Primaris
Healthcare Business Solutions

2019 External Quality Review
Information System Capabilities Assessment

UnitedHealthcare®

Measurement Period: Calendar Year 2018
Validation Period: Apr-Jun 2019
Publish Date: Oct 18, 2019

MoHealthNet

Table of Contents

1.0 Introduction and Methodology

Primaris Holdings Inc. (Primaris), assessed UnitedHealthcare's Information System, Resource Management, Data Processing, and Reporting Procedures. The purpose is to analyze interoperability and reveal the extent to which UnitedHealthcare's information systems can support the production of valid and meaningful performance measures in conjunction with their capacity to manage care of their members.

Primaris bases their methodologies directly on the CMS protocol: External Quality Review (EQR) APPENDIX V-Information System Capabilities Assessment (ISCA). (Attachment A-Tools for Assessing Managed Care Organization (MCO) Information Systems; and Attachment B-Information System Review Worksheet and Interview Guide.)

Data collection, review, and analysis is conducted for each review area via the ISCA data collection tools, interview responses, security walk-throughs, and claim/encounter data lifecycle demonstrations.

The ISCA review process consists of four phases:

Phase 1: The MCO's information system standard information is collected. Primaris sends the ISCA data collection worksheet to the MCO with a deadline to be completed and returned electronically to Primaris prior to the scheduled on-site review activities. (The deadline for submission of documents was Apr 6, 2019).

Phase 2: Review of completed worksheets and supporting documentation. All submitted documentation is thoroughly reviewed, flagging answers that seem incomplete or indicated an inadequate process for follow-up. The follow-up questions and review takes place during an on-site visit (held on Jun 26, 2019).

Phase 3: Onsite review and walk-throughs. Primaris utilizes time on-site to review any propriety material, live system and security walk-throughs, and interview other members of staff related to their information systems management.

Phase 4: Analysis of data collected during pre and on-site activities. Primaris compares and scores the findings directly against industry standards. Specific focus on 45 CFR Part 160 & 164, section 2.26 of the MHD contact, and Medicaid Management Information System (MMIS).

2.0 ISCA Scoring Key and Standards

2.1 Scoring Key

Each subsection of the ISCA is awarded one of the three scoring options: Not Met (fail), Partially Met (pass), or Met (pass). In the event a Partially Met or Not Met score is awarded, recommendations will be provided to the MCO by Primaris. Additionally, the MCO has the

option to request technical assistance from Primaris via MHD to assist with any recommended improvement activities. Scores for the ISCA align with other EQRO protocols (e.g., compliance with regulations) and are based on the standards for Met, Partially Met, or Not Met criteria.

Scoring Table 2-1 presents the scoring key used and descriptions.

Table 2-1: Scoring Key

Scoring Key	Description
Met (pass)	All necessary requirements were proven to be satisfied with supporting documentations, system demonstrations, and staff interviews.
Partially Met (pass)	Some supporting evidence and/or positive results that meet majority *(at least half plus one)* of the requirements and industry standards. *Example: MCO has well-structured documentation around information system processes, and mostly positive results. MCO is fully aware of their opportunity for improvement around their paper claims process and tracking. They have a plan in place working on improvement, provided evidence such as meeting minutes, calendar invites, etc. All supporting active improvement activities.*
Not Met (fail)	No supporting evidence or positive results to meet requirements and industry standards. *Example: MCO has no documented processes in place to support their ability to track a claim, which was originally paper, back to its original source. In fact, in the on-site interviews 3 employees mentioned their lack of ability to backtrack as a pain point in their day-to-day activities.*

2.2 Scoring Standards

Scoring Standards Table 2-2 presents the detailed Federal regulations, Missouri HealthNet Division (MHD) State contract requirements, and industry standards against which UnitedHealthcare was evaluated.

Table 2-2: Scoring Standards

Citation	Source	Description
45 CFR Part 160	Health & Human Services (HHS)	Code of Federal Regulations for General Administrative Requirements' compliance and

		Enforcement for Maintaining Security and Privacy.
45 CFR Part 164 Subpart C	Health & Human Services (HHS)	Code of Federal Regulations Subpart C Security Standards for the Protection of Electronic Protected Health Information.
45 CFR Part 164 Subpart E	Health & Human Services (HHS)	Code of Federal Regulations Subpart E Privacy of Individually Identifiable Health Information.
42 CFR Part 438 Subpart E	Health & Human Services (HHS), Centers for Medicare and Medicaid Services (CMS)	Code of Federal Regulations Subpart E Quality Measure and Improvement; External Quality Review.
42 CFR Part 438 Subpart H	Health & Human Services (HHS), Centers for Medicare and Medicaid Services (CMS)	Code of Federal Regulations Subpart H Additional Program Integrity Safeguards.
Section 2.26 MHD Contract	Missouri Health Department (MHD)	Claims Processing and Management Information Systems section.
NIST	National Institute of Standards and Technology	"The Information Systems Group develops and validates novel computational methods, data/knowledge mining tools, and semantic services using systems-based approaches, to advance measurement science and standards in areas such as complex biological systems, translational medicine, materials discovery, and voting, thus improving the transparency and efficacy of decision support systems" **
ANSI ASC X 12	American National Standards Institute, the Accredited Standards Committee	"The American National Standards Institute (ANSI) chartered the Accredited Standards Committee (ASC) X12 to develop uniform standards for inter-industry electronic exchange of business transactions, namely electronic data interchange." ***

References: *** - *https://www.nist.gov/*

*** - https://www.edibasics.com/edi-resources/document-standards/ansi/

3.0 Summary of Results: UnitedHealthcare

UnitedHealthcare passed the ISCA in all seven (7) areas, receiving a fully 'Met' score result for the overall ISCA score (Table 3-1). UnitedHealthcare meets all contractual obligations for information system management and have well documented processes and procedures in place to allow their information systems to be adequately monitored and maintained. During the on-site review the team focused on data integrations, data integrity, and data security.

Table 3-1: Section Score Results

ISCA Section	Description	Score Result
Overall ISCA Score	Total Score for UnitedHealthcare.	**Met** (pass)
A. Information Systems	Assess MCO's management of its information system.	**Met** (pass)
B. IT Infrastructure	Assess MCO's network and physical infrastructure.	**Met** (pass)
C. Information Security	Assess the security level of MCO's information systems.	**Met** (pass)
D. Encounter Data Management	Assess MCO's ability to capture and report accurate and meaningful encounter data.	**Met** (pass)
E. Eligibility Data Management	Assess MCO's ability to capture and report accurate and meaningful Medicaid eligibility data.	**Met** (pass)
F. Provider Data Management	Access MCO's ability to maintain accurate provider information.	**Met** (pass)
G. Performance Measures and Reporting.	Assess the MCO's performance measure and reporting process.	**Met** (pass)

A. Information Systems

This section of the ISCA evaluates the MCO's management, policies, and procedures surrounding its information systems. Detailed review is conducted to thoroughly assess the information systems capacity for collecting, filtering, transforming, storing, analyzing, and reporting Medicaid data.

Key scoring points of well-managed systems include:

- Data structure that support complex queries that can be changed by well-educated staff.
- Secure access via authentication with role-based permission levels.
- Written policies and procedures that support industry standards and best practices for IT management.
- Reasonable system response times, bidirectional.
- Complete and consistent testing procedures, with documentation and access logs.
- Clear version control procedures with documents access instructions.
- Ability to make changes to systems with minimal disruption to users.
- Adequate training and user documentation for new employees and on-going training programs.
- Open communication with end users of information systems changes, issues reporting, and updates.

UnitedHealthcare is fully compliant with the key scoring points of a well-managed Information System structure.

UnitedHealthcare utilizes Oracle 12c, a relational database, for their database management system. They have a robust range of well-integrated languages and programs such as PL-SQL, VB.NET, C#, ASP, ASP.NET, Crystal Reporting, VBA and Cobol. Currently there are 70 programmers trained and capable of modifying these programs with an average of 3-4 years' experience. The following quoted portion, pulled from UnitedHealthcare's final ISCA tool, was verified while onsite and/or in the submit documentation to the AWS S3 file share. UnitedHealthcare has high quality and accuracy in their mappings and documentation. All the information was up-to-date and well maintained.

"All users of UnitedHealth Group (UnitedHealthcare is the operating division of UnitedHealth Group) information technology systems are uniquely identified and authenticated before access to information assets and/or information technology system is granted. Provisioning access follows defined and documented processes for granting new or modified levels of information technology system access. Access to information technology system may only be granted when based upon documented business justification and approved by Management. The use of standard UnitedHealth Group provisioning processes and technologies, such as SECURE, provides a more granular level of Role Based Access Control (RBAC) and includes built in logging and monitoring capabilities. Access controls enforce separation of duties, where applicable, to minimize the risk of system misuse and reduce opportunities for unauthorized modification or misuse of data or services. Programmers are continually trained with CBT, WebEx, and in-person training. Policy requires they complete 40 hours per year."

Internal trainings are tracked through a learning management system, LearnSource. UnitedHealth Group's Optum Technology departments have tailored and aligned their teams' training to match current needs and future strategy. Additionally, based on job responsibilities, many employees obtain technical and/or security-related professional certifications, such as CISA, CISM, CISSP, CNA/CNE, etc. Based on their job function, employees are also required to take various mandatory training courses each year.
UnitedHealthcare does not verify code by analyzing defect rates but rather by performing code reviews. The reviews have proven to be a more proactive way of measuring performance. The defect rates are calculated after the code has been delivered, so it lessens the chance to catch errors before being pushed. UnitedHealthcare looks at the code in a code review process before it is ready for deployment. This also provides the opportunity for analyzing programmer performance during the code reviews, which is a highly effective method in identifying knowledge gaps and training needs amongst their programming staff.
UnitedHealth Group may utilize outsourced vendors to provide maintenance/development and testing support for their claim production applications that augment UnitedHealth Group Optum Technology's primary teams. These relationships are managed and approved by UnitedHealth Group management teams. In addition, all vendors are contractually managed to specific terms supported by a Security and/or HIPAA/GLB Exhibit (when appropriate) attached to the master services agreements executed with each vendor.
UnitedHealthcare's Facets Development Group adheres to a weekly integrated release schedule to manage version control of code sets. Each release is governed by shared deliverable schedules, gates, and deadlines that all team disciplines follow. Code management is governed by a release code management team utilizing GitHub and Endevor tools. UnitedHealthcare's Information Technology staff is able to readily access the well documented process they follow during code reviews, modifications, and approvals. Code is checked out, modified, and unit tested by programmers under the strict control of the of these code management tools and the Facets release management staff. The Application Development Repository/United Development Process release process is followed to promote this code change into production.

Strengths

- Policies and procedures readily available to all necessary staff.
- Availability of thorough and accurate information system mapping documents.
- A clear training and continued education program for their staff.
- Testing processes and development methodologies meet and exceed industry standards.

- Change requests processed in-house with strict guidelines and managed by current staff members.

Weaknesses

No weaknesses discovered or calculated for the Information System section of the ISCA.

Table A-1: Information System Scoring Results

Sub-section	Issues	Score	Citation/Standard
IS Management Policies	None	●	45 CFR 160, 45 CFR 164, Section 2.26.8 MHD Contract
Reconciliation and Balancing	None	●	Section 2.26.5 MHD Contract
Training	None	●	45 CFR 164.132
Testing Procedures	None	●	NIST
System Changes and Version Control	None	●	NIST, Section 2.26.2 MHD Contract
EDI	None	●	45 CFR 164.312, ANSI, Section 2.26.5 MHD Contract
TOTAL SCORE	None	●	**Met – Pass**

B. IT Infrastructure

This section of the ISCA evaluates the MCO's network infrastructure and ability to maintain its equipment and telecommunicates capacity to support end users' needs.

Key points of well-managed and maintained IT Infrastructure include:

- Adequate maintenance staff of maintenance contracts to ensure timely replacement of computer equipment and/or software.
- Adequate staff or contracts that ensure timely responses to emergent and critical system failures.
- Redundancy within the data center hardware that minimizes the length of system outages, loss of data, and disruption of end user service.
- Business continuity and disaster recovery (BCDR) plans that are maintained and tested regularly.

● **UnitedHealthcare is fully compliant with the key scoring points of a well-managed and maintained IT Infrastructure.**

In both the mainframe and distributed environments, UnitedHealthcare's backup and recovery policy requires maintenance of two copies of operational data at its secured technology centers. A Virtual Tape Library System is maintained at the primary data center that emulates physical tape and stores data on hard drives for the purpose of daily operational recovery in case of data corruption or accidental deletion. The data is then electronically transmitted to another disk-based array or Physical Tape Library located in UnitedHealth Group's geographically dispersed data center(s). UnitedHealth Group maintains sole custody of the data at all times by transmitting over our secured channels. UnitedHealthcare has a thorough training program for employees and contractors that is relative to their performing roles, responsibilities, and actions in a disaster scenario. The program consists of seven sections that everyone must complete, consisting of: 1. Enterprise Resiliency & Response Program web site. 2. Enterprise Disaster Recovery Services web site. 3. Event Management Program Training. 4. Business Continuity training. 5. Disaster Recovery Training. 6. Periodic awareness promotions. 7. Annual testing process for BCDR training. All testing results are reported to senior leadership at UnitedHealthcare and must include plans to address identified gaps where Recovery Time Objective goals are not met.

In addition, it is UnitedHealthcare's policy and standard that BCDR Plans must be developed, tested, and maintained to limit losses caused by disruptions to critical business operations and to enable efficient and effective recovery. Per UnitedHealthcare's backup strategy, systems and databases are backed up daily and they maintain their own tape management storage facility within the managed data centers. The data input into the application is validated for accuracy. Validation checks are performed on the application to detect data corruption and the results are reported. The application's authenticated state is maintained for every data transaction for the duration of that session.

Strengths

- Primary and back-up disaster recovery physical site servers.
- Comprehensive and proactive BCDR plan.
- Clearly documented infrastructure allowing for comprehensive maintenance.

Weaknesses

No weaknesses discovered or calculated for the Information System section of the ISCA.

Table B-1: IT Infrastructure Score Results

Sub-section	Issues	Score	Citation/Standard
Redundancy	None		45 CFR 164.308, NIST, Section 2.27 MHD Contract

Data Center/Server Room	None	●	45 CFR 164.308
Backup	None	●	45 CFR 164.308, NIST
Network Availability	None	●	Section 2.26.8 MHD Contract
TOTAL SCORE		●	**Met - Pass**

C. Information Security

This section of the ISCA evaluates the MCO's information system and the safeguards in place to proactively avoid malicious access to facilities and/or data systems, intrusions, and breaches of protected health information (PHI) and personally identifiable information (PII).

Key points of well-managed Information Security protocols include:

- Physical security safeguards are in place and at all facilities.
- Policies and procedures that comply with national healthcare security standards, include specific references and guidelines for mobile devices, and are routinely reviewed and updated.
- Procedures to remove/modify access to systems when an employee, contractor, or user leaves. Including a plan in place for expedited access removal as needed.
- Dedicated security administration staff, adequate to support the organization and its internal and external users.
- Policies and procedures that comply with HIPAA Security and Privacy standards, including the reporting and remediate of security and privacy breaches.

● **UnitedHealthcare is fully compliant with the key scoring points of well-managed information security protocols.**

UnitedHealthcare has a well-established and robust security infrastructure in place. The provisions in place for physical security regarding the computer systems and manual files are well outlined and defined in 5 core documents shared with Primaris during pre-onsite and onsite activities. The subject focus among these documents were physical security, access control, access management, identification and authorization, and personnel security. All protocols followed are based on industry practices, all applicable regulatory obligations, and customer considerations.

The following provisions are in place for UnitedHealthcare's computer system and manual files. This list is a highlighted summary of their infrastructure regarding physical security of their premises, documents, computer facilities, terminal access and levels of security.

Physical security controls are in place to protect all non-public areas from unauthorized access. Unauthorized individuals are prohibited from being in non-public areas. Physical access must be limited to the minimal physical access necessary to perform the employee's, contractor's, or external party's job function. All individuals entering a UnitedHealthcare's non-public area must identify themselves with their UnitedHealth Group-provided access badge. If an individual does not have a UnitedHealth Group-provided access badge, the individual must be authorized by management prior to being granted access. Periodic reviews are conducted to ensure building access is appropriate. Access logs and card reader activity are monitored for suspicious activities of unauthorized access attempts. All visitor access to UnitedHealth Group non-public areas must be logged. Visitor access logs must include the following details, at a minimum: 1. Visitor's name, 2. Visitor's signature, 3. Acknowledgement of visitor identity verification by review of a government-issued photo or other appropriate identification (ID), 4. Visitor's company name, 5. Time of entry, 6. Time of exit; and, 7. Name of UnitedHealth Group-badged employee or badged contractor who will serve as escort. Visitor logs are secured when not in use, and are retained for an appropriate length of time, per the Corporate Record Retention Schedule and the Enterprise Records Information Management (ERIM) Policy.

All employees and contractors who use UnitedHealthcare's Information Assets and Information Technology (IT) system are required to be made aware of and fully comply with UnitedHealthcare's Information Security Policies. As a part of new employee and contractor training, employees and contractors are required to acknowledge their understanding and acceptance of UnitedHealthcare's Information Security Policies and Privacy Policies. On an annual basis, employees and contractors will acknowledge a continued obligation to abide by the UnitedHealthcare Information Security Policies. Managers are responsible for communicating and promoting their direct reports' compliance with UnitedHealthcare's Information Security Policies and Control Standards. Managers are also responsible for taking appropriate actions to reinforce compliance and respond to suspected violations. The current version of this security standard is maintained in UnitedHealthcare's eGRC Policy Center, accessible by all individuals with a need to access.

When a UnitedHealthcare-owned workstation is assigned to an employee or contractor, they are required to log on to a UnitedHealthcare-owned or managed network at least once every 30 days to keep the workstation active and appropriately patched. For Optum Information Technology (IT) managed workstations: After 30 days without accessing the

network, the workstation will become inactive. Inactive workstations are not able to log into a UnitedHealthcare-owned or managed network. Rejoining the network will require validation of patching status by the supporting UnitedHealthcare IT organization, which may require a reimage of the workstation.

Any individual or system that access Protected or Confidential Information owned or managed by UnitedHealthcare are required to have their identity validated and access authorized by the appropriate manager or delegate prior to accessing requested resources. The acceptability, validation, and verification of identity evidence must meet the requirements of the type of resource access requested. Each individual or system that is granted access must be approved by the appropriate management, individual, or team. Designated privileged security groups must be the only group with local administrative privileges on a server. UnitedHealthcare's policy forbids any primary, secondary, or non-user IDs to be directly attached to the local admin, except for third-party applications that do not support Directory Services and/or Active Directory (AD) authentication. UnitedHealthcare utilizes multi-factor authentication (MFA) as an element of layered security controls to reduce risk associated with high-risk online activities.

Strengths

- Security policies are readily available, well documented, and well maintained.
- UnitedHealthcare provides HIPAA training and health care data best practices review.
- There are security procedures in place and documented for quick removal of a terminated employee.

Weaknesses

No weaknesses discovered or calculated for the Information Security section of the ISCA.

Table C-1: Information Security Score Results

Sub-section	Issues	Score	Citation/Standard
Physical Security	None		45 CFR 164.310, NIST, Section 2.26.4 MHD Contract
Security Policies	None		45 CFR 164.308, 164.312, NIST, Section 2.26.4 MHD Contract
Security Testing	None		NIST

Access Removal Policies	None	●	45 CFR 164.308, 164.312, Section 2.26.12 MHD Contact
Mobile Device Security and Policies	None	●	45 CFR 164.308, 164.312, NIST, Section 2.26.4 MHD Contract
TOTAL SCORE		●	**Met - Pass**

D. Encounter Data Management

This section of the ISCA evaluates the MCO's ability to capture and report accurate encounter data.

Key points of well-managed encounter data practices include:

- Documented procedures on encounter data submission, which include timeframes and validation check.
- Automated edit and validity checks of key fields.
- Production of error reports and procedures to correct those errors.
- Periodic audits to validate the encounter data.
- Reconciliation procedures that compare MCO's data to provider data.

● **UnitedHealthcare is fully compliant with the key scoring points of well-managed encounter data practices.**

UnitedHealthcare uses standard claims and/or encounter forms when receiving administrative data from their hospital, physician, home health, mental health, and dental sources. UnitedHealthcare can distinguish between the principal and the secondary diagnosis by placement on the claim form submitted which correlates to a specific field within the claim processing application. If a Medicaid claim is submitted from a provider and one or more required fields are missing, incomplete, or invalid, the claim is processed without payment and a remittance advice is sent to the provider requesting the missing information. To verify the accuracy of submitted information, edits have been established utilizing various tools, e.g., claim system, CES Facility editor, Webstrat, automation macro/robots to validate. The claim/claim line will flag with an error if an invalid CPT code or diagnosis code or code combination is entered. There are no circumstances where a processor can change claim information and there is no case where the content of a field is used differently from the intention of the description. In the case of a newborn claim, if the claim was billed under the mother's ID and the newborn ID was available, the ID would be

changed from mother's ID to the newborn ID. This change is completed in a designated and monitored process.

Claims that are received through the Clearinghouse or the Provider Portal (an intermediary) are not modified. UnitedHealthcare dental claims are processed by UnitedHealthcare Dental/Skygen, their dental vendor and are received by UnitedHealthcare as a dental encounter. The only changes made are the paid status and related payment processing information.

Claims for Medical and Behavioral services are processed for payment in UnitedHealthcare's CSP Facets claims system. Claims data is copied to an analytic platform SMART for use by multiple reporting and analytic processes including HEDIS measures. Claims data from all vendor encounters are also loaded to the SMART platform. ICUE is UnitedHealthcare's Utilization Management tool and contains service authorization data as well as lookup of CSP Facets data for member, claim and provider details. Community care is UnitedHealthcare's care management platform and contains claims information for purposes of care management. All claims are run through nightly batch processing.

The operational claims and member system (CSP Facets) currently houses online data since the start of the UnitedHealthcare's eligibility and member management in Missouri (prior to 5/1/17). UnitedHealthcare's SMART data warehouse analytical environment will house claim and member data for a minimum of 10 years. Encounters data is stored in the NEMIS platform for a minimum of 10 years. Historical data is accessed via a batch job. Historical data is uploaded back into the current Facets-CSP tables where it can be seen in the application. Batch jobs can be completed within 24 hours.

UnitedHealthcare estimates completeness using its proprietary reserving models that considers claims experience in aggregate and subsets of specific categories of care (e.g., inpatient, outpatient, physician) and are reviewed each month by Reserving Actuaries. Completeness is estimated using claims completion models that account for trend, seasonality, unit cost changes, special adjustments and claims payment speed. Claim completeness varies by month and by category. In general, claims are 90-95% complete after 3 months.

Medicaid claims are regularly audited for financial and procedural accuracy. Claims fall into the audit sampling group within one week after payment posts. Each week, 32 claims are randomly sampled from the platform universe via the Smart Audit Master (SAM) tool. Timeliness isn't included as part of the audit, but it is monitored daily by the Claim Team.

UnitedHealthcare utilizes the CSP Facets claims processing system and the Ingenix Claim Edit System (iCES and CES) to analyze professional and facility health care claims on a pre-payment basis. These systems are configured to automate industry standard coding practices, reimbursement policy (including CMS Medicaid NCCI guidelines and edits), and

Missouri State specific requirements. Professional claims editing is automated to systematically review the field validity of patient demographic and clinical data elements (age and/or gender to CPT and/or diagnosis) on each claim; and effective dated ICD-10, CPT and HCPCS code validation, based on the service dates and patient clinical data. Facility claims data are automated to systematically review code validity and reasonableness, against HIPAA-compliant healthcare code sets and industry standards (i.e. NUBC). These reasonableness tests include the Outpatient Code Edits (OCE) developed by the Centers for Medicare and Medicaid Services (CMS) for outpatient facility claims and NUBC. The systems handle both Outpatient code edits and Inpatient Diagnosis analysis for coding analysis and consistency.

CSP Facets will provide a prompt to the claims examiner via an error or warning message if there is a potential authorization match or if a service requires an authorization and no authorization is on file. If the claim requires medical review it will be pended internally and routed to Utilization Management for review. Once Utilization Management has completed their review the claim is routed back to the claim department for adjudication. A pended claims report is generated and reviewed daily by the claims management team and status is tracked for all pended claims. Claims submitted by capitated providers are held to the same claim guidelines and completeness requirements as non-capitated providers. Monthly reconciliation is done with both capitated providers and capitated vendors to validate the completion of data submitted.

United Healthcare's Missouri Managed Care Information System is built on their CSP Facets transaction processing system; which provides eligibility, enrollment, claims processing, benefits configuration, capitation, reporting capabilities and the source data for encounter data submissions. During UnitedHealthcare's weekly automated process, they collect encounter data in HIPAA transaction formats and code sets using strategic, internally-developed encounter data submission and reporting system, the National Encounter Management Information System (NEMIS). Their encounter data collection and submission process ensure that all data provided to MHD has first been tested for accuracy, completeness, logic and consistency. Vendor data is collected through claims and encounter files and is loaded both to the NEMIS platform for encounter processing to the state and the SMART Data Warehouse for analytic purposes including HEDIS reporting. All data transfers and downloads are automated.

A claim is scanned by the Regional Mail Operations (RMO) and assigned a Film Locator Number (FLN), the image is loaded to Intranet Document Retrieval System (IDRS). Claims are entered into NSF file format that is loaded in United Front End (UFE). UFE routes the claims to CSP Facets. If there is a delay in scanning, a claim can't be accessed/processed

until the image is available in IDRS. All scanning occurs within 24 hours of receipt at the mailroom. Mailroom maintains clean desk policy audit daily.
Medicaid eligibility uses the state 834 as the source of truth for Missouri Medicaid Eligibility. If there is a question on a specific member record it is verified through the state system to confirm eligibility. Claims for capitated providers are auto adjudicated by the claims platform and do not require manual intervention from the payment function teams. There is no message a claims processor would receive to indicate a claim is capitated and requires special processing. If a procedure code is missing, the claim is rejected, and a remittance advice is sent to the provider requesting the missing information.
Performance is monitored through timeliness, production, and claim payment accuracy standards. Current timeliness standard is meeting a 30-day turnaround time and current production standard is achieving a 14.2 claim per hour individual standard. Claim payment accuracy is 98.75%.

Strengths

- UnitedHealthcare has implemented adequate validation edits in its data processes.
- Encounter data is not altered by UnitedHealthcare but sent back to source for correction.
- Consistent communication regarding upcoming changes.

Weaknesses

No weaknesses discovered or calculated for the Encounter Data Management section of the ISCA.

Table D-1: Encounter Data Management Score Results

Sub-section	Issues	Score	Citation/Standard
Redundancy	None	●	45 CFR 164.308, NIST, Section 2.26.5 MHD Contract
Data Center/Server Room	None	●	45 CFR 164.308, Section 2.26.5 MHD Contract
Backup	None	●	45 CFR 164.308, NIST, Section 2.26.5 MHD Contract
Network Availability	None	●	Section 2.26.5 MHD Contract
TOTAL SCORE		●	**Met - Pass**

E. Eligibility Data Management

This section of the ISCA evaluates the MCO's ability to capture and report accurate Medicaid eligibility data.

Key points of well-managed and maintained eligibility data practices include:

- Uploading of monthly eligibility data from MHD with reconciliation processes in place.
- Uploading and applying eligibility data changes from MHD in between monthly file.
- Managing internal eligibility files to eliminate duplicate member records.
- Running reports to identify changes in eligibility that effect service data.

UnitedHealthcare is fully compliant with the key scoring points of well-managed and maintained eligibility data practices.

UnitedHealthcare has continued to update their Facets system as upgrades become available. The upgrade to Facets 5.2R2 completed on Sept 6, 2016. The upgrade to Facets 5.4R1 completed on Aug 19, 2017. The upgrade to Facets 5.4R4 completed on Feb 10, 2018. The upgrade to Facets 5.5R1 completed on Aug 18, 2018. In addition, all hardware and software are upgraded to the latest supported levels within UnitedHealth Group. The upgrades keep the Facets-CSP platform current with the TriZetto software. UnitedHealth Group have not implemented any new features at this time. UnitedHealthcare reports the upgrades had no effect on the quality and/or completeness of the Medicaid data collected. UnitedHealthcare uniquely identifies enrollees by using the capabilities within CSP Facets of auto-generating a unique identification number for newly enrolled members. In addition, CSP Facets has a unique group identification code. Under no circumstances can more than one member exist under the same member ID.

Medicaid disenrollment and re-enrollment information is entered in the CSP Facets eligibility module. Upon notification of a member's disenrollment, a termination date is entered. When the member's re-enrollment is received, the member is reinstated, and the effective date is entered in the eligibility module in CSP Facets. The member's disenrollment and re-enrollment dates are easily accessible for tracking and viewing in the CSP Facets system. The member will retain the same CSP Facets auto-generated ID. UnitedHealthcare's system configuration also allows for tracking of enrollees who switch from one product line to another. An enrollee's initial enrollment date with our MCO can be tracked. If a member enrolls in a new product line with our MCO a new enrollment date is assigned reflective of that product line. Medicaid and Medicare claim data can be easily tracked and linked within CSP Facets. Members simultaneously enrolled in both a Medicare product and a Medicaid product are also linked in CSP Facets by a Record Number and all

related encounter data can be identified for the purposes of performance measure reporting.

There is one circumstance in which a Medicaid member can exist under more than one identification number in UnitedHealthcare's system(s). If MHD sends a subscriber under different identification elements, the system may create a duplicate entry. A weekly report is run to identify members with more than one Subscriber ID record. If a member is found having more than one Subscriber ID record, the additional record is voided, and a note added with the correct CSP Subscriber ID. A member's CSP generated Subscriber ID can be changed if the member reports their ID card lost or stolen.

Newborns that are born to an existing Missouri member are assigned their own individual Subscriber ID number in CSP Facets based on the receipt of the 834 File. In some cases, newborns may be assigned a temporary Subscriber ID until information is received on the 834-file. Once information is received for the newborn on the 834 File the two ID's are merged, and the newborn is assigned a Subscriber ID. UnitedHealthcare's process involved a more manual and thorough process than typically seen. If there is a second ID, UnitedHealthcare verifies via their contact at MHD to properly connect the record ID's with the appropriate member (newborn and/or mother).

The Medicaid enrollment information is updated daily from the 834 files send from MHD. This consists of a daily add/update audit file that is manually reviewed and processed by enrollment. Regarding managing breaks in Medicaid enrollment, the 834-file received from MHD is considered the "source of truth". Enrollment and disenrollment dates are loaded to CSP Facets as received. If a member is disenrolled one day and re-enrolled the following day this is not considered a break in enrollment. The member is considered continuously enrolled. There are no internal restrictions for when Medicaid enrollees can enroll or disenroll, eligibility is determined by MHD. Membership information received on the 834 file is the source and is loaded to CSP Facets as such.

Medicaid member months are identified via a sweep of the member eligibility tables. Each eligibility segment is evaluated to determine the number of eligible days within a specific calendar month to determine either a partial or total member month for that segment. For example, if there are 30 days in a month and the member has less than 30 days total across all eligibility segments, they would not have a total member month. Medicaid member years are computed by taking the member months for a given measurement period and dividing by twelve.

Strengths

- Unique members' ID assignment and duplicate member safeguards.
- Monthly and/or daily eligibility files uploads, keeping information as updated as possible.

- Reporting in place to identify changes in eligibility status and reconciliation.

Weaknesses

No weaknesses discovered or calculated for the Eligibility Data Management section of the ISCA.

Table E-1: Eligibility Score Results

Sub-section	Issues	Score	Citation/Standard
Eligibility Updates and Verification Process	UnitedHealthcare reports the eligibility 834-file received is lacking current/correct demographic and contact information.	●	42 CFR 438.242, 438.608, Section 2.28.5 MHD Contract
Duplicate Management	None	●	42 CFR 438.242, 438.608
Eligibility Loss Management	None	●	42 CFR 438.242, 438.608
TOTAL SCORE		●	**Met - Pass**

F. Provider Data Management

This section of the ISCA evaluates the MCO's ability to maintain accurate and timely provider information.

Key points of well-managed provider data include:

- Establishing a communication process to update and maintain provider credentials, licenses, and skill sets.
- Supporting information system that integrate provider information with member and service data.
- Developing and maintaining policies and procedures that support timely exchange of provider information.
- Using provider data to edit encounter data to ensure that qualified providers are performing services they are qualified to perform.

● **UnitedHealthcare is fully compliant with the key scoring points of well-managed provider data practices.**

UnitedHealthcare updates their provider paper directories on a weekly basis. A weekly provider feed is sent to their vendor to update the most current provider data. This allows a member to get a current directory any time they request one via Customer Service area. The data is a direct reflection of what is in the system with no manual manipulation to the data. Members can call Customer Service and request a weekly updated directory via mail.

Rally is also available as a provider search tool online via UnitedHealthcare's website. Rally is updated daily except on Saturdays. Changes in directory information are driven by system updates to provider demographic information and newly loaded or terminated providers. Provider directories are refreshed with the most current provider data available at the time of the directory data inquiry. UnitedHealthcare's plan directory manager has change authority with approval from the health plan leadership.

UnitedHealthcare maintains provider profiles in their information system. The Network Database (NDB) is used as their validity source for their provider directories and data entered there flows through UnitedHealthcare's other systems in a standard data flow process. There are 41 data elements maintained and displayed for both paper and online directories and it includes standard demographics/contact information, languages spoken, accessibilities, etc.

Medicaid reimbursement rates and provider compensation rules are administered by dedicated teams in accordance with: a) the contractual requirements negotiated between UnitedHealthcare and the participating provider as permitted or structured according to a state (e.g. pay as state pays, % of Medicaid Fee for Service, etc.), or b) in accordance with non-participating pricing regulations as published by the state Medicaid agency. Updates to fee schedules, reimbursement rates and provider compensation rules are mechanically administered based on fee source publications from the state Medicaid agency or other negotiated contract terms. Fee schedules are loaded to have pricing applied automatically, unless there are specific edits in place due to PCA's, benefits, authorizations, etc. that will cause a claim to pend for manual review. Most provider types are configured for auto adjudication.

Strengths

UnitedHealthcare has an active/updated directory available to the public both in paper and online.

Weaknesses

No weaknesses discovered or calculated for the Provider Data Management section of the ISCA.

Table F-1: Provider Data Management Score Results

Sub-section	Issues	Score	Citation/Standard
Provider Directory Management	None		42 CFR 438.242, 438.608, Section 2.12.17 MHD Contract
Payment Reconciliation	None		42 CFR 438.242, 438.608
TOTAL SCORE			**Met - Pass**

G. Performance Measures and Reporting

This section of the ISCA evaluates the MCO's performance measure and reporting processes.

Key points of well-managed performance measures and reporting include:

- Use of encounter data, member data, and service data from an integrated database as the primary source for performance measurements.
- Policies and procedures that describe how the organization maintains data quality and integrity.
- Staff dedicated and trained in all tools to develop queries and tools for reporting.
- Support for continuing education of staff responsible for reporting metrics.
- Use of data for program and finance decision making.
- Use of analytics software and other industry standard reporting tools.

UnitedHealthcare is fully compliant with the key scoring points of well-managed performance measures and reporting.

Data sets for performance measurement are collected by querying the processing system online (CSP Facets) as well as by using relational database/data warehouse (SMART). SMART is the common analytical data warehouse for UnitedHealthcare

The CSP Facets production database can be directly accessed which contains claims, provider and member data. Data is extracted weekly and loaded to the SMART data warehouse. The SMART data warehouse also contains vendor data (RX, dental, lab and vision) loaded weekly and Care Management system data (Community Care and ICUE) loaded daily. If the report specifications require merging of these data sources the member can be linked across the multiple systems allowing consolidation of the sources. CSP and vendor data in SMART are stamped with a unique member identifier in addition to the CSP Subscriber ID, state Medicaid ID and/or SSN. Care Management data will contain CSP facets Subscriber ID, state Medicaid ID and/or SSN. The independent data sets can be merged using these identifiers common to the systems. Reporting can also pull directly from the production database if applicable. CSP Facets, Community Care, ICUE and vendor data files can all be utilized to create reports depending on the report requirements.

All source code is reviewed by an UnitedHealthcare senior analyst or manager for correctness; comparisons are made to prior period metrics and approval is required from the business owner before the report is placed in the production reporting schedule. Per UnitedHealthcare's maintenance cycle, data is reviewed and validated by the assigned analyst and the business owner after requirements have been verified and approved. If at any point during the development cycle the output is not reasonable or meeting the expected outcome, examples of data are isolated and run through the logic to determine the

underlying cause of the outcome. If necessary, requirements and SQL logic are modified until the accurate output is achieved. Reports submitted for production deployment are reviewed by a team review process.

All members must be identified as a Missouri member to be included in UnitedHealthcare's reporting. Unknown members are not included in any reporting. SQL logic will display a direct filter on the line of business specific to the performance measure of health plan thus ensuring only appropriate members are selected. SMART claim, member and vendor data are stamped with a unique member identifier. Care Management and CSP data also contains a system contrived member key. If Care Management data is merged with SMART member/claims/vendor data, the CSP facets Subscriber ID, State Medicaid ID or SSN from the Care Management data is linked to one of these values.

Monthly UnitedHealthcare runs and reviews their Data Integrity Executive Summary Report which includes several different metrics ensuring the accuracy and completeness of the data. These reports compare the current month's totals to the previous 12 months using Six Sigma standard threshold controls. If the current month's volume is three or more standard deviations from the mean, the metric will fail. For any of the failed metrics, the data integrity team will research, determine root cause and work with the appropriate teams to get the issue resolved.

During the report development process the analyst reviews the record counts against the logic to determine if volume changes are reasonable based on the filters applied in the logic. The analyst also compares the results to prior year results and existing metrics if applicable. This method is used to check the reasonableness of the integrated data. Reports are not created from a vendor software, UnitedHealthcare develops their reports in house. Reporting is sourced from UnitedHealthcare's SMART data warehouse, CSP Facets production data, or replicated copies of the transactional systems not from file extracts stored independently. The SMART data warehouse maintains a complete history of all data used for reporting. If reporting is sourced from CSP Facets historical data is maintained. If any historical or trend reporting is required, this can be accomplished via date manipulation of the report variables.

Strengths

- UnitedHealthcare employs many experienced staff members for developing queries and reports.
- Robust processes and documentation is available regarding performance measure reports.

Weaknesses

No weaknesses discovered or calculated for the performance measures and reporting section of the ISCA. However, a coding error (human error) was identified while validating

one the of the performance measures during an onsite visit (details are described in Performance Measures Validation report).

Table G-1: Performance Measures and Reporting Score Results

Sub-section	Issues	Score	Citation/Standard
Performance Measure Processes	None	●	42 CFR 438.242, Section 2.29.3 MHD Contract
Validation of Performance Metrics	None	●	Section 2.29.3 MHD Contract
Documentation of Metrics	None	●	Section 2.29.3 MHD Contract
TOTAL SCORE		●	**Met - Pass**

4.0 Recommendation

A complete assessment of UnitedHealthcare's Information System's documentation and related onsite activities revealed an opportunity for improvement concerning the data collection and integration structure with the 834 file routinely received from MHD. Demographic data is often incorrect or missing as it comes to UnitedHealthcare. MHD's file feed is a one-way feed and therefore values that are incorrect or missing cannot be updated in the MCO's repository. Any information attempted to be updated is overwritten by the next load of the 834 file.

Primaris strongly recommends that MHD and UnitedHealthcare work towards a collaborative solution for the ability to update and access more accurate and useful member demographic data. This will aid in keeping member information updated and create a complete data integration solution delivering trusted data from various sources.