by plan compliance officers and validated with our state clients) and as requested by health plan management.

Electronic Data Interchange (EDI)**.** The EDI team develops and programs solutions for service oriented architecture (SOA) and electronic data interchange to support the communication between applications and services provided to our health plans, members, providers, and state agencies including all HIPAA compliant and proprietary transactions between these entities.

Eligibility. The eligibility and remittance team identifies and documents individual state requirements and customizes the member eligibility and demographic portions of AMISYS Advance accordingly, as that eligibility data pertains to claims processing.

Encounters Reporting. This group is responsible for ensuring that encounter data systems are configured to support the various needs of state agencies and in accordance with contract specifications. This team is also responsible for managing the day-to-day operations of the encounters submissions as specified by the Encounters Business Operations (EBO) group and our Health Plans.

Member and Provider Relationship Management. This team is responsible for the configuration and on-going support of our member and provider relationship management tools including all provider management systems: prospecting, credentialing, enrollment and contracting functions within our Provider Relationship Management (PRM) system. This team also configures our Member Relationship Management (MRM) system for member master data management, including the administration of our master member index. Please see Questions R.4 and R.11 for more information on MRM and PRM. The team also configures our Microsoft Customer Relationship Management (CRM) system for DHH call tracking specifications for providers and members. Finally, the team works across the organization to ensure accurate provider and member data integration across the Information Technology platform, such as member and provider data in AMISYS Advance for claims processing functions.

Chart R.12-C: Infrastructure Services. Our infrastructure team supports the foundation of our information and telecommunication services ensuring a highly available, secure, and HIPAA compliant MIS environment. Within the Infrastructure Services group are the following teams:

Business Continuity. This team is responsible for the life cycle of business continuity services, including business continuity plan development, writing, and exercising, which is repeated annually to meet state regulatory compliance and internal governance requirements. This team facilitates crisis management, disaster recovery exercises, awareness, and pandemic planning. They also own the relationship with SunGard who provides Centene and all our health plans with work area recovery resources such as our brick and mortar and mobile recovery units that will serve as a workplace for our employees in the event an office location is damaged or unusable.

Database Services. This team provides expertise in data architecture and modeling to deliver data to systems and end users in an efficient and controlled manner. They are responsible for daily management and administration of databases and work closely with other teams moving, backing-up, and restoring data as needed.

Network Services. The Network Services Team manages Telecommunications, Networking, and Messaging Services by planning, building, administering, and monitoring these services. They ensure the stability and performance of Centene's LAN/WAN circuits for all corporate, health plan, and specialty sites. Within Network Services, the Telecom team manages our telephony system for the corporate Voice Over IP (VOIP) system, all call centers, and cellular devices. They ensure that telecom services are configured through call management applications according to business need and they manage and monitor the equipment, hardware, and provider relationships to provide these services.

IS Operations. IS Operations oversees job scheduling and execution, making sure jobs necessary to run our applications and services are processed in correct order, begin at the appropriate time and are completed accurately. The data center team also monitors facilities, ensuring power and cooling are functioning appropriately. Along with the IS Security team, they also manage asset inventory services for all IT assets (NOTE: Asset management at an aggregate level is managed by the Centene's Finance Department, although detail inventories are tracked within IS Operations for integration with our Configuration Management Database.) IS Operations is also responsible for the management of the Storage Area Network (SAN) support team, which includes storage and backup administration.

IT Security. IT Security is responsible for establishing and maintaining the confidentiality, integrity, and availability of all information technology services. They set and enforce policy and services to meet HIPAA regulations as well as internal levels of information security established by management. This department also oversees user access requests that come through the Service Desk and investigates security incidents.

Service Desk. The Service Desk provides the interface between Information Technology services and our employees and external users of our systems (e.g. such as authorized DHH users). They serve as the single point of contact for all users and they handle all incidents, access, and service requests related to IT either by resolving them directly or escalating them through the proper channels. They are responsible for logging all requests and for following them through resolution and closing. Our Electronic Data Interchange (EDI) Service Desk provides direct support to our Providers' technical staff, providing assistance with EDI.

System Services**.** System Services oversees and administers servers, operations and provides *second tier application support*. Within Systems Services, the server team is responsible for the build and administration of servers and the operating systems on which our applications run. They provide back-up and restoration services, application administration, and second tier application support. This team is also responsible for the support of various infrastructure and middleware applications including WebSphere, Tibco, and SharePoint.

Chart R.12-C: Medical Management Systems. Our Medical Management Systems team will work closely with LHC's Vice President of Medical Management, to configure our integrated Medical Management applications to support quality, coordinated managed health care delivery. This team maintains the Care Management/Service Coordination systems, advanced analytics applications for quality and HEDIS reporting, predictive modeling, assessments and risk profiling, and business intelligence tools to assist in identifying opportunities for care. This team also architects and models our Enterprise Data Warehouse (EDW), so our Business Intelligence team can offer a flexible and intuitive framework that securely delivers accurate, actionable information. Our External Web Services and Portal teams develop and maintain our Member and Provider Portals, and our Internal Web Services team supports CNET, our internal web communications service. Within the Medical Management Systems group are the following teams:

Medical Management Systems**.** According to state specifications, the Medical Management team configures TruCare, our integrated health services management platform, to the requirements of DHH including in- and out- patient authorization requirements, Health Risk Screening questionnaires, triggers, rules, and alerts.

Centelligence™. This team is tasked with providing management and health informatics to internal users developing strategic solutions and offerings to increase service levels and improve business operations. They focus on the ongoing enhancement of our Centelligence™ informatics and reporting capabilities, including our Catalyst QSI (HEDIS Reporting), Impact Pro (one of the predictive modeling components in our predictive modeling system, along with Centene proprietary software) and Impact Intelligence (our provider profiling and clinical quality improvement system). The team also works with our Business

Intelligence team and all our health plans aligning overall Enterprise IT initiatives in support of new business implementations.

Enterprise Data Warehouse - Data Integration. Leveraging our Informatica Extract/Transform/Load (ETL) software, this group designs and implements solutions to receive data from a variety of sources, stage, transform and load it into our Enterprise Data Warehouse (EDW). The EDW is the central component underneath our integrated, service oriented architecture and this team ensures the data is normalized and ready to be consumed by all systems that need the data. The team also designs the solutions and tools that support the exchange of health information between the EDW and other organizations, such as Emdeon, through whom we deliver explanation of payment and electronic funds transfer payment solutions to our providers, and Healthcare Insight (HCI) who supports our claim processing and fraud, waste and abuse detection efforts. Please see section J, question 2 for more information on our use of HCI.

Web Services & Portals. The Web Services and Portals team provides the external web solutions used by the general public as well as the extensive features of our secure member and provider portals. This team is also responsible for the development and on-going maintenance of internal web based solutions, known as Intranet Services, or CNET.

Chart R.12-D: Claims Operations Center. The VP of Claims Operations will oversee the processing of LHC's claims by a *Louisiana-dedicated unit* within the Claims Operations Center. The claims operations center identifies and trends performance issues, develops and updates policies and procedures, issues related bulletins when work processes change, and ensures any process improvement changes are implemented correctly. The claims operations team also analyzes root causes and recommends changes to workflows and system configuration to improve performance and productivity. Within the Claims Operations Center group are the following teams:

Claims Operations. This team is responsible for the timely, accurate, and efficient processing of all claims and correspondence. This includes the initial receipt of all paper and electronic claims, appropriate scanning, vertexing, routing and adjudication of over 24M claims per year. In addition, various provider contact center teams provide first time resolution on any claims related inquiries.

Benefit Configuration. This department is responsible for the accurate and timely system configuration and coding of all benefit, fee, and pricing change requests for accurate claims processing. This includes the validation and interpretation of contract rules and agreements, system coding, user acceptance testing, migration to the production environment and ultimately auditing for configuration accuracy.

New Business Integration. The team is responsible for full end-to-end implementation of new health plans. This includes detailed analysis of the initial RFP for full understanding of the contract, benefit and system configuration, claims and encounter testing and development and monitoring of post implementation progress.

Encounters. The department is fully accountable for the successful submission of encounters to the state. This includes partnering with the various health plans and associated state entities for testing of encounter submissions. Their goal is to achieve a 98% acceptance rate for all encounters.

Process Improvement and Operational Support. This dedicated team works in coordination with our Business Process Optimization department (described above) and has primary accountability to improve the overall efficiency of the claims department through the use of various analytical tools including *Six Sigma* and *Lean* methodologies. This team also includes the claims audit team whose data serves as input to the various projects that lead to further operational efficiencies.

Experienced Leadership

The Public Sector MIS experience of our 275 IT professionals will ensure a smooth introduction of Louisiana Healthcare Connections (LHC) in Louisiana. One hundred percent of our IT staff and resources

are focused exclusively on managing Public Sector programs: a critical differentiating factor of our organization. Below is a brief description of the experience our senior leadership team brings to LHC and DHH in service of the Louisiana Medicaid program.

Donald Imholz

Executive Vice President, Chief Information Officer

Donald Imholz has worked in Information Technology for 30 years, the last 3 of those years in healthcare as CIO for Centene. Previous to this appointment, most of Don's career was in Aerospace where he held executive positions in all aspects of Information Technology. Don served as the CIO for all of Boeing Defense Systems, as well as in other management positions where he was responsible for all application development and support on a global basis. Don also worked outside of IT several times, with executive assignments in Engineering, Manufacturing, Finance, and Program Management. He is a thought leader in IT Strategy, Business and IT alignment, and system development processes. Don has extensive experience in delivering large, complex solutions and integrating systems and organizations. Since joining Centene he has aligned IT with business priorities, implemented best practices in system management, and migrated the organization to an Agile system development process. Don has led the transformation of Centene's system architecture, with virtually every system having been either significantly upgraded or replaced over the past three years. This has resulted in greatly improved scalability and enhanced business processes. Centene IT has been recognized with several awards, among them, inclusion among the Information Week 500.

Glen Schuster

Senior Vice President, Chief Technology Officer (LHC's Information Management and Systems Director)

Glen Schuster has worked in Information Technology for 17 years, 15 of those years in healthcare. For the past six years, he has served as Senior Vice President and Chief Technology Officer at Centene. Glen is a thought leader in Business and Systems Integration and Solution Delivery Excellence. He has deep experience in delivering large, complex solutions in healthcare and drives Centene's technology strategy to provide innovative solutions, such as Centelligence™ informatics and business intelligence platform, and CenTraCare, Centene's suite of information-based tools for our Patient Centered Medical Homes (PCMH's). He has successfully led Centene through many significant market expansions and continues to advance their business through application architecture, IT governance, and ensuring a strong, resilient infrastructure. In the last three years, Glen has led the efforts to work with Centene's states to promote Health Information Exchange (HIE) and help drive their markets to use Information Technology to help reduce costs and improve health outcomes.

Keith Hibbard

Vice President, Information Technology, Business Operations Systems

Keith Hibbard has worked in Information Technology/healthcare field for over 25 years, with 16 years focused on behavioral health. Over the past eight years at Centene, Keith has served as IT director over specialty product lines, Senior Director over IT Operations, and in the most recent two years as Vice President of Information Technology, Business Operations. Over his tenure at Centene, he has led the Information Technology areas related to: Provider Data Management, Business Configuration, Claims Operations, Clinical Data Management, New Business Implementations and EDI. Most recently, Keith has been responsible for the successful implementations of Member/Provider Customer Relations Management (Centene's MRM and PRM systems), HIPAA/NPI compliance, and EDI/X12 5010 compliance planning and execution.

Keith Bernier

Vice President, Information Technology, Infrastructure Services

Keith Bernier has worked in Information Technology for the past 17 years, 15 of those in the healthcare industry. The past five years he has led the Infrastructure and Operations departments at Centene Corporation with a focus on delivering reliable, secure, and scalable solutions. He has led large-scale datacenter transformations through the implementation of ITIL based methodologies and the use of

desktop, application, and server virtualization. He has successfully implemented highly available virtual call centers throughout the United States and continues to enhance customer support and satisfaction through the use of innovative technologies. For the past two years Keith has served as a member of the Citrix Customer Council.

Dustin Wilcox
Senior IT Director, Chief Information Security Officer
Dustin Wilcox has over 20 years experience in Information Technology with 15 years spent in both technical and strategic leadership positions. He has been a leading advocate in support of applied best practices in information security, compliance, and data privacy across a diverse array of industries including healthcare, financial services, defense, and energy. Since joining Centene in 2010, Dustin's leadership in business continuity planning and disaster preparedness has resulted in Centene being recognized as an innovator in the field of pandemic planning. Dustin holds or has held a number of advanced certifications including CISSP, CSSLP, GSEC, CCNA, and CNE among others. He currently serves on the Information Systems Advisory Board for the University of Missouri, St. Louis; is a thought leader at the Center for the Application of Information Technology (CAIT) Information Security Roundtable at Washington University in St. Louis; and is a leading member in the Metropolitan St. Louis CISO Roundtable.

Glen Woita
Director, Business Continuity (LHC's Business Continuity Planning and Emergency Coordinator)
Mr. Woita brings 19 years of deep industry knowledge in all phases of Business Continuity Planning (BCP), Crisis Management, IT Disaster Recovery and Audit Management. He is experienced across multiple industries with a strong focus on managed health care. His areas of expertise include enterprise wide-business continuity management, team building/facilitation, business recovery strategies and incident/crisis management delivery. His current responsibilities include planning for and managing crisis events impacting Centene and health plan operations. He also leads Centene's Pandemic Planning preparedness efforts, and participates on a local steering committee of business professionals to address the impact of a pandemic and bio-terrorism on local, county, state, and national levels. His track record includes strong professional relationships with C-suite management working within matrixed organizations and implementation of Six Sigma techniques to improve customer service and reduce expenses. Glen has been a Certified Information Systems Auditor (CISA) since 1994 and Certified Business Continuity Professional (CBCP) since 2000. He obtained Information Technology Infrastructure Library (ITIL) version 3 certification in October, 2008.

Nate Moore
Vice President, Information Technology, Medical Management Systems
Nate Moore has worked in Information Technology for 18 years, 13 of those years in healthcare. He currently serves as Vice President at Centene, with responsibility over our business intelligence and compliance reporting platform, Centelligence™, our medical management solutions, web portals, and mobile applications. Nate has extensive proven delivery experience using a variety of innovative solutions including market/health plan implementations, electronic health records, informatics and advanced analytics, and medical management platforms, such as the CenTraCare suite of technology enabled tools supporting PCMH's and Health Homes. The solutions delivered by his innovative leadership have been recognized regionally by *Gateway to Innovation*, and nationally by *Information Week*. In the last three years, Nate has led our efforts working with our provider partners to promote advanced medical management analytics and data integration to help reduce costs and improve health outcomes utilizing Information Technology.

Richard Garrison
Senior IT Director, IT Architecture, Technology Strategy and Service Continuity
Richard Garrison brings nearly 30 years of deep Information Technology knowledge and experience in advanced enterprise architecture and design techniques. Richard spent 17 years working for the Hewlett

Packard Company providing integration and implementation consulting services for complex infrastructure solutions for a diverse list of Fortune 100 corporations. He has both a keen understanding of broad technology solutions as well as the ability to communicate technical concepts with executive leadership. This has enabled him to assist Centene Corporation with developing and maturing a scalable, resilient, Highly Available IT Architecture to meet the company's growing business needs. Richard has introduced technologies and/or technology disciplines such as: Server Virtualization, Enterprise Storage, Information Service Management strategy, Standardized Operating Platforms as well as developing a robust Disaster Recovery program for Centene. Richard has also provided overall management/leadership on Centene's long term datacenter strategy which has resulted in creation of a new, 20 year life, corporate datacenter with a fully redundant disaster recovery datacenter. Richard joined Centene in 2004 and continues to provide strategic technical direction.

Kara House
Vice President, Business Process Optimization
Kara House has worked in the managed healthcare industry for over 10 years. At Centene, she has served as the leader of our Corporate Quality Improvement Department, and now serves our IS Department by applying her leadership in the areas of process improvement and optimization utilizing Lean Six Sigma tools and methodologies. Kara has experience in driving change, continuous quality improvement, maximizing efficiency, and implementing solutions that lead us to more efficient operations and better service to our customers.

Dessa Williams Hellige
Senior Director, Information Technology, IT Integration
Dessa Williams Hellige has worked in Information Technology for 19 years; 13 of those years in healthcare. She has a strong background in Electronic Data Interchange (EDI) transaction sets and translators, including 13 years in HIPAA related EDI transactions. Dessa started as a developer at Centene and has proven leadership skills that have placed her in roles implementing new lines of business as well as leading large scale software implementations. Over her tenure at Centene, she has led multiple Information Technology areas including member and provider related services, EDI, claims processing and payment, encounters and web. In the last 3 years, Dessa has led the effort to implement new technology around encounters and successfully implemented our IlliniCare health plan in Illinois.

Ed Gallegos
Vice President, Business Operations (LHC's Claims Administrator)
Ed Gallegos has worked in the healthcare industry for over 20 years; fifteen of those years have been leading and managing large scale claims and call center operations. He initially joined Centene as VP of Operations, which included claims and encounters processing, system configuration, operations training, audit, and quality improvement initiatives. In addition to his extensive operational experience, Ed held various key positions that included VP of Human Resources as well as VP of Diversity and Cultural Competence at Blue Cross and Blue Shield of Florida (BCBSF). His efforts at BCBSF in the latter role led to BCBSF ranking nationally among the top 50 companies for Diversity. He also successfully led BCBSF to national recognition in customer service as measured by J.D. Powers for three consecutive years. Ed is considered an innovative and results oriented individual as proven by his accomplishments over his career. He has broad and deep experience in executing large scale operational efficiencies while focusing on delivering exceptional customer service. His experience in leading national group health plan accounts such as General Motors, Ford, and the Federal Employee Program (FEP) and others resulted in favorable rankings in performance. He has made significant improvement in driving results at Centene since his arrival.

MIS Titles and Functions

The MIS titles and functions within the IT organization are:

Chief Information Officer (CIO), Mr. Don Imholz. Our CIO is responsible for the strategic direction of Centene's Information Technology organization. He reports to the CEO and Board of Directors. The CIO defines IT priorities based on business need and direction, provides adequate resources and training to implement quality IT solutions, and ensures continuous improvement of MIS management and business processes.

Chief Technology Officer (CTO), Mr. Glendon Schuster. Our CTO along with the CIO identifies business and technology trends through involvement in professional communities, stakeholders meetings and his participation as a member of the senior management team helps to establish direction and governance of the MIS organization. The CTO communicates the company's technology strategies to our state clients, stakeholders, and investors, and assures the successful execution of technology solutions through selection, development, and deployment.

Under the direction of these two positions, Centene's MIS is broken down into departments with specific functions which are described below. Each department is led by a Vice President or Senior Director. The positions and functions within the MIS organization are similar, with the difference being the service or solution provided. To eliminate redundancy – these positions and a functional description of each are listed, followed by a description of each team and their objectives.

Managers and Supervisors – They ensure quality deliverables are completed on time and within budget, employees are aware of their priorities and are developed professionally, and a healthy team environment is maintained. Reporting to Managers and Supervisors are:

Administrators – In their respective areas, they are responsible for the day to day operations of the systems within their area, running unscheduled jobs, reviewing results of scheduled jobs monitoring, and system documentation.

Analysts – They interpret and link business needs and objectives in application development and support activities. They analyze user requirements, procedures, and problems to automate processing or to improve existing computer systems. For example, a security analyst analyzes and identifies issues related to the security of IT systems and data, and proposes solutions to mitigate risk. A business analyst, analyzes business processes, identifies needs and problems, and works with teams to provide technology solutions.

Developers – They develop IT solutions and enhancements to existing systems using various programming languages. Developers are responsible for the quality of code used for programming and ensuring development is in line with designs and requirements.

Engineers – They drive the design of and build solutions that create, maintain, interface, or transform data to support a complete business need for their application module and understanding of how the application fits into a larger business context.

Solutions Architects – They are responsible for the analysis, design and development of the technology solution being delivered to the business cross-domain and cross-functionally to ensure that what is delivered will meet the requirements of the business within the framework of the IT environment.

Specialists – They interface between business end users and the IT organization addressing and resolving basic issues related to their service area. They are responsible for escalating to their technical specialists' issues that they cannot resolve.

Technicians – They have a sound technical understanding of the IT environment in which they work. Their function is to support their team in practical and tactical areas as opposed to strategic. A database technician, for example, might be engaged in creating tables, relationships and implementing the design of a database engineer.

Question R.13

Electronic Claims Submissions / Electronic Funds Transfers

R.13 Describe what you will do to promote and advance electronic claims submissions and assist providers to accept electronic funds transfers.

Centene and Louisiana Healthcare Connections (LHC) know from our claims processing reporting and analytics that an electronically filed claim results in a faster, more accurate process; allows us to utilize the information sooner in care of our members; and is better for our environment. Our experiential data shows that when providers prepare claims electronically, the time from service to submission to Centene is abbreviated by more than *half* the time compared to claims submitted on paper. This means that we obtain the data earlier, can process the claim faster, our Case Managers can utilize the information sooner in the care of our members, and we can display the information sooner to our providers via our secure LHC Member Health Record. Please reference our response to R.15 on how LHC will support the meaningful use of electronic health data. Our technology allows us to validate much of the data submitted at the earliest possible stage in the process, which results in more accurate and complete data received. Please see our response to Q.1 for more information on our claims processing capabilities and R.2 and R.4 for our data integrity processes and controls.

For these reasons, we aggressively educate and support our providers across all Centene health plans on the benefits and methods of Electronic Data Interchange (EDI) claim submission with the result that, between June 1,2010, and June 1, 2011, approximately 85% of all medical claims were submitted electronically to Centene across all our health plans. Likewise, LHC will mobilize our team of Provider Relations Managers, Provider Service Representatives, Case Managers, and others who work with our providers to encourage EDI claim submission.

We do recognize that provider capabilities related to submitting electronic claims vary based on a provider's technological support and expertise. We also recognize smaller providers face unique challenges. That is why we support a growing variety of online, EDI, and Electronic Funds Transfer (EFT) for claim payment options so each provider can select the best approach for their practice.

Enabling Electronic Submission of Claims

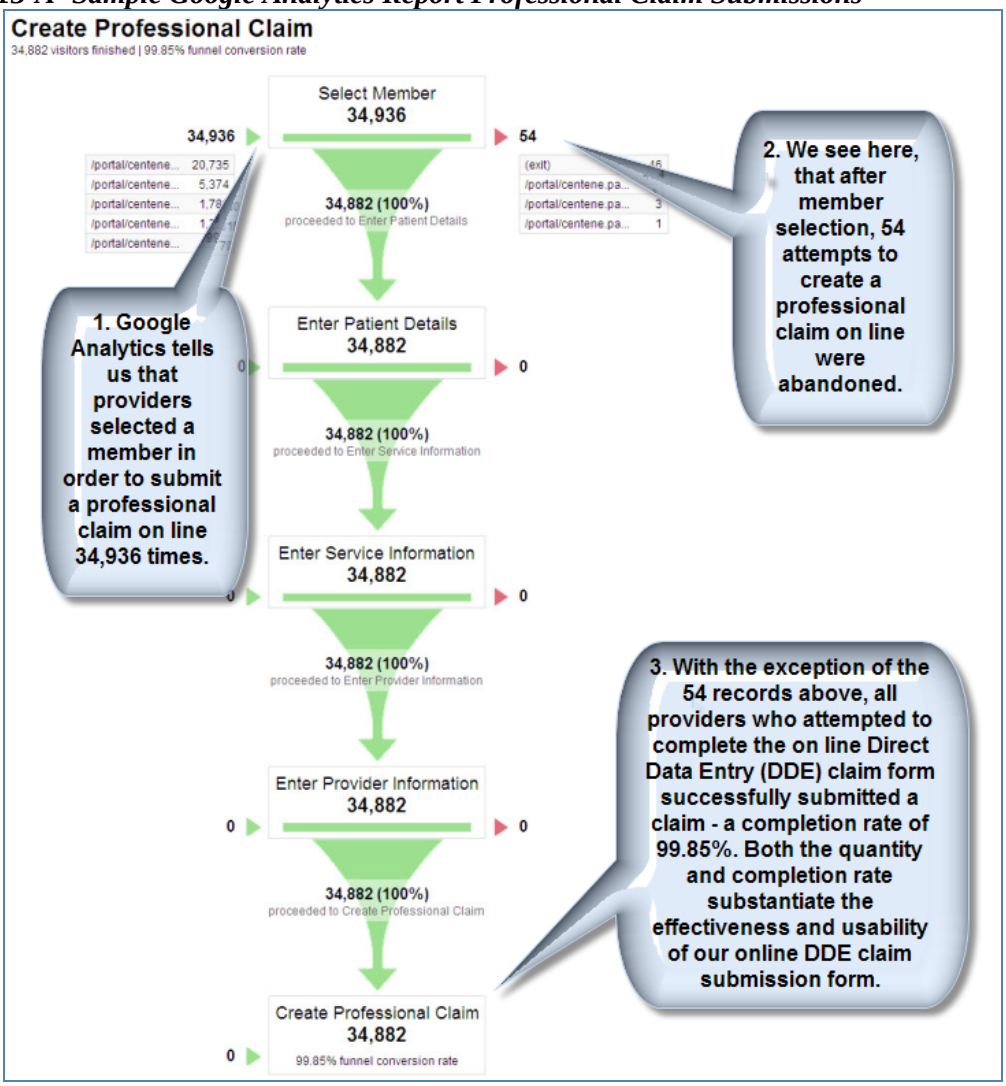
LHC and Centene will deploy multiple technical resources and business processes to encourage EDI submission of claims while we continue to look for new ways to enhance our tools and assist our providers in the claim submission process. Outlined below are several of the resources we have available today that we will provide to LHC providers.

LHC Provider Portal. We will customize a version of our Provider Portal exclusively for LHC. Providers who register for access to this secure web content will have access to multiple administrative self-service and clinical application tools. Among these are the following administrative functions that support and encourage EDI. Please see our response to R.15 and G.12 for more information on our Provider Portal.

Direct Data Entry (DDE) Claim Form. Today, our Provider Portals allow for the HIPAA compliant entry of individual *professional* and *institutional* claims via *form templates* directly through our Provider Portal. When claims are submitted utilizing this template on our portal, the data goes through the same rigor for data and field validation as do HIPAA 837 transactions. To encourage paper claim submitting providers to use this facility, when a provider submits a ***professional*** *claim* via our online Direct Data Entry (DDE) form, we will adjudicate that claim and post the final disposition of the claim on our Provider Portal within ***two business days*** of receipt *and* we will pay that claim on the next check run. This not only benefits LHC, but the provider as well due to rapid payment. If the provider signs up for one of our EFT options below, the transaction completes in an even timelier manner. If, for any reason, we are unable to meet this "two business day claim finalization" service level (e.g. claim is flagged for fraud investigation or medical necessity review), our *Automated Work Distributor (AWD)* claim workflow system will alert our LHC claims staff to contact the provider and help them understand the status of their claim. This service level is made possible through the integration of our Provider Portal, *EDIFECS*, AWD, and *AMISYS Advance*, our core claims processing system. See our response to Q.1, Q.3, and R.11 for more information on these *integrated* systems supporting our claims processes.

To illustrate how well-utilized and effective our DDE professional claim entry form is, we show production results for a one month period for one of our largest health plans in ***Figure R.13-A Sample Google Analytics Report Professional Claim Submissions*** below.

Figure R.13-A- Sample Google Analytics Report Professional Claim Submissions



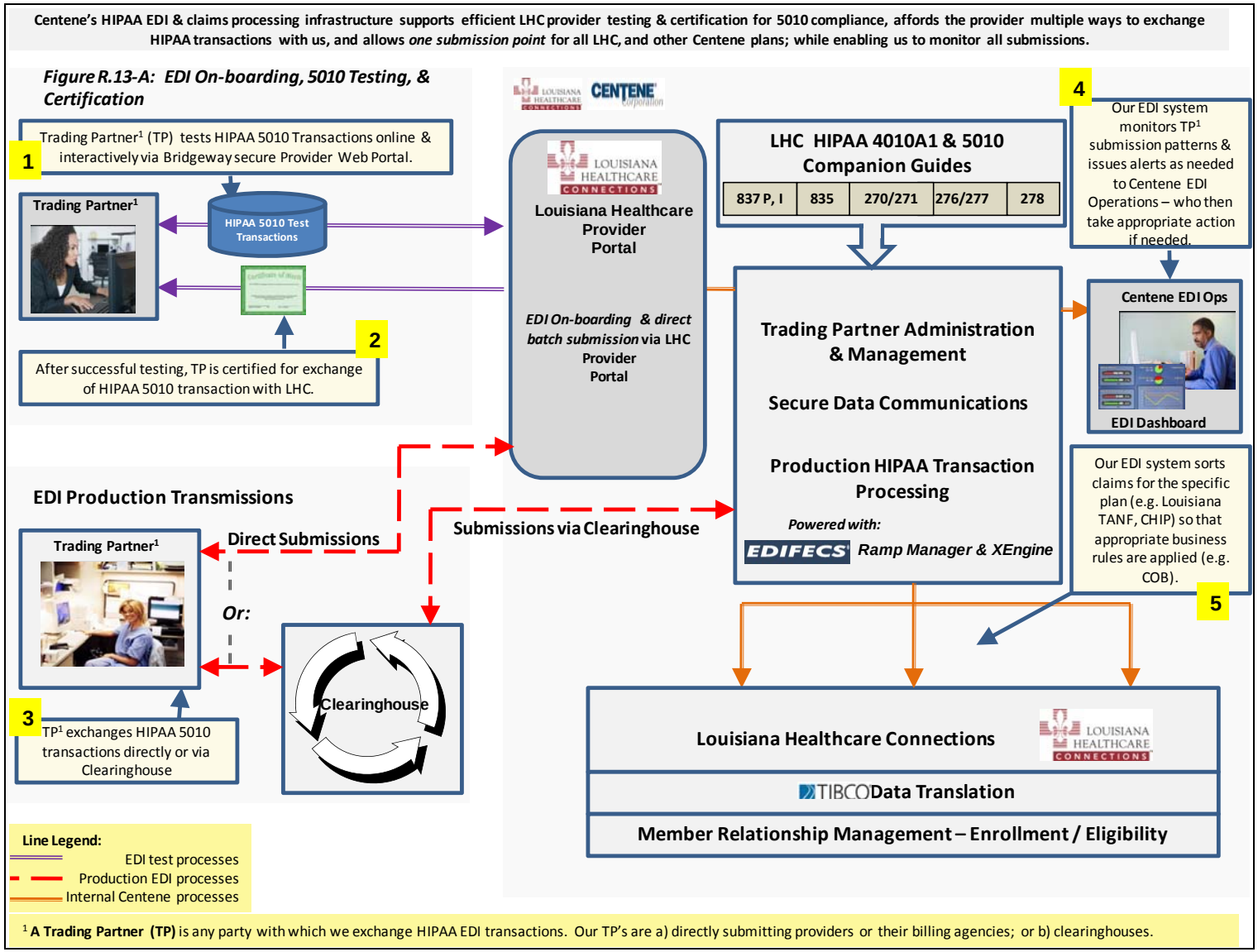
HIPAA 837 batch claims. We also support the online submission of HIPAA 837 batch claims directly through our Portals. Supporting this feature is our EDIFECS Ramp Manager tool which facilitates the process for EDI on-boarding. *EDIFECS Ramp Manager* is an interactive tool available on our Portal that allows providers to test their EDI transactions directly with us and, once approved, certify them for direct submission of HIPAA 5010 claim transactions to us via our Provider Portal. EDIFECS Transaction Manager, another component of our EDIFECS system, will allow LHC to continuously monitor provider EDI submission patterns and thus help to ensure consistent levels of EDI service. Please see ***Figure R.13-B EDI On-boarding, 5010 Testing & Certification*** below for a visual description of this process. Beyond claim and remit transactions, providers connecting directly through LHC and Centene via EDI will receive direct assistance from our EDI Help Desk to implement the broader HIPAA transaction set, including 270/271 Eligibility Inquiry and Response; the 276/277 Claim Status Inquiry and Response; the 278 Service Authorization Request and Response; and (for providers sufficiently equipped) HL7 based

transactions, such as the Continuity of Care Document (CCD) and Scheduling Interface Unsolicited (SIU) for collaborative scheduling. Please see R.15 for more information.

Claim Adjustments and Additional Claim Information. Providers will also be able to submit *claim adjustments* and *additional claim information* on our Provider Portal, such as an Explanation of Benefit (EOB) from another insurance carrier further ensuring that claim submissions are complete. Enabling a provider to submit this information to electronically through our Provider Portal rather than via paper mail or fax to LHC, enables faster overall turnaround time (TAT) in claim adjudication and payment.

HIPAA 837 Professional and Institutional EDI claims from multiple clearinghouses. Centene supports *over 60 trading partners* across 11 states who file HIPAA 837 EDI claims on behalf of our providers. In fact, we will accept claims from any clearinghouse that meets our performance and service quality standards and can implement our HIPAA companion guides.

Figure R.13-B EDI On-boarding, 5010 Testing & Certification



Enabling Electronic Funds Transfer

Like EDI claims submission, Electronic Funds Transfer (EFT) affords both our providers and LHC administrative and financial efficiencies, and we actively encourage our providers to sign up for one of the three EFT options we offer:

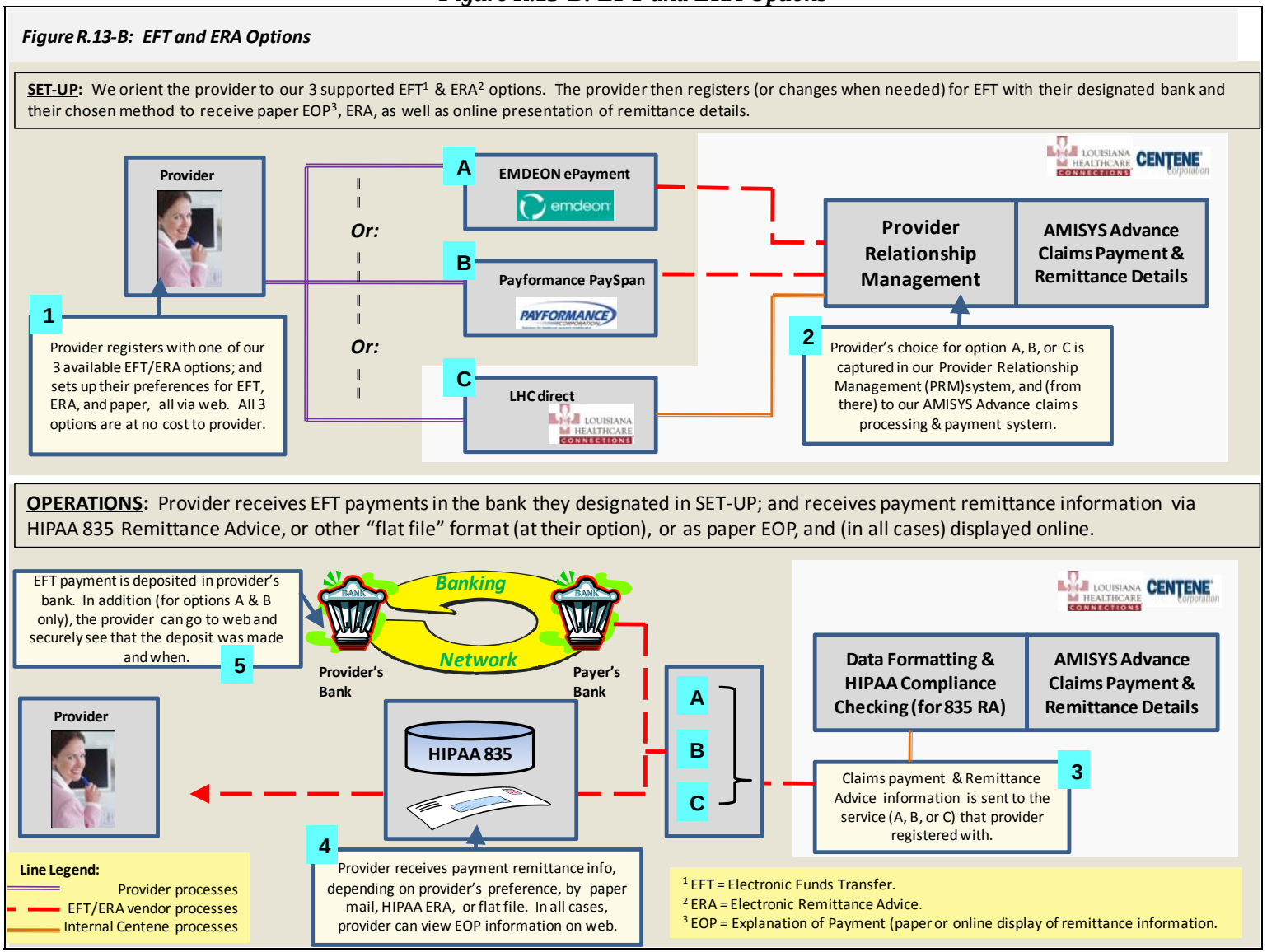
EMDEON ePayment (ePayment). Our providers will be able to go to the ePayment site, register, and set up their bank account for EFT. Once set up, the provider can view remittance information online on the ePayment site and/or download a HIPAA 835 ERA transaction file for import and processing as detailed information into the provider's practice management system and/or financial system, to support the provider's accounts receivable processing. Providers who use EMDEON's practice management hosted service or submit their claims to us via EMDEON, will also be able to take advantage of the "integration" efficiencies ePayment supports.

PayFormance. PayFormance offers our providers a comprehensive payment management solution which is "clearinghouse agnostic". PayFormance supports online EFT enrollment and activation, including bank depository accounts and remittance preferences, and provides online capability for viewing detailed remittance information, as well as the ability to download HIPAA 835 electronic remittance files directly to the provider's practice management system and/or financial system (as above).

Electronic Funds Transfer. To initiate EFT directly with LHC, all a provider will have to do is complete an LHC EFT Agreement. Upon acceptance, LHC will deposit payment for claims directly into the provider's bank account.

Electronic Remittance (ERA). Providers can view ERAs through our Provider Portal and can request a printed version of their electronic remittance advice.

Figure R.13-B: EFT and ERA Options



Enlisting, Training, and Supporting Providers

LHC realizes that technology only partially addresses the effort to encourage EDI submission of claims and will therefore supplement our technology options with active and aggressive provider education, one-on-one assistance, and other training methods to motivate a wide audience. Below we list some of the methods that have helped us to achieve high rates of EDI claim submission and that we will utilize in Louisiana to encourage our providers to move to EDI.

- Centene offers an **EDI Help Desk** to communicate directly with providers or clearinghouses that may experience issues or have questions about electronic submissions. EDI Help Desk technicians *reach out* and work directly with providers who currently submit electronic claims or have high rejection rates and help resolve any issues that cause claim rejections. The EDI Help Desk also offers *training or technical expertise* to encourage EDI submissions from those providers not yet submitting claims electronically. Our EDI help desk will be accessible from the LHC provider services *options on our Interactive Voice Response* system. EDI Help Desk staff respond to all voice messages and emails within 24 hours, and they are available to participate in *conference calls* with providers, software vendors and clearinghouses as needed.
- Our LHC Provider Claims Educator and Claims Liaison will be well trained in our electronic submission offerings and will work with the provider community directly to facilitate enrollment; walk them through the Portal submission options, in training sessions or through web-ex type sessions; and generally be available to support providers with any issues or barriers they have regarding EDI and EFT.
- We will organize outbound campaigns using our ***Provider Relationship Management (PRM)***. We will leverage this tool when appropriate to communicate with providers, such as to recruit providers, to exchange EDI with us and to make them aware of our EFT capabilities. We can also conduct outbound phone campaigns and complete provider phone surveys using ProviderReach. *Please reference R.11 for more information on our PRM system.*
- Through our Provider Portal, LHC providers will have the ability to view and refer to LHC Claims Adjudication logic in detail, using the **Clear Claim Connection** tool. Designed by McKesson Information Solutions, Inc., Clear Claim Connection "mirrors" how Centene's claims software evaluates medical code combinations during the adjudication of a claim. This tool allows the provider to access LHC claim auditing rules and clinical rationale, which results in cleaner claim submissions and less chance of misunderstanding between provider and LHC.
- We will send **EOP stuffers** containing the benefits of filing electronically and EFT payment.
- **Quarterly Provider Newsletters** sent to specialist and PCP office locations geared toward billing and coding staff within a practice or facility and emphasizing EDI and EFT.
- When appropriate, we will deliver training to providers through *web seminars or webinars*. Our Cenpatico Arizona affiliate has used this method and has received *universally* positive feedback on this form of training. We have found that provider participants, especially those in the rural areas, appreciate the interactivity webinars offer.
- We will routinely evaluate the need to host *workshops* to assist provider staff in understanding the benefits of EDI and EFT, to discuss new policies and procedures regarding claims submission.

Administrative Efficiency Report. LHC will develop a provider scorecard that will compare a provider's pattern of paper versus electronic claims and reimbursements against all contracted providers. The report will be available to internal staff who work directly with providers (via PRM system) and directly to our providers, via our LHC Provider Portal. This report will be a valuable tool for staff as they work one-on-one with providers regarding EDI claims submissions. The data in this report will demonstrate the connection between a provider's claims submission practice and the impact on their business in terms of claims accuracy and reimbursement turnaround. By pulling the data together and presenting it in this format, LHC staff will be equipped with powerful and easy-to-understand information

that will resonate with providers as we work together to improve EDI participation and reduce administrative costs. After we have oriented the provider to the report and its use, LHC will make this information available to providers via secure Provider Portal for their on-going reference. For more information on our PRM see R.11 and for more information on our Provider Portal applications, please see R.10 and R.15.

Sample *Administrative Efficiency Report*

Healthplan:

Provider:		Billing Practitioner(s):			
TIN:	570769093	NPI:	1023069580	Name:	JAMES J MORRISON
Name:	DOCTORS CARE	NPI:	1033175096	Name:	HANCE H OLIVER
Address:	300 Julia Street	NPI:	1083662241	Name:	SALVATORE CARMINE
	New Orleans, LA 70130	NPI:	1083677157	Name:	IVET E HUDSON

12 Month Claim Summary:

Overall

	Paper:	9.8%			EDI:	87.6%			Web	2.6%		
Type	Reject %	Accepted	Paid %	Denied %	Reject %	Accepted	Paid %	Denied %	Reject %	Accepted	Paid %	Denied %
New	**6%**	**29**	**88%**	**12%**	**3%**	**830**	**92%**	**8%**	**0%**	**10**	**100%**	**0%**
Professional	6%	29	88%	12%	3%	830	92%	8%	0%	10	100%	0%
Institutional	0%	0	0%	0%	0%	0	0%	0%	0%	0	0%	0%
Adjustments	**6%**	**20**	**95%**	**5%**	**3%**	**210**	**89%**	**11%**	**0%**	**22**	**100%**	**0%**
Professional	6%	20	95%	5%	3%	210	89%	11%	0%	22	100%	0%
Institutional	0%	0	0%	0%	0%	0	0%	0%	0%	0	0%	0%

Top Reject Reasons:	Top Denial Reasons:
1) Invalid/unreadable 837 File Format	1) DENY: AUTHORIZATION NOT ON FILE
2) Invalid Payer ID	2) BILL PRIMARY INSURER 1ST. RESUBMIT WITH EOB.
3) Unreadable Paper Deliveried	3) COVERAGE NOT IN EFFECT WHEN SERVICE PROVIDED

Your Submissions:

Total Paid $ 479,472.00 Average Daily Volume $ $ 2,397.36

	Submissions		Date Of Service to Date Received Average				Date Of Service to Date Paid Average				Your Average Receivable	
	You	Top Quartile	You		Top Quartile		You		Top Quartile		Days	$
EDI	**87.64%**	**98.48%**	**20**	**days**	**18**	**days**	**13**	**days**	**9**	**days**	**35.0**	**$ 2,101.10**
Paper	9.76%	1.52%	32	days	25	days	15	days	11	days	3.9	$ 233.89
Web	**2.60%**	**0.00%**	**2**	**days**	**1**	**days**	**10**	**days**	**8**	**days**	**1.0**	**$ 62.37**
Total	**100.00%**	**100.00%**	**21**	**days**	**18**	**days**	**13.1**	**days**	**9.2**	**days**	**40.0**	**$ 2,397.36**

Opportunity:

Potential Reduction of Receivable with move to Top Quartile: 5.1 days $ 73,360.44

Payment and Remit:

Payment Method: Paper Check Additional Receivable Reduction Potential for moving to EFT: $ 7,192.08

* assumes 3 day delay for mailing and deposit of check

Remittance Advice: Paper EOP Estimated paper savings for moving to Electronic Remit: 800.00 Sheets

2 trees

Question R.14

Years of Support of Current Information System Software Versions

R.14 Indicate how many years your IT organization or software vendor has supported the current or proposed information system software version you are currently operating. If your software is vendor supported, include vendor name(s), address, contact person and version(s) being used.

Continuously Enhanced Software Built On Longstanding Medicaid and CHIP Experience

Centene Corporation (Centene) will provide local and enterprise level Management Information System (MIS) hardware, software systems, and communications networking for Louisiana Healthcare Connections (LHC). Throughout Centene's 27 years of supporting Medicaid and/or CHIP managed health programs, we have *carefully* but *continuously enhanced* the individual components and integration of our software architecture, building on our core system foundation, including our claims processing system, AMISYS Advance, which we have operated and upgraded over the past 15 years, and our Enterprise Data Warehouse (EDW) at the heart of our data integration and informatics strategy.

Ensuring Reliable Operations While Continuously Introducing Meaningful Innovation

Capitalizing On Software Trends. Table R.14-A below offers a summary view of Table R.14-B. There continues to be an accelerating proliferation of software applications and version updates in the information technology market that are feasible for productive use and offer reliable and new administrative, clinical, and systems functionality. Table R.14-A reflects this fact and the observation that today almost half of the software versions in our portfolio are 3 years old or less. Our vendors are increasingly able to produce enhanced software versions in accelerating timeframes. More than 70% of our software today has been enhanced within the past 3 years. We view this software "vitality" factor as ***completely supportive*** of our basic approach to software management, which is to use "best of breed" software to offer the most reliable, yet innovative and valuable business and systems functionality to our clients, providers, members, and users.

Table R.14-A: Age Mix of Software Versions and Use at Centene

	Percentage Breakdown by Age of Software Components in Centene Portfolio	
	Column A: Most Recent Version Supported by Vendor	**Column B: Software Product In Production Use at Centene**
Less than 3 years	**72%**	**41%**
3 years or more	**28%**	**59%**

In order for us to manage this type of frequent software "refresh," we have developed two core competencies:

- Implementation and support of industry standard integration interfaces
- Disciplined, auditable, yet rapid change management protocols and tools.

A Software Architecture Designed For Interoperability

Our Service Oriented Architecture (SOA) approach to software deployment uses industry standard, message-oriented interfaces, such as Java Messaging Services (JMS), Open Database Connect (ODBC), Service Oriented Access Protocol (SOAP) web services and other open interoperability tools, and affords us maximum flexibility in incorporating best of breed solutions quickly and responsibly into our overall MIS in strategic timeframes yet with limited project risk. Please refer to Section R.4 for more information.

Change Management Discipline Allows Greater Ability To Assimilate New Software

We balance the demand for software reliability, data integrity and availability with the need to *carefully* infuse relevant new software versions and innovations. We implement changes and deploy new and updated software through well-documented Software Development Life Cycle (SDLC) and MIS operation techniques, and in partnership with our clients, providers, and users. Our use of the AGILE method for SDLC allows us to formulate, develop, test, and introduce new software versions quickly, yet within the confines of auditable change management, allowing for total project risk mitigation. Our clients, partners, and users are able to see and experience new functionality *incrementally* so that processes can be enhanced smoothly and documented with clearly identifiable revisions, and training courses can be updated with new functionality "curricula," incorporated seamlessly and naturally.

In addition, every year we review and compare all hardware and software components in our integrated MIS portfolio with the latest product versions from our vendors and overlay the projected needs of our business for the following year. The output of this effort is our Strategic Technology Refresh Plan (Systems Refresh Plan), which serves as our annual roadmap for planned introduction of new software versions for both Centene proprietary and vendor supported software components. We will supply DHH with a copy of our Systems Refresh Plan each year.

Perhaps the most critical component of our approach to significant software updates and new software integration is our *regular communication with our state partners, which will include DHH,* about any material updates related to our MIS operations.

Please see Table R.14-B below for Centene's integrated enterprise software portfolio that we propose to employ for Louisiana's CCN Program. We have organized our major systems according to the business processes they support.

Table R.14-B

Application	Application Description	Current Version	Support by Vendor	# Of Yrs. Version Supported	# Of Yrs. used by Centene	Vendor	Vendor Address	Contact Info
Medical Management								
TruCare	Clinical Case Management	4.3	Yes	< 1	< 1	CaseNet	23 Crosby Drive Bedford, MA 01730	Jon Abad 888-701-0886
InterQual	Medical Necessity Criteria software	4.4	Yes	1	9	McKesson Health Solutions	275 Grove Street, Ste 1-110 Newton, MA 02466	Jude Okolie 617-273-2894
Centelligence™ Platform								
Enterprise Data Warehouse (EDW)	DBMS Platform for the Enterprise Data Warehouse	13.00.00.22	Yes	2	2	Teradata	10000 Innovation Dr. Dayton, OH 45342	Andy Gilbert 513-319-7122
Executive Dashboard	Reporting dashboard	5.15.0	Centene	2	2	Custom	N/A	N/A
XCelsius Enterprise	Dashboard and Visualizations	2008 SP1	Yes	3	3	SAP	3999 W. Chester Pike Newtown Square, PA 16097	Mike McQuaid 919-386-5476
Business Objects Crystal Enterprise XI	Compliance reporting and Business Intelligence tools	XI 3.1	Yes	3	3	SAP	3999 W. Chester Pike Newtown Square, PA 16097	Mike McQuaid 919-386-5476
Impact Intelligence	Utilization, patient outcomes analytics software	1.3	Yes	1	< 1	Ingenix	12125 Technology Dr. Eden Prairie, MN 55344	Jennifer Felt 952-833-7100
Impact Pro	Predictive modeling and care management analytics software	5	Yes	1	2	Ingenix	12125 Technology Dr. Eden Prairie, MN 55344	Jennifer Felt 952-833-7100
Quality Spectrum Insight (QSI)	Performance measurement and Quality Improvement (QI) reporting - HEDIS	13	Yes	1	2	Med Assurant, Inc.	1559 Janmar Road Snellville, GA 30078	Bill Carden 770-982-8022 ext. 6162
Negotiator	Contract modeling software to aid in analysis of new or modified provider contract	1	Centene	N/A	N/A	Custom	N/A	N/A
Power Center	Extract, Transform and Load Automation Tools	8.6.0	Yes	2	6	Informatica	100 Cardinal Way Redwood City, CA 94063	Wayne Dye 310-643-4522

LOUISIANA HEALTHCARE CONNECTIONS

Application	Application Description	Current Version	Support by Vendor	# Of Yrs. Version Supported	# Of Yrs. used by Centene	Vendor	Vendor Address	Contact Info
Power Exchange	Updates EDW in near real time with changes from core applications	8.6.1	Yes	2	6	Informatica	100 Cardinal Way Redwood City, CA 94063	Wayne Dye 310-643-4522
Web Services								
Provider/Member Portal	Secure web based portals for secure transactions with members and providers	7	Centene	1	6	Custom	N/A	N/A
Clear Claim Connection	LHC claim auditing rules accessed through the provider portal	5.0	Yes	2	7	McKesson Health Solutions	275 Grove Street, Ste 1-110 Newton, MA 02466	Jude Okolie 617-273-2894
Claims Processing								
Amisys Advance	Eligibility, enrollment, claims processing, COB	4.0	Yes	2	15	DST Health Solutions	2400 Thea Drive Harrisburg, PA 17110	Kathleen McCarthy 717-703-7188
AWD	Document and workflow management	10	Yes	< 1	< 1	DST Health Solutions	2400 Thea Drive Harrisburg, PA 17110	Kathleen McCarthy 717-703-7188
ClaimsXten	Medical review and code auditing	CXT.2.0	Yes	4	4	McKesson Health Solutions	275 Grove Street Newton, MA 02466	Jude Okolie 617-273-2894
MACESS.exp (Includes IMAX and Storage)	Document imaging, OCR, and document management	IMAX - 4.40	Yes	5	9	SunGard Workflow Solutions	104 Inverness Center Place Birmingham, AL 35242	Terry Clanton 205-408-3480
EXP Form Works/RRI	Image Storage	Form Works 4.0	Yes	5	9	SunGard Workflow Solutions	104 Inverness Center Place Birmingham, AL 35242	Terry Clanton 205-408-3480
Encounters								
Xpress Encounter pro	Encounter Processing	3.1	Yes	1	1	Medical Data Express	908 W Chandler Blvd, Bldg A Chandler, AZ 85225	David Abraham 480-839-0420
Member and Provider Relationship Management								
Customer Relationship	Integrated member/provider inquiry, tracking,	2011	Yes	<1	< 1	Microsoft Corporation	One Microsoft Way Redmond, WA 98052	425-882-8080

Application	Application Description	Current Version	Support by Vendor	# Of Yrs. Version Supported	# Of Yrs. used by Centene	Vendor	Vendor Address	Contact Info
Management (CRM)	management							
Portico	Provider credentialing, demographics, financial information	6.1	Yes	3	3	Portico Systems	518 East Township Line Rd, Ste 100 Blue Bell, PA 19422	Connie O'Brien 215-358-3800
Emptoris	Contract management and reporting	7.5.9.1	Yes	< 1	2	Emptoris Inc.	200 Wheeler Road Burlington, MA 01803	Bryan Drumm 952-473-2600
Enterprise Content Mgmt. (ECM)	N/A	N/A	Centene	N/A	N/A	N/A	N/A	N/A
After Hours NurseWise Support								
N Centaurus Telehealth Triage	Nurse triage and call center workflow for NurseWise	2010	Yes	3	<1	LVM	4262 E. Florian Ave. Mesa, AZ 85206	Adan Garcia 480-633-8200, ext. 264
Telecom Services								
Avaya Communication Manager (CM)	World class call routing and applications; call centers managed through automatic call distribution (ACD) and advanced vectoring	5.2.1	Yes	1	7	Avaya Inc.	211 Mt. Airy Road Basking Ridge, NJ 07920	866-Go-Avaya
Avaya Call Mgmt. System (CMS) Supervisor	Tracks and reports information processed through the ACD	14	Yes	5	7	Avaya Inc.	211 Mt. Airy Road Basking Ridge, NJ 07920	866-Go-Avaya
Avaya Voice Portal	Speech-Enabled self-service IVR	5.1	Yes	1	1	Avaya Inc.	211 Mt. Airy Road Basking Ridge, NJ 07920	866-Go-Avaya
Middleware Services								
Business Connect	Data translation software; supports HIPAA, other ANSI, proprietary formats	3.6.0	Yes	2	7	TIBCO Software	3303 Hillview Avenue Palo Alto, CA 94304	Kevin Niblock 650-846-1000
iProcess Suite	Rules engine	4.1.1	Yes	2	3	TIBCO Software	3303 Hillview Avenue Palo Alto, CA 94304	Kevin Niblock 650-846-1000
Edifecs X-Engine	HIPAA compliance checking: translator/	6.2.1	Yes	1	6	EDIFECS	2600 116th Ave NE, Ste 200 Bellevue, WA 98004	Sue Powers 517-887-0717

Application	Application Description	Current Version	Support by Vendor	# Of Yrs. Version Supported	# Of Yrs. used by Centene	Vendor	Vendor Address	Contact Info
	validator component of EDIFECS							
EDIFECS Ramp Manager	Automate EDI trading partner administration	6.4	Yes	1	< 1	EDIFECS	2600 116th Ave NE, Ste 200 Bellevue, WA 98004	Sue Powers 517-887-0717
Diplomat Transaction Manager	Enterprise file transfer; supports FTP, SFTP, or local network delivery	3.5.3	Yes	<1	4	Coviant Software	60 Thoreau Street Concord, MA 01742	Jim Cutler 781-534-5163
Change Management								
Service-Now	Enterprise service desk software: incident, problem, change management	Fall 2010	Yes	< 1	< 1	Service-Now	120 S. Sierra Ave. Slana Beach, CA 92075	Steven Tito 630-786-1592
Compliance								
Compliance 360	Enterprise governance, risk management, compliance and audit management solution	2011.1.3.21	Yes	11	5	Compliance 360, Inc.	3780 Mansell Road, Ste 200 Alpharetta, GA 30022	Chris Faklaris 678-527-2453

Question R.15

Supporting Meaningful Use of Current and Future Federal IT Mandates

REDACTED

R.15 Describe your plans and ability to support network providers' "meaningful use" of Electronic Health Records (EHR) and current and future IT Federal mandates. Describe your plans to utilizing ICD-10 and 5010.

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Question R.16

Protecting Confidentiality of Records

R.16 Describe the procedures that will be used to protect the confidentiality of records in DHH databases, including records in databases that may be transmitted electronically via e-mail or the Internet.

Organizational Processes and System Controls Engineered for Safeguarding Confidentiality

Centene uses a comprehensive array of information security and confidentiality best practices combined with rigorous safeguards, policies, strong authentication, monitoring tools, and automated business processes to ensure systematic, ongoing, and auditable adherence to HIPAA regulations, mandates, rules, and standards per HIPAA Security (45 CFR 164), HIPAA Privacy (45 CFR 160 and 164), HIPAA Transaction & Code Set (TCS) (45 CFR 164), and applicable privacy and security regulations originating from the American Recovery and Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health Act (HITECH). We *are* and *have been* compliant with HIPAA on or before the respective effective dates of each HIPAA rule, including the HIPAA Security Rule. In short, our plan to continue meeting and exceeding HIPAA mandates centers on our existing, comprehensive, and constantly updated controls, policies, and processes described below.

Our ability to create, access, transmit, and store Protected Health Information (PHI) in accordance with DHH and HIPAA Security (including Confidentiality) and Privacy mandates stems from our design, maintenance, and use of administrative, technical, and physical security *safeguards* and *controls* under the guidance of Centene's Compliance Officer, Chief Information Security Officer, and General Counsel. These mechanisms ensure that:

- Only appropriately authorized personnel are granted access to LHC and Centene systems based on specific job roles
- All remote access to LHC systems and data requires multifactor authentication and is limited in accordance with HIPAA Minimum Necessary access requirements
- Physical access to sensitive computer facilities is restricted
- Systems are deployed and processes defined to safeguard data and monitor security events.

We adhere not only to HIPAA but also to Sarbanes Oxley (SOX) security requirements. We have built a comprehensive information security approach founded in the belief that the best way to ensure compliance is through the strict implementation of information security best practices. In our case, those best practices are most appropriately defined by the National Institute of Standards and Technology SP-800 series of documents, as well as the security practice models defined by the International Information Systems Security Certification Consortium (ISC2). At the core of our information security and compliance strategy is the internationally recognized triad of security: Availability, Integrity and, of course, **Confidentiality** which we implement through a series of layers.

- **Availability**. Centene has carefully designed our MIS for maximum availability. Our network infrastructure provides multiple paths through which our applications and users can securely reach data from all user connections. Our systems, server, and storage architectures were chosen for their high availability and security, and our core business applications run on virtualized server clusters providing the highest level of system uptime. Our Business Continuity and Disaster Recovery Plans anticipate risks in availability to Centene and our health plans and are tested annually. Please see section R.3 on Availability, Business Continuity and Disaster Recovery for more details.
- **Integrity.** Our MIS contain several types of controls to maintain information integrity, depending on the data processing, transmission, receipt, or storage application. Our controls are tested both via ongoing processes, such as edit enforcement routines for data load processes, via our own internal spot audits and several external audits, including our annual SAS/70 Type II and Sarbanes-Oxley Section 404 Management Controls audits. These controls are designed to verify that the data entered into our systems is correct and has not been inappropriately altered. Every change is tracked by user and time/date stamped for auditing purposes. All of our core business applications do not allow the alteration of finalized records. LHC will work with DHH to develop a methodology to spot audit

these controls and will provide the results of these audits to DHH. Please see section R.2 on Integrity, Validity and Completeness of Information for more details.

- **Confidentiality.** Centene has fully implemented Role-Based Access Control (RBAC) so data can only be accessed, created, or changed by those who have the authority to do so. In addition, we maintain confidentiality of electronic data and systems through multiple layers of controls. These layers include mechanisms we designed to keep unauthorized people from accessing systems, such as complex passwords, secure file systems, encryption, two-factor authentication for remote access, and strict policies and procedures regarding the handling and use of Protected Health Information (PHI) and other confidential data. In addition, our Network Operations Center (NOC) monitors network access attempts to protect Centene systems and databases from unauthorized access. The Centene Corporate Ethics and Compliance department monitors PHI sent outside of the organization monthly to ensure proper safeguards. These controls, policies and procedures are described in detail below. Please also see our response to section R.7 on Addressing Requirements In Section 16 of the RFP.

Confidentiality of DHH Records

Centene and LHC are trustees of valuable and confidential information that belongs to our members and state clients, and we *rigorously* employ the most thorough administrative, technical, and physical security safeguards and processes.

Administrative Safeguards (45 CFR 164.308). Our Administrative Safeguards engage our internal users, contractors and clients through documented policies and systematically enforced procedures.

Access Management. We use Oracle's Virtual Private Database (VPD), Microsoft Active Directory Application Mode (ADAM) and IBM Tivoli Directory Server (TDS) to restrict access to Protected Health Information (PHI), based on a user's job function.

Role Based Access Control. LHC and Centene have implemented Role Based Access Control (RBAC) for all core business applications. RBAC eliminates the problems inherent with assigning access rights on an individual basis. RBAC addresses security risks by defining employee access rights based on the employee's job functions or responsibilities, including whether that employee has access rights to update information or view only. To implement RBAC, department managers define the functions and minimum access rights (roles) employees need to accomplish their jobs. Centene then maps each job function or position to a set of responsibilities associated with that job function, and to a collection of work roles and security RBAC profiles. Centene's IT Security Department conducts Role Based Access Control (RBAC) tests to ensure application access has been appropriately provisioned, as described below. Our IT security staff may, depending upon an employee's job responsibilities, expand, limit, or eliminate that employee's access to PHI or other confidential information at any time. In addition, a Centene information security officer or an LHC Manager must approve an employee's access to information if that access request is not part of a standard security profile commensurate with the normal responsibilities of the employee's position. Depending on the type of access being requested, the Centene security officer or manager must obtain the approval and sign-off from the appropriate functional vice president.

Segregation of Duties. Centene enforces strict control over ***global application and systems access*** via a series of interconnected technical and administrative controls. Centene has implemented RBAC for all core business applications such that the individuals responsible for provisioning application access, for example, to AMISYS Advance (our enterprise core claims processing system), are not themselves members of roles that have rights to perform transactions within those applications. Furthermore, our monitoring regimen mitigates the risk of security personnel modifying their own roles, or provisioning new roles for themselves, by logging all changes to access, issuing privileged access reports for periodic review by application owners, and by notifying oversight personnel when there are any changes to highly privileged administrative roles. Administratively, we enforce separation of duties such that the individuals that provision front-end access to the network and core applications do not have rights to provision access

to crucial back-end components such as Business Objects and the Enterprise Data Warehouse; the reverse is also true. Likewise, they do not have rights to provision physical access to the areas where systems are housed. In addition, we document and enforce access control policy that explicitly defines role limitations and access review requirements for applications in our environment. For example, our access control policy for AMISYS Advance requires that the system be audited monthly to ensure that no single role, or no combination of roles granted to a single user, has rights to setup a member, setup a provider, and process a claim.

Password Controls. Centene's IT security staff strictly control password length, complexity, and lifetime to ensure that passwords cannot be easily compromised. Centene users are systematically forced to change passwords every 42 days and they are unable to reuse the last 10 passwords they created. Inactive PC workstations are automatically locked. After three failed login attempts users are locked out and must contact the Centene Service Desk to have the account unlocked.

Access Changes. Centene's Human Resources (HR) staff manage all individual security change requests through a documented security authorization and implementation process. For employment separation situations, HR staff notify the Centene Service Desk at least two days prior to a planned employment separation, or *immediately* by phone if the employment separation is not planned.

Auditing Systems Access and Usage. In addition to controlling access, Centene monitors and audits logins as a *second layer* of security. As part of our auditing process, IT system administrators routinely check log files to ensure unauthorized login attempts have not occurred. Our IT Security professionals ensure that any access identified as inappropriate or conflicting with defined and approved segregation of duties rules is immediately addressed. IT system administrators maintain an incident reporting file providing the date, time, and comments regarding any unauthorized attempts. We use BindView software to automate, monitor, and record the regular certification by Centene managers of appropriate subordinate access to our systems. Our IT Security staff also use Spector software to audit the appropriate use of applications, systems, company email, and use of the Internet from Centene PCs.

Database/Application Security: *Anti-virus and Anti-spam.* Centene is vigilant about protecting our systems from malicious software. We have implemented an enterprise edition of the McAfee e-Policy Orchestrator (ePO) product, including McAfee Virus Scan 8.7 antivirus program and Host Intrusion Protection System (HIPS) 7.0, across our organization. Additionally, we utilize Websense (formerly SurfControl) web security and spam blocking software to prevent virus, spam, denial of service, and phishing attacks. Centene updates virus definitions every *30 minutes* to ensure the most up-to-date protection is provided throughout our MIS, and Centene IT staff provide specific guidance and expectations to employees related to security incident response through our Incident Response Plan.

Security Awareness and Training. Centene trains all employees (including local plan employees) on policies and procedures regarding HIPAA as well as Sarbanes Oxley (SOX) regulations and rules regarding PHI security. All employees complete training shortly after their date of hire, upon job function changes, and when policies or procedures change. In addition, our Centene enterprise wide Compliance 360 compliance management system automatically issues emails to employees on annual "anniversary dates" of that employee's hiring, with a link to our Computer Based Training (CBT) modules on the Centene intranet (CNET). Compliance 360 records whether that employee completed their refresher course and whether the outcome was successful or not.

Risk Management and Mitigation. Centene conducts detailed technical risk assessments and testing of our MIS and key business processes on a regular basis. These activities include both regularly scheduled assessments as well as periodic, on-demand, assessments necessitated by significant changes in the threat environment, or specific requests by customers or business partners. These assessment activities are further augmented by our mature vulnerability management program which includes the regular scanning of our MIS against both new and existing exploits, and to verify continued regulatory compliance. In all cases, should material defects or weaknesses be discovered, they are prioritized based on risk, mitigated, and retested to validate resolution. Testing is performed using both internal resources and reputable third-

party providers. Risk mitigation and management is overseen by Centene's experienced Internal Audit Team with independent validation from our third-party audit partner, Ernst and Young. Included among Centene's in-depth risk management and mitigation program are established procedures to detect and mitigate any unnecessary or otherwise inappropriate disclosure of PHI. PHI related incidents are reported immediately to the Centene Privacy Officer within the Centene Compliance Department, as well as to our HIPAA Security Officer. Centene requires our subcontractors and business associates to sign a Non-Disclosure Agreement and/or Business Associate Agreement, requiring adherence to all HIPAA mandates, including notification of security incidents.

Centene's IT Department documents changes to the IT environment quarterly and attests to the impact of any such changes, certifying the ongoing effectiveness and adequacy of controls to mitigate risk.

Business Continuity Program (BCP). Centene's IT Department provides a comprehensive array of Business Continuity Planning (BCP) tools and services to LHC including, but not limited to: disaster recovery, crisis management, plan creation, plan testing, pandemic response, business impact assessment, and work-place violence preparedness. Each location has documented plans, updated yearly, that detail recovery procedures for every critical business process. Our BCP is designed to:

- Protect the health and safety of all LHC and Centene employees
- Ensure continuity of services to members and providers
- Minimize any adverse financial effects of a disaster
- Ensure that normal business operations are restored in a timely manner
- Provide a proper work environment for displaced LHC employees
- Provide a regularly tested business continuity system

Centene's comprehensive **Disaster Recovery Plan** (DRP) is supported by a secondary data center provided by SunGard Availability Services. In the event of a complete loss of the primary datacenter, critical services would return to operation in the SunGard facility within 36-48 hours from the time of the declared disaster. In addition, Centene is on schedule to complete implementation of a fully redundant, two-datacenter architecture in the 4th quarter of 2011. This second enterprise datacenter will enable enhanced recovery service levels and provide for near real-time recovery of critical business systems and services.

Today, we use SunGard Mobile Recovery and Metro Center Solutions to provide flexibility in meeting the workspace and business process recovery needs of each location. SunGard's NotiFind™ Emergency Notification Service is used to communicate instructions to employees no matter what happens to prevailing communications systems at the time of disaster. Continuous improvement is achieved by employing annual plan reviews and exercises to maintain a continuous evergreen recovery status. For more information on our Emergency Response and Continuity of Operations planning, reference our response to sections M.1, M.2, and R.3.

Physical Safeguards (45 CFR 164.310). The Centene corporate datacenter building in St. Louis, Missouri, houses our core data and voice communications systems, securely connected via our internal Wide Area Network (WAN) to our information technology assets located throughout our local LHC offices. Centene physically protects all core business application and telecommunications systems in our corporate datacenter with limited and strictly controlled access. We secure our Centene datacenter and all Centene corporate and health plan facilities via proximity card access on all external doors, elevators, and the internal entry doors on each floor. Additional physical security controls include digital security cameras, multiple security guards who are on duty at all times, and panic switches installed at each reception desk. Our corporate datacenter has yet another layer of proximity card control, restricting access to authorized personnel only. This card access system records all access attempts/card swipes whether successful or not. We also monitor, record, and audit access and movement using multiple cameras throughout our corporate datacenter, including all entry points into the datacenter room. Centene

datacenter staff follow documented policies and procedures related to requesting, obtaining, monitoring, and auditing access to the datacenter.

Our receptionists require that all visitors sign in and out at the front desk; are issued a temporary badge; and are accompanied by an employee when visiting a Centene facility, including our corporate datacenter. The Centene Director of Systems Services must authorize Centene corporate datacenter access requests and grants authorization on a need basis *only*. Our IT staff require that vendors performing services within the Centene data center sign in and be escorted into the facility by authorized personnel only. In addition, we require that every visitor to the network room in our corporate datacenter sign into a log book indicating the time, employee escort, and purpose of their presence in the network room. We also require that visitors sign out when leaving network rooms. We will provide escorted access to our datacenter to authorized DHH or Federal representatives, when requested, or provide access by other means, such as secure WebEx, to inspect the quality, appropriateness, and timeliness of services performed by LHC. Each month, the Manager of Centene Datacenter Operations reviews the sign in log to ensure that only appropriate physical access requests are approved.

Device and Media Controls. We track the receipt, storage, deployment, movement, and disposal of all PC workstations, laptops, and Personal Electronic Devices (PED's) through our ServiceNow System. Our IT Asset Coordinators at Centene work with our IT Liaison in the local plan office, including LHC, to ensure that any movement or re-assignment of MIS hardware is approved by management and is documented and tracked in ServiceNow. When we reassign, dispose, or donate any PC, we erase all data on the machine using secure data erasure software from Blancco, Ltd. Our data erasure tools and methods fully comply with HIPAA Security and US Department of Defense Clearing and Sanitizing Standard 5220.22-M. For any device or media that management approves for disposal, and after all data is removed, our vendor, EPC, Inc. (EPC) picks up the device(s), physically destroys them, and confirms to us that the device(s) have been destroyed. EPC is AAA certified by the National Association for Information Destruction, Inc. (NAID).

All Centene and local plan users who are issued PC's, laptops, and/or PED's must follow stringent policies on the use of this equipment. Desktop machines are physically locked to fixed structures in our offices. Users must attach their laptops to docking stations with cable locks or lock those laptops in filing cabinets in their offices when not in use. Our Internal Audit Department regularly checks that this policy is followed. All Centene laptops are equipped with McAfee's Safeboot full-disk encryption software to ensure continued data protection even if the device is lost or stolen. Users are required to store all Protected Health Information (PHI) and other confidential information on the Local Area Network (LAN) servers instead of using the hard drives of their desktop PCs.

Our laptop machines are equipped with Absolute tracking software so that lost or stolen devices can be physically located when connected to a network. In order to prevent disclosure of PHI, if a device is lost or stolen, access to that device (laptop, Blackberry, etc.) is automatically revoked and data is deleted remotely by authorized IT staff.

Technical Safeguards (45 CFR 164.312). ***Network Security.*** To secure the internal data network, Centene employs an array of industry best-practice technologies such as firewalls, Access Control Lists (ACL), Terminal Access Controller Access-Control System Plus (TACACS+), Demilitarized Zones (DMZ), Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN), Data Loss Prevention (DLP), Secure communication protocols (SSH, SFTP, etc.), and SSL encryption for secured web communications. Our IT supervisors monitor network security using advanced event management and correlation tools on a routine basis, and our network engineers routinely implement restrictive VPN tunnels for secure connectivity with our external Trading Partners, such as our state clients. All such implementations are audited and approved prior to production by our Information Security staff to ensure adherence to policy and observance of least privilege.

Secure Remote Access. As a part of our commitment to the comprehensive implementation of information security best-practices, Louisiana Healthcare Connections (LHC) and Centene Corporation

will use award winning SecureAuth® Identity Enforcement Platform (IEP) software to provide secure ***multifactor authentication*** for LHC employees and business partners, including authorized DHH representatives, who require remote access to Centene information systems. IEP will be one of the core components on our defense-in-depth strategy ensuring that only authorized individuals are allowed remote access into our Cisco Virtual Private Network (VPN), Microsoft Outlook Web Access, and Citrix published applications. In addition, the extensible and flexible nature of the IEP software allows it to be quickly integrated to protect any other applications that might be deployed in the service of the Louisiana Coordinated Care Network Program.

Patch Management. Windows Server Update Services (WSUS), System Center Configuration Manager, and Eminentware are used to deploy and manage the latest Microsoft and third-party software updates to computers running the Windows operating system. In addition to these technologies, Centene utilizes NeXpose's Rapid7 tool for vulnerability assessment, policy compliance, and remediation management. The tool scans Web applications, databases, networks, operating systems, applications, and other software products to locate threats, assess their risk to the environment, and distribute remediation tasks. Centene has a dedicated Patch Engineer that coordinates with various administrators to ensure network vulnerabilities are identified and patched in a timely fashion thus reducing the risk of a vulnerability being exploited. Each of these tools is configured to provide management reports, which are reviewed regularly to ensure that patches and updates are current and that Centene's overall residual risk and security posture fall within acceptable limits.

Managing Security Breach Risk: Intrusion Prevention Systems. The primary function of an Intrusion Prevention System (IPS) is to monitor and prevent attempts to breach security and gain unauthorized access from inside or outside our network. Centene employs next-generation SourceFire 3D® IPS appliances together with SourceFire 3D® virtual IPS sensors to keep unauthorized users from infiltrating our network. By utilizing an array of sensors strategically placed throughout the network, we are able to simultaneously protect *multiple gigabits* of network traffic traversing all of the subnets on our LAN and WAN with the flexibility to operate in promiscuous or inline modes. In addition, our RSA enVision Security Information and Event Management (SIEM) system monitors and alerts security staff, in real time, of internal and external system threats and configuration changes that could be exploited.

Encryption Technologies. We support multiple encryption technologies to protect data and communications both at rest and in transit in and out of Centene and LHC.

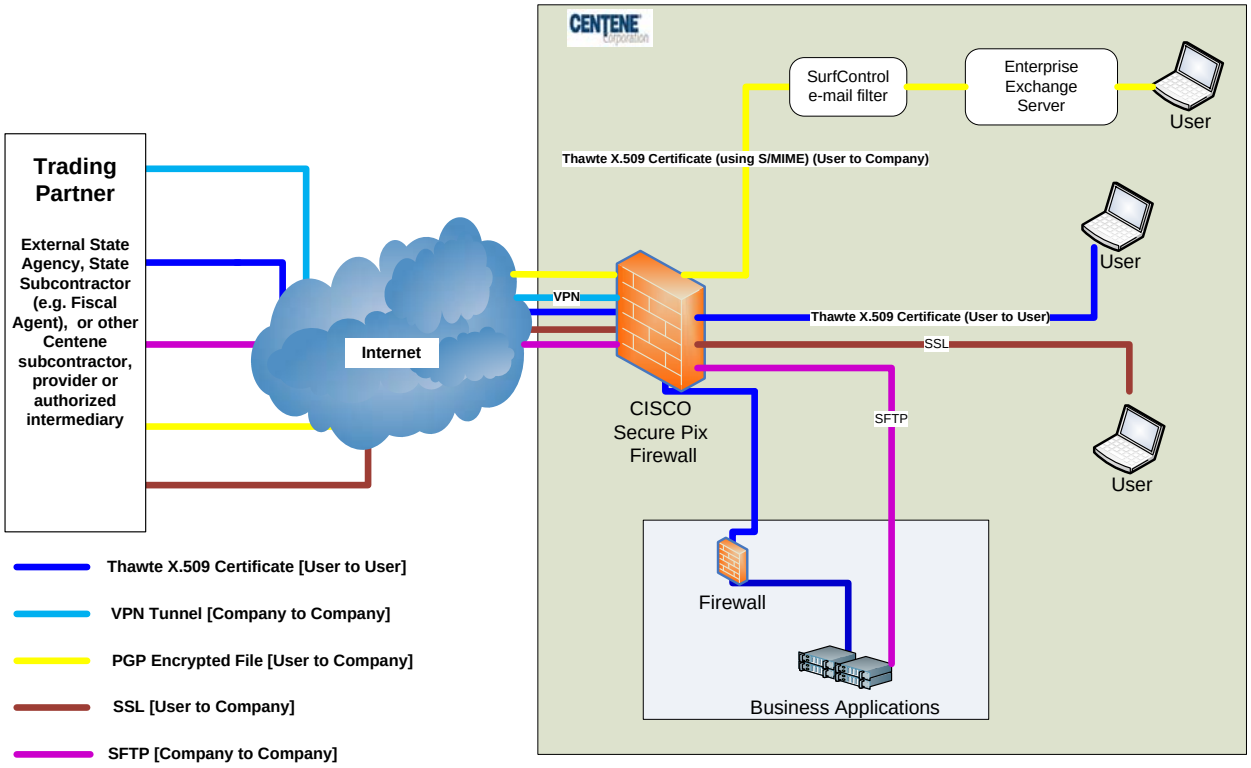
E-Mail. Centene supports several email encryption methods for secure communications, all of which are compliant with HIPAA and Sarbanes Oxley (SOX) rules and regulations. Centene's primary method for securing email communication between systems, sites, and/or domains is Transport Layer Security (TLS). TLS is an industry standard protocol for securing electronic communication and is designed to prevent eavesdropping, tampering, and message forgery. TLS also supports endpoint authentication and communications privacy using digital certificates.

Centene's messaging systems also support industry standard email and web encryption protocols such as S/MIME and SSL. Centene has deployed Cisco's IronPort email security and encryption appliances at the network perimeter. These IronPort systems provide a seamless and integrated means to send encrypted emails to external parties. Centene also supports PGP Workgroup and third-party digital certificates for email encryption and HIPAA compliance where required. In addition, we use Vericept data loss prevention tools to monitor and control PHI data usage. Vericept technology provides multi-level content analysis for defining PHI in both structured and unstructured formats, and Vericept monitors data in motion as well as at rest. Vericept's capabilities enable us to identify and prevent potential HIPAA violations by detecting and preventing unauthorized transmission or access of such things as Social Security Numbers, medical account numbers, dates of birth, and dates of admission or discharge.

Laptops. We equip all of our laptops with McAfee's Safeboot full-disk encryption software.

Internet Encryption. See *Figure* R.16.1 below, which *partially* illustrates the encryption technologies used for communications between users inside the Centene family, including LHC, and outside the Centene enterprise. For security purposes, we cannot disclose ALL Internet security control details. Note that we can (and do) connect to some of our State clients via Virtual Private Network (VPN) or by dedicated leased line to a state client's private network. No matter the physical connection, we can (and do) support TCP/IP data communication protocols with our state clients.

Figure R.16.1 Encryption Technologies



Thawte x.509 Certificate [User to User]

We support the use of X.509 Certificates for secure encrypted user-to-user email messages, particularly for emails involving clinical review by medical professionals. For example, user A shares their public key with user B. Once user B has accepted user A's public key, user B can then send encrypted messages to user A. For user A to send encrypted messages to user B, user B must obtain an X.509 certificate and share their public key with user A.

VPN Tunnel [Company to Company]

We can (and do) establish company-to-company VPN Tunnels over the Internet typically from firewall to firewall in strict observance of best practices governing least privilege. While using a company-to-company VPN, all information transferred over the VPN is encrypted. A company-to-company VPN is typically two-way. Security is controlled internally by each company to set levels of access to information inside the company. Centene is currently using IPSec technology for VPN Tunneling. Centene also utilizes Secure HTTP and Secure FTP with SSL encryption for secure transmission of information.

PGP Encrypted File FTP [User to Company]

We support the use of PGP Encryption to encapsulate a file into a secure envelope or wrapper. The PGP encrypted file is transferred using any standard transfer method such as FTP or email.

SSL [User to Company]

We support Secure Socket Layer (SSL) encryption for a variety of uses, including interactive access by our users, to secure websites at our trading partners and to support web-based secure e-mails when our Trading Partners require this capability.

SFTP [Company to Company]

We support secure FTP with a number of our trading partners. Secure FTP allows us to exchange formatted data in encrypted manner securely over the open internet.

Audit Functions

Centene conducts in-depth technical risk assessments and penetration tests of our MIS and key business processes on a regular basis. These activities include a mix of regularly scheduled assessments as well as periodic, on-demand, assessments necessitated by significant changes in the threat environment or specific requests by customers or business partners. These assessment activities are further augmented by our mature vulnerability management program mentioned above, which includes the regular scanning of our MIS against both new and existing exploits and to verify continued regulatory compliance. In all cases, should material defects or weaknesses be discovered, they are prioritized based on risk, mitigated, and retested to validate resolution. Testing is performed using both internal resources and reputable third-party providers. Risk mitigation and management is overseen by Centene's experienced Internal Audit Team with independent validation from our third-party audit partner, Ernst and Young. As required, we will provide a security risk assessment and security plan to DHH and federal agencies within 15 days of contract award.

Continually Auditing Operations and Monitoring Regulations to Ensure Compliance. ***Internal Audit.*** Centene's Internal Audit Department (Internal Audit) conducts risk assessments and monitors internal controls over financial reporting, assessments of operational effectiveness of Centene health plans, which will include LHC, provider contracting, claims processing, and information technology (IT), including controls needed for HIPAA compliance. Internal Audit regularly evaluates our operations and systems to ensure risks have been identified, impact assessments are conducted, and adequate mitigation controls and monitoring are deployed to continually minimize risk. Our Business Continuity Team works closely with our Internal Audit Department to identify, report, and mitigate risk where possible. We will work with DHH to develop methodology for spot audits and will provide results of all such audits to DHH.

Compliance 360. Our Compliance Department uses Compliance 360 software to stay current with HIPAA, state contract obligations, and other relevant regulations. Compliance 360 enables our comprehensive approach to regulatory compliance and risk management through a single enterprise-wide platform. We use Compliance 360 for ongoing policy management, as a centralized regulation repository, for incident management and related reporting, contract management, surveys, remediation projects, audit management, self-assessment, and enterprise risk management. Compliance 360 incorporates updated databases of important federal, state, HIPAA, and accreditation agency regulations and standards, links regulatory and state contract requirements and regulations with internal compliance activities, policies, procedures, and projects. The bottom line: Compliance 360 helps us to remain a trusted and transparent partner of our state clients and in compliance with data confidentiality mandates.

Penetration Testing. Our IT Security Department conducts penetration testing on our systems, networks, and websites on an on-going basis. During these penetration tests, we attempt to penetrate our websites and email systems via such mechanisms as Denial of Service attacks, phishing, spoofing, and other tactics, as well as occasional social engineering tests, such as false emails allegedly from Centene or LHC employees inviting the receiver to click a malicious link. We also periodically retain an outside firm to perform penetration tests. In 2010, Centene contracted third-party firms to conduct both external and internal penetration tests using Via Forensics and Ernst & Young respectively. All identified issues were

prioritized by risk, remediated, and retested to ensure compliance. Additional third-party firms will be contracted to provide penetration testing services in 2011 to independently verify the security of Centene applications, systems, and networks.

External Audits. Centene undergoes regular external audits and completed the following reviews in 2010, which included examination of HIPAA, SOX Section 404 Management Controls, and other related controls and safeguards:

Information Technology Risk Assessment. As recently as 2010, Centene engaged Ernst & Young to review Centene's IT risk profile/risk universe, to ensure that we had identified appropriate risks, their potential severity, likelihood of occurring, and impact. Ernst & Young, LLP reviewed our organization's IT risk profile and provided a few additional risks for inclusion in the risk universe. Our IT risk profile is used in Centene's Enterprise Risk Management (ERM) process, which includes an ongoing review and assessment of Centene's risk environment with senior management.

Sarbanes Oxley Management Report on Internal Controls over Financial Reporting. Centene's management is responsible for establishing and maintaining adequate internal controls over financial reporting and supporting MIS controls, including those related to security and confidentiality. Each year, management conducts evaluations of the effectiveness of internal controls over financial reporting according to Sarbanes-Oxley Section 404 (SOX) regulations. Our Internal Audit Department and Ernst & Young, LLP conducted our most recent audit of these controls for the period ending December 31, 2010, and concluded that Centene's internal controls over financial reporting were effective. Centene's **assessment** of the effectiveness of internal controls for the period ending December 31, 2010, was audited by KPMG, LLP, another public accounting firm. *No significant deficiencies or material weaknesses were identified.*

SAS 70 Type II. KPMG, LLP performs this annual audit for Centene to test the design of controls over Claims Processing and Datacenter Operations and the operating effectiveness of such controls, including those related to MIS availability, security, and data integrity. In its most recent SAS 70 Type II audit, performed in 2010, *Centene received an unqualified opinion from KPMG, LLP* (that is: KPMG did not discover any material adverse findings).