C.6. Management Information System

a. Provide a detailed description, diagrams and flowcharts of the Management Information System (MIS) the Vendor will use to support all aspects of Kentucky's Medicaid managed care program including the following subsystems:
   i. Enrollee Subsystem
   ii. Third Party Liability (TPL)
   iii. Provider Subsystem
   iv. Reference Subsystem
   v. Claims Processing Subsystem (to include Encounter Data)
   vi. Financial Subsystem
   vii. Utilization/Quality Improvement Subsystem
   viii. Surveillance Utilization Review Subsystem (SURS)

As part of the response, include information about the following:

   i. Required interfaces, how the system will share and receive information with the Department, how the Vendor's system will use files provided by the Department, Subcontractors, providers, and other supporting entities.
   ii. Capability to store and use large amounts of data, to support data analyses, and to create standard and ad hoc reports.
   iii. Extent to which these systems are currently implemented and integrated with other systems, internal and external, and the Vendor's approach for assuring systems that are not fully implemented and integrated will be ready to begin operations on required timeframes.

Diagrams and flowcharts should show each component of the MIS and the interfacing support systems used to ensure compliance with Contract requirements.

b. Provide a description for and list of potential risks and mitigation strategies for implementing new information systems and changes to existing systems to support the Kentucky Medicaid managed care program.

c. Describe the Vendor's current and planned use and support of new and existing technology in health information exchange (HIE), electronic health records (EHR), and personal health records (PHR).

d. Describe the Vendor's approach to assessing integrity, accuracy, and completeness of data submitted by providers and Subcontractors.

e. Provide a description of the Vendor's data security approach and how the Vendor will comply with Health Insurance Portability and Accountability Act (HIPAA) standards including the protection of data in motion and at rest, staff training and security audits.

f. Describe any proposed system changes or enhancements that the Vendor is contemplating making during the anticipated Contract Term, including subcontracting all or part of the system. Describe how the Vendor will ensure operations are not disrupted.

Passport Highlights: Management Information System

How We're Different	Why It Matters	Proof
Leading-edge technology platform leverages Social Determinants of Health (SDoH) data and advanced analytics to predict adverse clinical events and social needs to direct resources to the most impactable members	• Addressing social risks is essential to creating an individualized approach to whole-person care • Leveraging community-based organizations impacts broader social issues across the Commonwealth	• Passport's platform can accurately identify members 6-12 months *before* they have an acute clinical event over 80% of the time • Among those members who were proactively identified for SDoH outreach, 100% self-reported an SDoH need and 90% reported multiple needs
Passport's has the best of both worlds - Kentucky staff who understand local issues and have built lasting stakeholders relationships augmented by leading edge technology and clinical research from Evolent	• Evolent brings large-scale and industry-leading technology and population health insights to support the Commonwealth's goals for the Medicaid Program • Fully integrated administrative and clinical platform initially developed by UPMC, one of the largest provider-owned Medicaid health plans in the nation	• 3.7 million lives managed on platform today • Passport was the only managed care organization (MCO) selected by the Department of Medicaid Services (DMS) to demonstrate readiness for Kentucky HEALTH. After jointly developing requirements with DMS, Passport implemented all necessary system changes in a phased approach to meet individual requirements
Passport is fully integrated and operational with DMS, providers and vendors in Kentucky today	• During the implementation of the 2021 contract, there will be no disruption to members, providers or other stakeholders, and continuity of currently functioning operations will be maintained	• Passport has over 250 data interfaces configured and operational that would not need to be reimplemented for the 2021 contract

Introduction

Over the last two decades, Passport has developed, refined and operated a robust Management Information System (MIS). The MIS and its subsystems are fully operational, already configured to meet the needs of DMS and currently functioning within the guidelines and specifications of the Commonwealth, including required interfaces. Our MIS meets or exceeds all Kentucky Medicaid Managed Care Program subsystem requirements, including enrollee/member, third-party liability (TPL), provider, reference, claims/encounter processing, financial, utilization data/quality improvement, surveillance utilization review, reporting and testing. The existing integration with the Commonwealth, providers and vendors will provide continuity with all stakeholders, as reimplementation is not required with Passport.

Our MIS is scalable to accommodate additional member populations, as well as new program requirements, as demonstrated recently with Kentucky HEALTH. Passport was proud to serve, on the behalf of DMS, as the Kentucky showcase MCO to Centers for Medicare & Medicaid Services (CMS). We worked collaboratively with both DMS and contracted vendors to demonstrate our readiness to execute new Medicaid program requirements, including 834 file consumption, corresponding plan mapping for the Kentucky HEALTH population and automated delivery and monitoring of data extracts. Our MIS stands ready to execute on current and future program requirements.

In 2016, we proudly transitioned to the Evolent Health (Evolent) Identifi℠ Platform, an MIS designed to support population health via the Identifi Population Health Management (PHM) system, followed in 2017 by the transition to support health plan administration via Identifi Health Plan Administration (HPA). At the core of Identifi is the enterprise data warehouse (EDW) and strong data integration and orchestration components that seamlessly combine administrative (payer), clinical, provider and self-submitted data from multiple, disparate sources powering a suite of fully interoperable modules designed for value-based care. This includes our industry-leading predictive modeling algorithms for member risk identification and the Identifi Engage mobile app, which is used to enhance member engagement in treatment. The response to 6a is organized as follows:

Passport MIS Description and Overview

Passport MIS Components
- Identifi HPA
- Identifi PHM

Passport MIS Subsystems
- Enrollee/Member Subsystem
- TPL Subsystem
- Provider Subsystem
- Reference Subsystem
- Claims Processing Subsystem

- Encounter Processing Subsystem
- Financial Subsystem
- Utilization/Quality Improvement Subsystem
- Surveillance Utilization Review Subsystem (SURS)
- Member/Provider Services and Telephone Management

Subcontractor Management Information Subsystems

- CVS/Caremark
- Beacon Health Options
- Avēsis

Passport MIS Reporting Capabilities

Passport MIS Testing Infrastructure

Passport MIS Hardware and Architecture

- Identifi HPA
- Identifi PHM

Passport MIS Configuration Management

Required Interfaces

Passport Capability to Store and Use Data

Passport System Implementation and Integration

Passport MIS Description and Overview

Passport understands and will comply with all the MIS requirements as described in Section 15.0 of the Draft Medicaid Managed Care Contract and Appendices.

Our MIS is a suite of fully interoperable component layers that enable Passport staff and administrators, care teams and providers to operate in a connected approach and work from a single view of the member. The platform represents an end-to-end, enterprise-level, integrated MIS and population management platform with functionalities and process flows that support the requirements of the Kentucky DMS and the Kentucky Medicaid Managed Care Program. Each subsystem supporting DMS requirements is addressed in two (2) Passport MIS platform components and is outlined in **Exhibit C.6-1**.

Evolent has a Network Operations Center (NOC) in place that provides 24/7 IT infrastructure and application monitoring through industry-leading tools, such as SolarWinds and DotCom-Monitor. Detailed standard operating procedures (SOPs) for intervention, remediation and escalation are in place for any alerts generated by the monitoring tools for conditions that meet alert thresholds that might affect uptime or performance (e.g., memory consumption, disk/storage availability, Central Processing Unit (CPU) use). In addition to proactively preventing possible service interruptions, data from the Service Desk serves as a critical input to the Passport ITIL-based problem management function for identifying root causes of matters. This provides us with the insight necessary to drive platform improvement and appropriately invest in architecture and infrastructure.

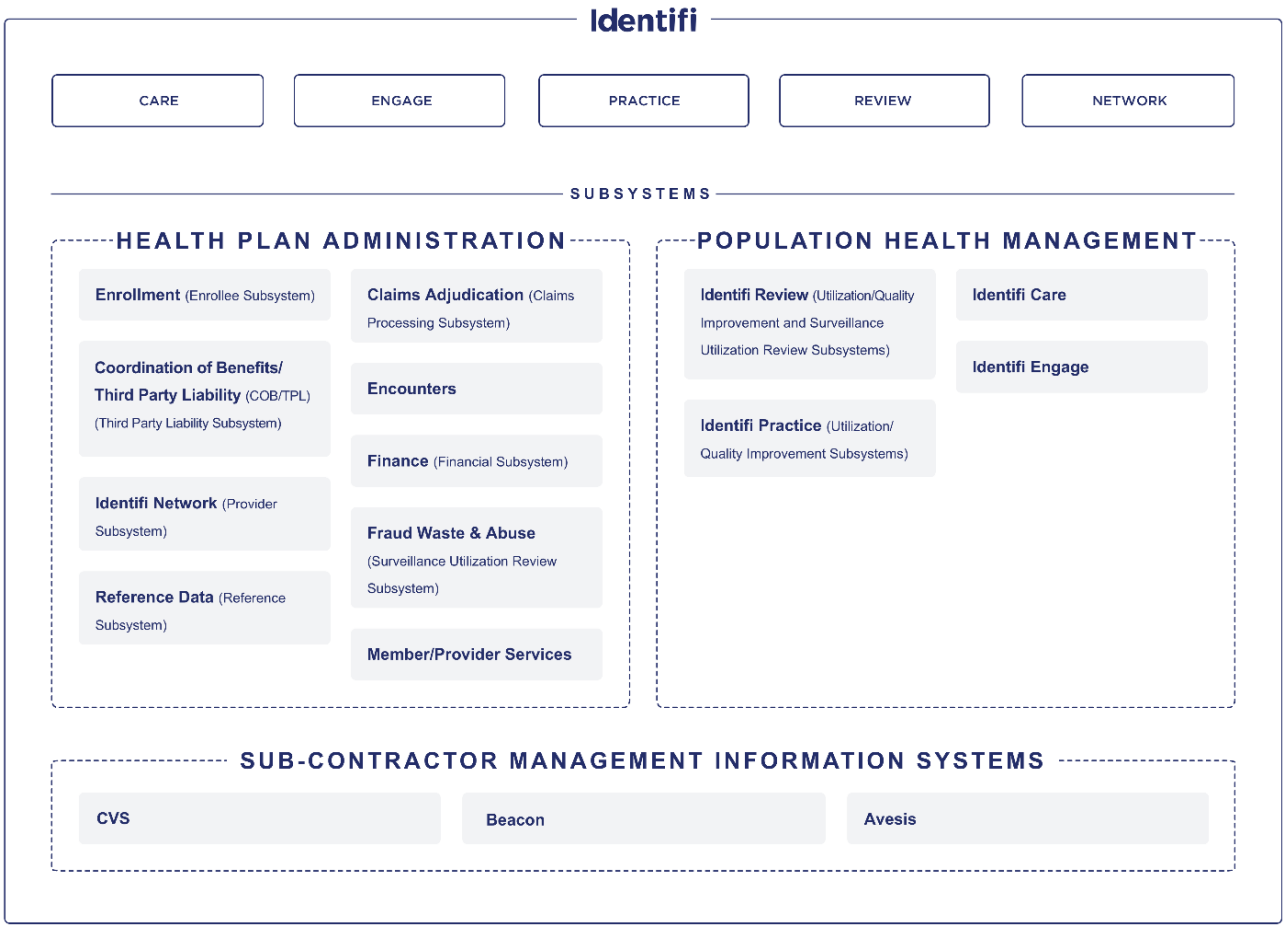
Evolent has recently made a significant investment in the technical architecture underlying the application platform to enhance stability, improve performance and provide for data, usage growth and expansion. Within the past nine (9) months, Evolent has installed a new NetApp storage platform, adding over 124TB of SSD storage in the production data center, added six (6) additional servers (close to 3TB in memory) and expanded the production web server environments.

Exhibit C.6-1: Identifi Platform MIS

Passport MIS Platform	Passport MIS Module (*Kentucky Medicaid Subsystem*)
Identifi HPA	• Enrollment **(*Enrollee/Member Subsystem*)** • Coordination of Benefits (COB)/TPL **(*TPL Subsystem*)** • Identifi Network **(*Provider Subsystem*)** • Reference Data **(*Reference Subsystem*)** • Claims Adjudication **(*Claims Processing Subsystem)*** • Encounters • Finance **(*Financial Subsystem*)** • Fraud Waste and Abuse **(*Surveillance Utilization Review Subsystem*)** • Member/Provider Services
Identifi PHM	• Identifi Review **(*Utilization/Quality Improvement and Surveillance Utilization Review Subsystems)*** • Identifi Practice **(*Utilization/Quality Improvement Subsystems)*** • Identifi Care *(Population Health Program/Care Management)* • Identifi Engage *(Population Health Program Mobile Application)*
Subcontractor Management Information Systems	• CVS • Beacon • Avēsis

The Passport MIS aligns system platform components with the functional areas required to support all aspects of the Kentucky Medicaid Managed Care Program as further depicted in **Exhibit C.6-2**, which illustrates the Identifi Platform infrastructure, system components, data and process workflows for the key business subsystems.

Exhibit C.6-2: Identifi Infrastructure and Subsystems



A detailed description of the Passport MIS platform components and modules and corresponding DMS subsystems comprised in each of the two (2) components is provided next.

Passport MIS Components

Identifi Health Plan Administration (HPA)

The Identifi HPA component supports core administrative and operational functions, including enrollment/member management, provider management and networking, reference management, financial management, claims and encounter processing and TPL processing. The MIS can process electronic data transmissions securely to add, delete or modify membership records with accurate begin/end dates; track covered services received by members; and maintain those covered services accurately and fully as Health Insurance Portability and Accountability Act (HIPAA)-compliant encounter data transactions. Using HIPAA-compliant electronic data interchanges (EDI), the MIS can transfer encounter data transactions and maintain a history of changes, adjustments and audits for current and retroactive data. Passport's MIS Business

Continuity and Disaster Recovery Plan (BC/DRP) has documented procedures and processes for accumulating, archiving and restoring data in the event of an MIS or subsystem failure.

Identifi Population Health Management (PHM)

The Identifi PHM platform component and modules enable Passport staff, care teams, physicians and administrators to operate from the same connected platform, working from a unified view of member health history, activity and care. The Utilization/Quality Improvement Subsystem is housed in this component. By using diverse data sets, the system identifies "impactable" members with high precision, engages both members and physicians in best practice management of care and analyzes both clinical quality and operational performance in near real time. The Identifi system derives these capabilities from its best-in-class intelligence engine and uses proprietary stratification and predictive modeling algorithms that transform data into a comprehensive profile of member health. Impactable members are prioritized and engaged through a variety of Identifi workflow modules for improved coordination of care, health outcomes and total cost.

At the core of our MIS's population health management system is our data integration services, member-centric EDW and advanced clinical profiling logic scalable to support different lines of business, stratification and predictive analytics. The MIS suite of predictive models and evidence-based criteria is used to identify and prioritize the most impactable members at the right time for the most appropriate clinical program and/or intervention. Members identified for intervention are stratified into risk levels through a predictive modeling process to prioritize the outreach and management. The predictive models identify members based on their likelihood of experiencing specific impactable outcomes within the next six to nine (6-9) months, such as an ambulatory care-sensitive hospital admission. The configurable rules engine is powered by proprietary clinical content, algorithms and best practices, which are continually improved through rigorous evaluation and innovation based on evidence from an ever-growing underlying data set. The rules engine intelligence includes 1,400+ preconfigured clinical rules and measures, including risk management, clinical and quality rules, and offers the ability to develop custom predictive and stratification logic to solve local market problems.

One of the most frequently cited measures of predictive performance is the model's c-statistic (the measure of the area under a reviewer operating characteristic (ROC) curve). A c-statistic of 0.5 indicates a random chance at predicting a future event (e.g., a coin flip), while a value of one (1) is a perfect predictor. A model with a c-statistic of 0.8 or higher is considered to have strong predictive ability. The MIS c-statistic is 0.82, significantly higher than the rest of the industry and indicative of strong predictive ability.

The Identifi PHM system's suite of stratification predictive models targets "impactable" future members, events and medical expenses, as further summarized in **Exhibit C.6-3**.

Exhibit C.6-3: Predictive Model Performance Metrics

Example Model	Description	Performance
Ambulatory Care-Sensitive Model	*Predicts the risk of inpatient (IP)/emergency department (ED) use for members (includes pediatrics) with one (1) of five (5) major chronic conditions*	c-stat = 0.82
Readmission Risk Model	*Real-time identification of members who are likely to be readmitted (unplanned) within thirty (30) days of discharge for any reason*	Thirty percent (30%) more accurate than the commonly used length of stay acuity of admission, comorbidities, emergency room visits (LACE) tool
Inappropriate ED Use Model	*Real-time identification of risk of inappropriate ED utilization using socioeconomic (SES) indicators, drive times and distances, among other variables*	Sixty percent (60%) more accurate than traditional (three (3) or more ED visits)
High-Risk Maternity Model	*Predicts the risk of high-cost adverse neonatal outcomes (preterm, respiratory distress and neonatal abstinence)*	Greater than ten percent (>10%) more accurate than academic published literature
Behavioral Health (BH) Risk Model	*Predicts risk of a BH-related event (inpatient and ED) and identifies members with undocumented BH issues using alternative data sets*	Two (2) times more accurate than using prior diagnosis alone
End of Life Model	*Predicts twelve (12)-month mortality using claims, clinical and social determinants of health*	Eight (8) times better than Charlson Comorbidity Index alone
New Member High-Risk Model	*Predicts risk of a new member becoming high cost at enrollment using demographics, benefit, geospatial and census data*	c-stat = 0.80 (without any medical claims data)

The system also contains the Identifi modules, a suite of modular and fully interoperable user modules that leverage outcomes from the MIS suite of predictive models and evidence-based criteria, and accesses the Identifi data infrastructure in real time while also supporting key administrative and operational functions, as well as DMS subsystems.

Passport MIS Subsystems

C.6.a.i. Enrollee/Member Subsystem

Passport's Enrollee/Member Subsystem, administered through Identifi HPA, supports DMS member requirements in maintaining accurate member records, which is the foundation for delivering effective services to Kentucky Medicaid members. Passport's Enrollee/Member subsystem houses and maintains accurate current and historical demographic data for all members and has been key to Passport's ability to provide demographic information to claims processing, supply data warehouse and online provider resources for eligibility checking, apply TPL information to claims processing to ensure that Medicaid is the payer of last resort, match primary care providers (PCPs) to each member required to have a PCP, track early

and periodic screening, diagnostic and treatment (EPSDT) preventive services and referrals, track members who are enrolled in the "lock-in" program and reconcile our capitation payment from DMS.

Passport currently receives and processes electronically transmitted enrollment and eligibility data in a HIPAA 834 file format from DMS daily enrollment files and monthly and quarterly enrollment and disenrollment reconciliation files. Within 24 hours of receipt, eligibility and enrollment databases are updated within our EDW and used by our various Identifi modules based on well-developed processes for enrollment, disenrollment and reconciliation, among others. To effectively manage the accuracy of the membership data, files are processed in the order in which they are received, and records are processed in chronological order for each member. Eligibility transactions are compared to existing member records and updated or added as necessary. Our system then completes an immediate and fully automated comparison to identify discrepancies between our system of record and the enrollment report file received from DMS. All transactions are loaded immediately. Identified discrepancies are categorized for research and resolved as needed.

Passport understands the importance of keeping its system synchronized with the Commonwealth's member eligibility data. The process of eligibility loading and updating has been identified as an area for improvement where Passport has made significant architectural investments. As a result, the daily and monthly eligibility files are consistently loaded into the platform timely and accurately. Demonstrating success, the last two (2) full monthly eligibility files were loaded into the platform in under nine (9) hours after receipt.

The system resources are constantly monitored throughout this process. Monitoring outputs are used to help refine physical server design and expansion to ensure continuity of process results. The system design is set to achieve the target results while ensuring capacity for transaction growth.

Passport will continue to leverage its system to quickly identify and resolve discrepancies between our internal membership records and the information we receive on DMS eligibility and enrollment files. The daily 834 files are transactional and provide us with the needed adds, terminations and changes to each member's eligibility records. A brief summary of these processes within the member subsystem follows.

The "health coverage (HD) segment" of the ANSI-compliant 834 file containing plan information will continue to be invoked when ingesting the records. The file itself can determine program participation, providing the information to map the members to the correct "plan" in our core system (where the "plan" correlates directly to the benefits the program allows). Additional identifiers are loaded in our front-end database for reconciliation and reporting. If no program information is available on the daily 834, the member files load to a "pending plan" until the system receives the 834 audit file and, when received with the program information available, membership is assigned to the correct "plan" in the core system. The maintenance code given will determine if the member file will be an addition, termination or change in information. "date or time DTPDTP segments" for eligibility are compared to existing members and are used to create new member records or update current records. For terminations and/or retro-terminations,

specific processes assess prior claims payments for recoupment of funds when retro-termination activity occurs. Retro-additions also have a process to reconcile claims payments for eligibility claims that are pending.

Retroactively Enrolled Members

The monthly ANSI-compliant 834 file is used to reconcile membership in our core system to the state's full file. Once all daily files are consumed, Passport typically receives an "audit file" from the state that provides all the records for active members for the current month. The programming uses member-matching criteria, including first/last name and date of birth (and other identifiers when necessary), to determine if the member is active in the system. Members who are active on the 834 audit file are found in our core system and compared to the data elements. Members who do not exist in the core system are then added, along with the information available on the 834, such as program IDs in the "HD segment" and "DTP segments" for effective dates. Members who are in our core system but not on the 834 audit file follow a process called "termed by absence (TBA)." The member is TBA on the last day of the previous month depending on the Commonwealth's rules for his/her audit file.

Tracking Member Eligibility End Dates

Identifi HPA processes member files received from DMS and is the source of truth for information for all platform systems. Any changes in a member's eligibility type typically occur in the 834 audit file, where the "HD segment" holds the program information. Each time we load the audit file, this program is compared to what is in our core system. If there is a change, then the eligibility segment is terminated and a new one is created with the new effective date of the program. In addition, the Passport Enrollee/Member Subsystem will be used to develop the following reports and files for submission to DMS, as outlined in Section 37.0 of the Draft Medicaid Managed Care Contract, including Appendix D in **Exhibit C.6-4**.

Exhibit C.6-4: Enrollee Services Reports

Report Number	Report Name	Frequency
10	*Enrollment Report*	Quarterly
11	*Ineligible Assignment*	Daily (as needed)
12	*Newborn Enrollment Report*	Monthly
13	*Changes in PCP Assignment Initiated by Member, Provider or MCO*	Quarterly
14	*Member Outreach Report*	Quarterly
15	*Member Services Annual Report*	Annually
16	*Member Call Center Report*	Quarterly (or more frequently as requested by department)
17	*Marketing Activities Report*	Quarterly
18	*KY HEALTH Call Center Reports*	Monthly
19	*EPSDT CMS–416 Report*	Annually

C.6.a.ii. Third Party Liability Subsystem

Passport's TPL Subsystem, administered through Identifi HPA, supports DMS's TPL requirements by supporting multiple levels of other carrier coverage at a member level, with associated effective and termination dates. COB coverage can be updated through batch or manual mechanisms where eligibility details may be updated through the consumption of an 834 file and submitted through electronic transactions or done manually in the user interface (UI) by authorized users. Most eligibility COB updates are executed in real time, so claims are adjudicated against updated information to flag potentially cost-avoiding claims and reduce benefit expenditures.

Passport's claims processing system uses diagnosis/procedure codes to read service-based rules, including parameters for handling benefit limitations, deductibles, copays and COB situations. The software engine adapts to rapidly changing business/regulatory environments, automates business processes, enhances efficiency, provides the flexibility to administer diverse plan designs and integrates with third-party solutions. The claims payment process for nonparticipating providers is identical to the process for participating providers but requires prior authorizations for out-of-network care. Our COB strategy uses proactive solicitation of other coverage to ensure Kentucky Medicaid is the payer of last resort without disruption to our members' care. Our process is highly collaborative and will involve regular interaction with TPL staff, other plans and insurers and families and caregivers as needed.

Multiple COB payment methodologies can be configured, including traditional, benefit-less benefit, Medicare as primary and COB savings bank calculations. Passport employs IT infrastructures and data mining algorithms that were custom-built for Medicaid COB and payers for a balanced approach to cost avoidance and recovery. Member records will be updated to reflect COB when we receive confirmation of TPL, including receipt of primary payer documentation (e.g., EOB).

If a claim is received with COB information that has not already been captured by our system, then the following workflow will be executed to ensure proper research/documentation and prompt adjudication of claims:

1. Claims with COB or primary payer information on the X12 837 file and no active COB segment for the date of services will be routed to eligibility and enrollment staff.
2. The eligibility team will update the member's COB segment within five (5) business days of receipt.
3. Following completion, the member's file will be updated accordingly.

When a third-party is liable, we deny the claim and notify the provider of the denial/other payer liability. Processing systems capture these claims for cost avoidance and TPL savings. Additional COB activities are summarized in **Exhibit C.6-5**.

Exhibit C.6-5: Performing COB and TPL

Performing COB and TPL	
COB When a Third-Party Payer Covers the Service	The following processes are used to coordinate care and payment when a service is covered wholly or in part by a third-party payer. This includes the following: 1. Kentucky Medicaid does not cover the service, but the service is covered through a third-party payer. 2. Kentucky Medicaid and the third-party payer cover the service, but Passport is only liable for the coinsurance/copayment expenses (including situations where Medicare is the primary payer).
Coordinating Care	The member's care team will coordinate member referrals to PCPs, specialists and local hospital staff. We will also reach out to the primary payer of services when appropriate (e.g., if the primary payer is the Medicare special needs plan). In cases where the other payer does not provide care management services to the member, our care team will access coverage information and help the member navigate his/her health care coverage across health care payers. Third-party coverage data is available to the care team through employee records maintained on the MIS. Care team members will coordinate with the member's provider(s) to ensure that services are billed appropriately to the correct payer.
Coordinating Payment	Passport will adjudicate claims involving third-party coverage using rules ensuring that the member's Medicaid benefit is the payer of last resort. Our claims processing system receives and stores other insurance coverage information received from DMS. Claims edits ensure that claims for services rendered to members with identified third-party resources are processed through our COB process. When a service is not covered by Kentucky Medicaid but is available from a third-party payer, the claim will be denied as a noncovered service (a remark code on the provider explanation of payment (EOP) will identify the service as denied). If the member record has a COB indicator, our denial notice to the provider will include an alert message that other coverage may be available. They can then work with their members to submit a claim to the third-party payer. Claims for covered services eligible for COB are submitted with the following information: complete/accurate claims data, eligibility and provider data and primary payer's EOBs for all services rendered, including the date the primary payer finalized payment. If multiple primary payers exist, the earlier information must be submitted for each payer.

Our processes are driven by the need for the claim to include primary party COB information. Passport does not process claims that have not been submitted to the primary payer first. For services covered by a third-party and Kentucky Medicaid, the claim will be processed first by the third-party payer. The EOB from the third-party will be used to determine coinsurance/copayment expenses for which Kentucky Medicaid is liable.

The TPL Subsystem houses and maintains verified sources of primary and secondary insurance coverage for Passport members and allows Passport to process and maintain updates received from DMS following verification, including TPL carrier, casualty and resource files. The TPL Subsystem is used to develop TPL and related claims payment reports outlined in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices and noted in **Exhibit C.6-6**.

Exhibit C.6-6: Claims Payment and Additional TPL Reports

Report Number	Report Name	Frequency
Claims Payment		
53	*Post-Payment Billing Recovery*	Quarterly
54	*COB Savings*	Monthly
55	*Medicare Cost Avoidance*	Monthly
56	*Non-Medicare Cost Avoidance*	Monthly
57	*Potential Subrogation*	Monthly
58	*TPL*	
Additional TPL Reports: (Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices)		
Cost-Avoidance Summary Savings Reports (including Medicare but identifying it separately)		Monthly
Listings and Totals of Cost-Avoided Claims		Monthly
Listings and Totals of Third-Party Resources Used		Monthly
Reports of Amounts Billed and Collected, Current and Historical, from the TPL Recovery Tracking System, by Carrier and Member		Monthly
Detailed Aging Report (for attempted recoveries by carrier and member)		Monthly
Report on the Number and Amount of Recoveries by Type (examples include fraud collections, private insurance)		Monthly
Report on the Unrecoverable Amounts by Type and Reason, Carrier and Other Relevant Data on an Aged Basis and in Potential Dollar Ranges		Monthly
Report on the Potential Trauma and/or Accident Claims for Claims That Meet Specified Dollar Threshold Amounts		Monthly
Report on Services Subject to Potential Recovery When Date of Death is Reported		Monthly
Unduplicated Cost-Avoidance Reporting by Program Category and by Type of Service (with accurate totals and subtotals)		Monthly
Listings of TPL Carrier Coverage Data		Monthly
Audit trails of Changes to TPL Data		Monthly

C.6.a.iii. Provider Subsystem

Passport's Provider Subsystem is supported through the Identifi Network module. Identifi Network is our web-based provider data management module allowing network managers to create, maintain and access provider directory data that supports the DMS Provider Subsystem and network requirements. It provides a central location for network managers to document changes and track interactions with providers and

provides the workflow and analytics tools for network administrators and executives involved in provider data lifecycle management. Identifi Network also supports Passport's provider data management workflows to add and track the lifecycle of provider data ranging from enrollment to termination and the association of providers to network, subnetwork, tiers and practices. Identifi Network also allows for comprehensive views and management of provider data.

Passport understands the importance of members having access to the appropriate level of care at the right time. Accessibility to the provider network is monitored by the Provider Subsystem to provide the most precise analysis of member access to network providers. Our Provider Subsystem supports the following processes:

- Proactively evaluate network adequacy
- Automation of member PCP assignments
- National Committee for Quality Assurance (NCQA) Certified Web and Print directories
- Assist with call center referrals
- Illustrate that services, service locations and service sites are available and accessible to provide all covered services on an emergency or urgent care basis
- House information obtained through the provider enrollment and credentialing/ recredentialing process that includes:
  - Ownership and tax structure
  - Demographics
  - Facility accreditations
  - Licensure and certificates
  - Provider type or specialty
  - Education, training, board certifications and work history
  - Malpractice history
  - Sanction information
  - Attestation of practitioner's health status and loss or limitations on licensure or privileges
  - Practitioner hospital affiliations
  - Practitioner group affiliations
- Primary source verification of NCQA, CMS and Medicaid data elements
- Claims system agreement for claim reimbursement
- Approval for network participation

The Provider Subsystem holds licensure information, including number, state, status and effective/termination dates. Passport uses Aperture for credentialing application review and identification of deficiencies and missing information. Aperture credentials a wide variety of providers and facilities by providing compliance-driven, software and professional service solutions. Additional information about Passport's credentialing process is available in **Section C.17 Provider Services**.

Reconciling the Master Provider File to Provider Certification and Claims Payment

The Passport Provider Management team will generate a weekly internal report that identifies providers who are no longer attested and require a hold added to their claims payment system record and/or were previously on hold in the system, are now attested and need the hold removed. These holds will deny payment to the respective providers indicated by the appropriate remark code, per the payment denial status code descriptions.

The reports in **Exhibit C.6-7** are produced using information housed in this system as required in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices.

Exhibit C.6-7: Provider Services and Network Reports

Report No	Report Name	Frequency
20	Provider Credentialing and Contracting Status Report	Quarterly
21	Provider Network Status Report	Monthly
22	Provider Network File Layout	Monthly
23	Network Adequacy Exceptions Report	Quarterly
24	PCP Assignment Report	Quarterly
25	GeoAccess Network Reports and Maps	No less than quarterly and more frequently as required by the Department
26	Timely Access Reports	No less than quarterly and more frequently as required by the Department
27	Provider Compliance with Access Requirements Report	Annually
28	Denial of MCO Participation	Monthly
29	Federally Qualified Health Centers and Rural Health Centers	Quarterly
30	Provider Call Center Report	Quarterly or more frequently as requested by the Department
31	Telehealth Reporting	Annually

C.6.a.iv. Reference Subsystem

Passport recognizes the need for an extensive Reference Subsystem that supports current referenceable data, as well as maintains historic data to ensure accurate and timely payment of claims and encounter processing. There are two (2) key components—Identifi Platform and its Claims Processing Subsystem, Identifi HPA and the EDW—that serve as the primary reference systems to support DMS's Reference Subsystem requirements, including referral data inputs, interfaces, processing and maintenance.

Passport's Claims (Processing) Subsystem, administered through Identifi HPA, is integrated with Payer Compass, which also allows for provider pricing, claims/clinical edits of our codes and reference data, as well as diagnosis-related group (DRG) grouping. The MIS system houses reference data relating to pricing, diagnosis, procedure, edit/audit criteria and reimbursement configuration references, codes and data.

The Identifi EDW supports inputs related to National Drug Codes (NDCs), CMS–HCPCS updates, ICD-9 and ICD-10, DMS III diagnosis and procedure updates and American Dental Association (ADA; dental codes). Code set updates are initiated through our reimbursement team; this is a collaborative effort with our configuration and database administration team. Once the code sets are updated, there is a stringent testing process to ensure the loaded information is correct and approved before production is granted. Our code updates follow a schedule where possible. We generally update the following codes:

Annually/Biannually:

- American Medical Association (AMA) on an annual basis
- The CMS ICD-10 on an annual basis
- Each year, the ADA data files are released and posted to the Optum data portal toward the end of the fourth quarter of the current year (e.g., for 2020, it will be posted during December 2019)
- Current Procedural Terminology (CPT) on a biannual basis
- The National Uniform Billing Committee (NUBC) institutional claim codes (condition code, value code, occurrence code, bill type, etc.)

Quarterly:

- CMS and HCPCS
- The National Uniform Claim Committee (NUCC) taxonomy codes

Monthly:

- NDC codes are supplied by Medispan every month, during the first week of the month for ingestion

When posted:

- American Hospital Association (AHA)
- The CMS National Plan and Provider Enumeration System (NPPES) NPIs

Most years, the AMA also releases some corrections on nonscheduled release quarters. These files are posted no less than thirty (30) days prior to the effective date of the changes.

The Identifi EDW processes reference data and maintains current and historical reference data, assuring that updates do not overlay or otherwise make historical information inaccessible. This is fundamental to ensure appropriate support to care management and utilization management (UM) functions, which leverage data that has been processed through advanced clinical profiling logic. Passport's Reference Subsystem also maintains a full procedure data set (containing medical-surgical, ADA dental and other professional service codes), as well as HCPCS pricing modifiers and specific codes for other medical services that DMS deems necessary to maintain and process in the Reference Subsystem. The Reference Subsystem maintains descriptions and maintains a diagnosis data set using ICD-9, ICD-10 and DSM III codes, which supports relationship editing between diagnosis codes and claims information.

Passport continually monitors many different sources to ensure that we have the most current information in our Reference Subsystem. Passport also uses clinical editing software, integrated through Payor Compass, for enhanced clinical and business rule editing for claims. This system allows us to ensure that professional and outpatient hospital claims are paid in accordance with the applicable medical policies, as well as

generally accepted clinical edits. In addition, for claims and encounters, the Reference Subsystem allows for maintenance of pricing for procedures and drugs, as well as diagnosis and edit/audit criteria.

C.6.a.v. Claims Processing Subsystem (to include Encounter Data);

Claims Processing Subsystem

Passport's Claims Processing Subsystem, administered through Identifi HPA, ensures compliance to DMS claims processing requirements. It supports Passport's medical claims processing. The Claims Processing Subsystem is extremely flexible and enables us to administer highly customized requirements specific to the Kentucky Medicaid contract, including benefits, eligibility, fee schedule and provider service location configuration. During the various stages of the adjudication process, this integrated Medicaid management information system (MMIS) interacts with membership eligibility, TPL data, product benefit parameters, provider pricing agreements, medical management requirements and clinical editing information to provide accurate and highly automated adjudication of claims and/or encounter submissions. Claims processing uses diagnosis codes and procedure codes to read service-based rules and includes parameters for handling benefit limitations, copays and COB situations. This powerful software engine does the following:

- Adapts to rapidly changing business and regulatory environments
- Automates business processes
- Enhances efficiency
- Provides the flexibility to administer diverse plan designs
- Integrates with third-party solutions

Identifi accommodates, and currently administers, all major payment methodologies, including fee-for-service, capitation, case rates, per diems, DRG, percentage of billed, UCR, percentage of UCR, Resource Based Relative Value Scale (RBRVS) with Graphic Practice Cost Index (GPCI), bundling, per diems, tiered per diems, lesser of billed and calculated rates, treatment case and many more. The system is capable of auto-adjudicating professional claims as well as complex multiservice inpatient hospital claims.

The claims payment process for nonparticipating providers is identical to the process for participating providers but with the exception of ED use and requires prior authorization for out-of-network care. Claims from nonparticipating providers are paid based on the appropriate fee schedule or the payment terms of any applicable single-case agreement.

The Claims Processing Subsystem is one hundred percent (100%) web-based and can process and adjudicate claims and pre-adjudicate claims in real time. The system's automated rules and real-time workflow replace manual or batch review processes to reduce duplication errors while avoiding costly clinical review and prior-authorization processes. The system's flexible architecture is rules-based and object-oriented. Reusable objects, defined and configured by our business users, deliver innovation "on the fly" with

minimum maintenance and optimal system performance, all while accommodating all major payment methodologies.

The Claims Processing Subsystem integrates with the Enrollee/Member Subsystem in real time during claims processing. Information about the member and subscriber is retrieved from the submitted claim. Using member-matching rules, the appropriate member is found. The system confirms that the member is eligible for the date of service and then uses his/her benefit plan for that date to continue processing. Similarly, the claims Adjudication Subsystem is integrated with our Provider Subsystem. All providers included on the claim are searched in the provider system using provider matching rules. The provider contract information is then retrieved and used for claim pricing.

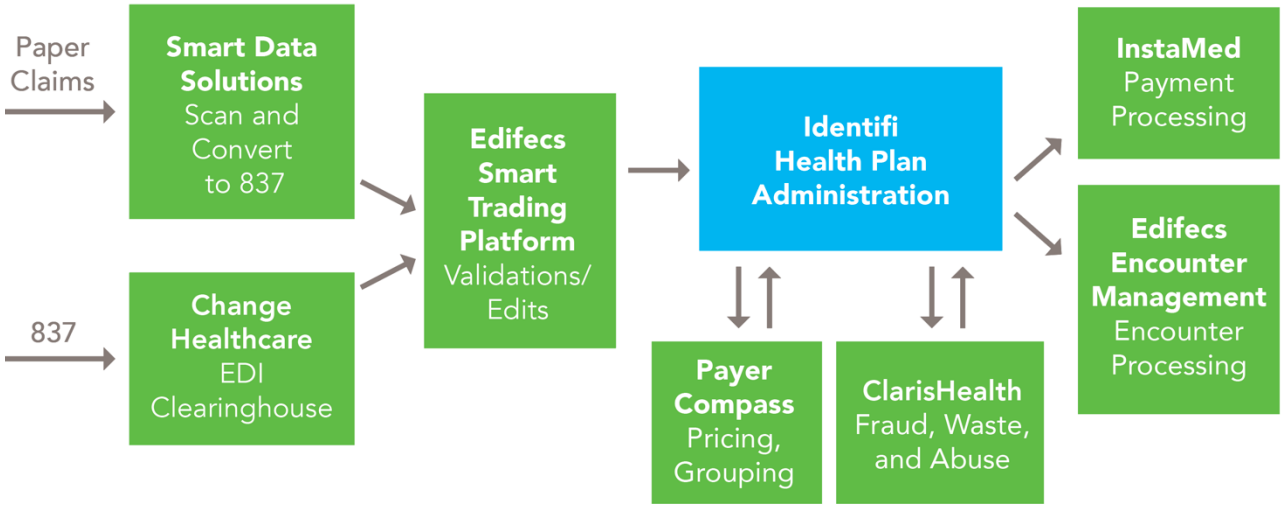
As claims are processed within the adjudication system, rules are configured to specify what services require pre-authorization. If a claim requires an authorization, the adjudication system will integrate in real time with the UM Subsystem to determine if a pre-authorization has been received and approved. If an approved authorization match is found, the available units will also be checked to determine if there are enough for the claim request.

When applicable, the claims adjudication system also tracks member accumulator data. Information about member out-of-pocket responsibility can be tracked at the plan year or calendar year. As new claims are received and processed, the member's current accumulator information is used in real time to determine his/her benefit module for the given claim. The claims adjudication system can also interface with other claims systems to consider their accumulator data when processing the claim in our system.

Providers can submit paper or electronic claims. Paper claims are scanned and converted to 837 format by Smart Data Solutions (SDS). Passport encourages providers to submit claims through a HIPAA-compliant EDI powered by the claims clearinghouse, Change Healthcare. Using Change Healthcare results in faster, more efficient and cost-effective claims submission and higher rates of automated clearinghouse payments. All paper and electronic claims inbound to Passport flow through the Edifecs Smart Trading Platform, which performs workgroup for electronic data interchange (WEDI)/strategic national implementation process (SNIP) and health plan-specific data validations. The flow of claims data into Identifi HPA and interaction with other subsystems is depicted in **Exhibit C.6-8**.

Approximately ninety-five percent (95%) of the claims currently handled by our Claims Processing Subsystem are submitted electronically, where seventy-seven percent (77%) are auto-adjudicated without any manual intervention. In addition, 70.3% and 92.7% of payment transactions are currently Automated Clearing House (ACH) and payment dollars, respectively. The claims adjudication system includes a tightly integrated workflow management solution. For claims that do not auto-adjudicate, configuration personnel set up queues for routing claims based on their status or reason for not auto-adjudicating. A web-based claims dashboard is available for the claims operations management to track in real time where claims are being pended and how many are in each pending queue. This information is used on the fly to help guide work assignments. Claims adjudicators use the workflow system to retrieve pended claims, make necessary edits and then resubmit the claims into the adjudication process.

Exhibit C.6-8: Claims Data Flow in Identifi HPA



In the event that DMS may require Passport to receive electronic claims through a DMS-contracted vendor, Passport will work to ensure that connections are in place for the MIS to receive the claims for processing. Claims that can be automatically adjudicated proceed through a comprehensive set of clinical edits, including National Correct Coding Initiative (NCCI) claim editing guidelines. Claims are auto-edited for errors, omissions and questionable coding relationships (such as bundling/unbundling, modifier appropriateness and duplicates) by comparing the billed data against an expansive database containing millions of government and industry rules, regulations and nationally accepted policies governing appropriate billing. The Claims Processing Subsystem applies medical necessity edits to detect procedures billed without supporting diagnoses or services based on national and local coverage determinations. The editing software maintains coding edits specific to Medicaid, which are separated by professional, inpatient and outpatient services. Those claims identified with edit issues are either forwarded to the manual claims review process, returned to the provider for correction and resubmission or referred to the Program Integrity Unit. We routinely track pended claims based on high-volume providers, reason codes and other trends to decrease the pend rate.

Passport will maintain and follow the DMS-approved plan of claims delivery and corresponding timelines. Our claims processing capabilities also include the register of the date a claim is received by Passport and a register of the detail of each claim transaction or action, including dates of service, at the time the transaction occurs. The system also has the ability to report each claim transaction by date and type to include interest payments, maintain information at the claim and line detail levels, maintain adequate audit trails, report claims performance measures to DMS and maintain online and archived files. As a part of the records retention policy, Passport will retain online automated claims payment history, as well as other

financial information and records, including all original claims forms, for ten (10) years post-contract as established in Draft Medicaid Managed Care Contract and Appendices, Section 37.0 Draft Medicaid Managed Care Contract and in accordance with 42 C.F.R. 438.2 and 907 KAR 1:672. This will allow the claims data to be easily sorted and produced in formats as requested by DMS on a set cadence or on an ad hoc basis.

The claims adjudication system has been architected with scalability and performance at the forefront. Processing of EDI 837 files is performed by splitting the claims and using multithreaded processes to adjudicate many claims in parallel. The system has demonstrated the ability to process large files containing upward of 20,000 claims in production operations. These large files process through the system in a couple of hours and do not interfere with any online users also interacting with the system. Claims adjudicators, customer service representatives and any other users of the system are free to use the platform while these claims are being processed. Also, in production operations, the system routinely handles very large institutional claims that contain over eighty (80) claim lines. The system is optimized for large claims and can handle all the outliers.

The system has also been architected to be highly available and fault tolerant. As the hardware infrastructure is designed using redundancy, there are rare instances where a large file may be interrupted during its processing. The system is designed to commit fully to an entire claim as a single transaction only if that claim is complete. Each claim is its own individual transaction. If a file does encounter an issue, then the file can be restarted and claims that have already finished will remain committed. Only the remaining claims must be processed.

As a part of the reporting suite for the Claims Subsystem, reports are available on a monthly cadence that showcases the number of claims received, paid, denied and suspended for the previous month by provider type with a reason for the denied or suspended claim; the number and type of services that are prior-authorized (PA) for the previous month (approved and denied); the amount paid to providers for the previous month by provider type; the number of claims by provider type for the previous month, which exceed processing timeline standards defined by the Department; and claim prompt pay reports as defined by the American Recovery and Reinvestment Act (ARRA). The reports in **Exhibit C.6-9** are produced using information housed in this system, adhering to the claims payment report requirements outlined in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices.

Exhibit C.6-9: Claims Payment Reports

Report Number	Report Name	Frequency
47	*Copayments*	…
48	*Encounter Data Comparison Report*	Quarterly
49	*Prompt Payment*	Quarterly
50	*Original Claims Processed*	Monthly
51	*Original Claims Inventory*	…
52	*KY HEALTH Original Claims Processed*	Monthly
53	*Post-Payment Billing Recovery*	Quarterly
59	*Out-of-Network Provider Report*	Quarterly
60	*Payment of Abortion Procedures*	Quarterly
61	*Monthly Benefit Payments*	Monthly
62	*Quarterly Benefits Payment*	Quarterly
63	*Provider Outstanding Accounts Receivables*	Monthly
64	*Provider-Preventable Conditions*	Quarterly

Encounter Processing Subsystem

Passport's Edifecs Encounter Management (EM) Processing Subsystem, administered through Identifi HPA, supports DMS encounter processing and management requirements and delivers a consolidated system that ensures accuracy, completeness and timeliness of encounter data submissions with robust capabilities to submit outbound encounters and regulatory financial fillings to meet all Commonwealth requirements.

Our EM and reporting process consists of four (4) key components: intake/preprocessing, encounter creation, submission, response and reconciliation across the following transaction forms, including 837I–Instructional Transactions, 837P–Professional Transactions, 837D–Dental Transactions, 278–Prior-Authorization Transactions, 835–Remittance Advice, 834–Enrollment/Disenrollment, 820–Capitation, 276/277–Claims Status Transactions, 270/271–Eligibility Transactions, 999–Functional Acknowledgment and NCPDP 2.2.

The entire process is managed by a set of components that track all aspects of the encounter data submitted, reconcile the DMS responses and coordinate resubmissions. A full suite of reports provide transparency to claims submission lifecycle and claims compliance. As detailed next, Passport's Edifecs Encounters Processing Subsystem is one component of a comprehensive strategy to improve and sustain optimal encounter submission and completion rates.

Accuracy, Timeliness and Completeness of Encounter Data Submissions

As referenced earlier in this response, Passport migrated to Identifi HPA in 2017 to increase our capabilities and to keep up with the changing health care industry. This was part of a larger effort to transform our business model, system infrastructure and employee talent to better serve our Kentucky constituents. Our Passport leadership acknowledged that business transformation was necessary to make our operations more scalable and agile to support the requirements and needs of DMS, our members and providers. An implementation of this scope and size is often complex and multifaceted, and we knew that we could encounter consequences. As we migrated to the new system, we experienced implementation challenges that impacted encounter data. We immediately began working to resolve the problems, and today, we have stabilized ongoing operations and are realizing positive results.

As Passport progressed through the business transformation, we addressed the issues we were experiencing. We strongly believe that we are on track to fully remediate our issues and, our resulting encounter completeness rates at year-end 2020 will be better than target thresholds.

While challenges as a result of new implementations may be common, we focused on ensuring that our members and provider community receive best-in-class service to minimize their exposure while we worked to effectively overcome the challenges experienced in the migration to new systems. Passport continues to remediate remaining issues. The changes made are resulting in improved encounter submission metrics, as evidenced by our improvement from Commonwealth fiscal year (SFY) 2018 to SFY 2019 in the following categories:

- **Submission Rate:** Throughput increased from eighty-eight percent (88%) to over ninety-five percent (95%). We are committed to achieving one hundred percent (100%) by year-end 2020.
- **Acceptance Rate:** Commonwealth acceptance of encounters improved from ninety-five (95%) to over ninety-nine percent (99%).
- **Completeness Rate:** Rates for complete encounters increased from eighty-seven percent (87%) to over ninety-six percent (96%). We are committed to achieving ninety-nine (99%) by year-end 2020.
- **Timeliness Rate:** New-day claims average timeliness rate improved from eighty-five percent (85%) to over ninety-five percent (95%).

Passport will continue to leverage a dedicated EM team to oversee our encounter data submission process and serve as a Kentucky-based point of contact for issues related to encounter submissions. Passport uses proven approaches for collecting, validating and submitting complete and accurate encounter data in a timely manner, consistent with regulatory requirements in Section 16.0 of the Draft Medicaid Managed Care Contract and Appendices.

Collecting Complete and Accurate Encounter Data

Passport manages all aspects of submission and reconciliation of encounters without the cost and complexity of operating multiple systems. Integrated exception management workflows drive rapid correction and resubmission of rejected encounters. Adjudicated medical claims are extracted from our Claims Subsystem and loaded into the Edifecs EM platform in a proprietary CSV file format. Edifecs EM generates outbound encounter extract files in accordance with Kentucky Medicaid encounter file submission specifications. The system queues and tracks the claims that have been extracted for submission and reconciles the acceptance, failure or warning status upon receipt of Commonwealth response files. The entire process starts with collecting all required components of an encounter into source input files that identify required data elements to be included in the claims extraction process. Encounter collection also includes data exchange with subcontractors/capitated providers, with our process including all finalized claims, paid and denied, as well as zero-dollar claims. Identifi's HIPAA-compliant EDI framework supports data exchange with providers/subcontractors who submit encounters for reporting to DMS. Submissions from providers/subcontractors are validated according to the processes outlined in **Exhibit C.6-10**.

Exhibit C.6-10: Encounter Submission Collection and Submission Process Steps

Process Step	Description
Validating Encounter Data	Prior to submission, our team validates files against X12/HIPAA standards using WEDI SNIP Level-4 verification. We apply state-specific rules (per DMS-prescribed formats for encounter submission) and custom rules in the verification process. We will support DMS's validation efforts by comparing chart reviews of samples of members to our reported member encounter data. Records/claims data and the validation of any files used in this process are available upon request. When modifications to the collection, validation or submission are necessary, Passport will follow an established process to make the necessary changes.
Submitting Encounter Data in a Timely Manner	Passport will submit encounter data files electronically. Our submission process reports encounter data using ASC X12N 837I, 837P, 837D and NCPDP file formats. Files are generated within two (2) business days of the end of each payment cycle. Passport will submit encounter data files to DMS monthly and include all encounter data and adjustments processed by Passport and our subcontractors. Passport ensures that DMS receives complete and accurate encounter data no later than thirty (30) days after the month the claim was adjudicated. This process includes encounter tracking to monitor its lifecycle (from initial extraction of the claim, to data validation status, to Commonwealth submission, to Commonwealth response). If an encounter returns with rejections, it is monitored for aging/resubmission. Daily reports are sent to work groups to ensure timely submission and corrective actions taken in situations where timely submission is at risk.

Process Step	Description
Monitoring for Completeness and Managing Nonsubmission	Passport will develop and submit an annual Data Completeness Plan to DMS for review and approval, describing how claims/encounters will be submitted accurately in a timely fashion by providers/subcontractors. We will demonstrate resolution and resubmission of denied encounters, outline our evaluation of provider/subcontractor compliance and show our process for acting on issues uncovered by our monitoring activities. Our approach includes a process for assessing the completeness of our files and addressing provider/subcontractor nonsubmission.
Assessing Completeness of Encounter Files	Passport validates subcontractor provider encounter files in-depth. We review the process for capitated providers to submit information sufficient to report encounters during the provider orientation process. In production, the encounter submission process performs a basic X12 WEDI SNIP Level-4 verification to assess submitted information completeness before file submission to DMS. Subcontractors notify their assigned encounter analyst by email when they have uploaded their weekly encounter files, including record counts. When the aggregated encounter file is compiled, Identifi HPA will produce a reconciliation report that shows encounters by subcontractors. Our analysts then verify that all subcontractor encounters are included in the file and compare record counts to validate completeness using internal monitoring reports to track subcontractor encounter submissions.
Managing Provider Nonsubmission	Passport will monitor capitated provider submissions to detect incomplete or nonsubmission based on historical service patterns. Capitated providers will undergo annual medical record audits to ensure that they have been submitting complete and accurate encounters. If incomplete or nonsubmission is suspected, our Encounter Department will contact the provider to address the concern. Consistent issues with incomplete or nonsubmission will result in the provider being required to implement corrective action. If a provider cannot address these issues, then his/her provider agreement will be amended to end the capitated arrangement, and the provider may also be reviewed for possible fraud, waste and abuse (FWA) and may be referred to investigation.
Managing Subcontractor Nonsubmission	Passport will work closely with our subcontractors on issues related to encounter submission. Our subcontractor oversight process includes specific steps to ensure timely and accurate submission of encounter data. Encounter reporting processes are used with all subcontractors included in this proposal who will be handling provider payments. The Encounter and Data Operations teams will maintain a subcontractor contact list for any issues that occur during submission (e.g., host connection issues, file nonreceipt or file validation failure). Inbound data will be proactively monitored against expected delivery dates/frequencies, and any deviations from expected schedules will be logged and promptly investigated for root cause and remediation.

Data quality and integrity upon receipt of data will be monitored throughout processing. Upon operational ingestion of data, we will execute quality checks, as well as customized plan-specific validations. We monitor key volume and metric trends on an ongoing basis, measuring against historical trends and upper/lower control limits for consistency and completeness in inbound data. We use these monitoring procedures and alerts to ensure that we receive timely and accurate encounter data submissions from subcontractors. Encounter analysts meet weekly with each subcontractor to discuss encounter data and provide error resolution prior to our monthly submission of data to DMS. All reported encounter data will have procedure, diagnosis and other codes as explicitly directed by DMS. If exceptions need to be made to these standards, these exceptions will be considered on a code-by-code basis upon approval from DMS through a written request from Passport. Passport will also use the provider numbers as directed by DMS for data submissions. Further details on the encounter submission process are provided in **Section C.7 Encounter Data**.

C.6.a.vi. Financial Subsystem

Passport's Financial Subsystem, administered through Identifi HPA, supports DMS's administrative and financial requirements. Passport's Financial Subsystem leverages data that has been processed within its Claims Subsystem. As outlined earlier, a key component of Passport's MIS is the Claims Processing Subsystem in partnership with InstaMed® for the payment functionality. Collectively, the Financial Subsystem circumscribes processing around claim payments, adjustments, accounts receivable and other financial transactions. We maintain the remittance address in the claims system while InstaMed maintains provider Electronic funds transfer (EFT)/electronic remittance advice (ERA) election information or provider bank account information. We produce HIPAA-complaint 835 files as part of the check-run process and pass those files to InstaMed.

Providers enroll directly with InstaMed for EFT/ERA payment and transmission. If a provider is not enrolled with InstaMed, the remit address information from the 835 is used to create a paper check and EOP that is mailed to the provider. InstaMed operates a 24/7/365 technical and operational infrastructure with over 99.9% uptime. InstaMed is compliant, independently certified and audited at the highest levels for both health care and payment processing.

This process ensures that all funds are appropriately disbursed for claims payments and that all post-payment transactions are applied accurately to produce remittance advice statements, explanation of benefits (EOB) and a multitude of financial reports. To close out the claims processing cycle, Passport processes two (2) remittance cycles a week. Providers' selections with regard to bank account remit address, format and media for remit and other payment-related data define where payment is made. This data, along with any current adjustment data (for example, negative balances), are taken into account in the remittance processing phase. Passport's Financial Subsystem allows for updates of provider payment data; tracking of financial transactions, including TPL recoveries; and maintenance of adjustment and recoupment processes.

Passport's system also allows for processing of recoupments, mass adjustments and cash transactions, and it is able to accept retroactive changes to member financial liability and TPL retroactive changes and additional provider, member and reference data from the MIS.

All claims are processed on the Passport Claims Subsystem with the exception of pharmacy claims, BH, dental and vision claims. We encourage providers to submit claims through a HIPAA-compliant EDI powered by the claims clearinghouse, Change Healthcare. Using Change Healthcare means faster, more efficient and cost-effective claims submission and higher rates of automated clearinghouse payments, which in turn are issued from a Passport bank account. The built-in Change Healthcare functionality segregates the payments by categories, such as capitation, inpatient, outpatient, specialist and lab. The Change Healthcare file is balanced to the total of the check and EFT registers prior to being uploaded into the Passport system.

Pharmacy, BH, dental and vision claims are processed through subcontractors. Claim reports/invoices are received from subcontractors on a weekly basis. Each subcontractor issues the payments from its own bank accounts and receives reimbursement from Passport. The subcontractor data is balanced to the claims detail prior to issuing a wire payment to each subcontractor. The wires are entered into the Passport accounts payable system for accounting entry purposes and are part of the monthly bank account reconciliation process.

Passport's Financial Subsystem can perform payment processing, as well as adjustment processing. Any claims that have passed all required edits, audits and pricing processes (including any that are denied) are processed for payment by Passport. When performing and maintaining adjustment processing and its associated data, Passport's system can maintain original claims and their results of adjustment transactions in its claims history. The system is able to reverse the amount previously paid/recovered and then process the adjustment so that it can be easily identified, including editing, pricing and auditing each adjustment, which includes checking for duplication against other regular and adjustment claims. Negative adjustments are systematically satisfied by new provider claims payments without user intervention. Provider refunds, whether solicited or unsolicited, are also posted and reconciled in Passport's Financial Subsystem to specific adjusted claims, keeping the audit trail intact.

In addition to the automated payment and adjustment processing, identification of enrollment discrepancies and audits are performed on all manually written work completed by Enrollment Unit staff. Records are randomly selected, and an audit is performed on the work of any team member who completes enrollment functions, including processing of any new enrollments, and changes or deletions from the membership file. Detailed quality reports that document overall accuracy and error trends are provided to the manager on a monthly basis. This information is used for training and performance monitoring purposes.

The following reports in **Exhibits C.6-11** and **C.6-12** are produced using information housed in this system, adhering to the Administrative and Financial and Capitation Report requirements outlined in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices.

Exhibit C.6-11: Administrative and Financial Reports

Report Number	Report Name	Frequency
1	*Annual Managed Care Program Report*	Annually
2	*Operating Report*	Annually
3	*National Association of Insurance Commissioners (NAIC) Financial Statements*	Quarterly and Annually
4	*Audit and Internal Control Reports*	Annually
5	*Statement on Standards for Attestation Engagements (SSAE) No. 16*	Annually
6	*Medical Loss Ratio (MLR) Report*	Quarterly and Annually (with annual audits)
7	*Total Cost of Care (TCOC) Per Member Per Month (PMPM)*	Annually
8	*Expenditures Related to MCO's Operations*	…
9	*Pass-Through Payment Reporting*	Quarterly

Exhibit C.6-12: Capitation Payment Reports

Report Number	Report Name	Frequency
44	*Capitation Payment Request*	Monthly
45	*Capitation Duplicate Payment*	Monthly
46	*Capitation Adjustment Requests*	Monthly

C.6.a.vii. Utilization Data/Quality Improvement Subsystem

Utilization review/quality improvement and SURS are supported by the PHM system component, including the Identifi Review, Identifi Care, Identifi Practice and Identifi Engage modules described below.

Identifi Review is Passport's UM application with service-level agreement (SLA)-driven workflows and medical policy administration to support DMS utilization review/quality improvement and SURS by reducing inappropriate utilization. Passport's full suite of UM interventions includes prior authorization/prospective review, inpatient concurrent review, post-acute care/retrospective review, referral management, member and provider appeal, and member complaints and grievances. The data derived within the Identifi Review application fosters the development of robust utilization data to aid in quality improvement activities. Identifi Review allows Passport to actively monitor and manage underutilization and overutilization of services across the health plan.

Key features of Identifi Review include:

- Collaborative, SLA-driven workflow across UM teams with appropriate medical director escalation
- Auto-fulfillment of UM letters and electronic faxing for outbound communications
- Integrated appeals workflow and processes

- Fully enabled medial management through integration with Identifi Care
- Efficient medical necessity review through integration with InterQual and a license with Milliman
- Single point of access to view member profiles and member history
- Provider authorization request and submission status through integration with Identifi Practice
- On-demand, real-time reporting to track productivity, SLA adherence, IP utilization, etc.

Identifi Review maximizes the return on investment (ROI) of clinical resources by providing UM nurses with complete and real-time clinical and financial information and by pairing with Identifi Care to enable a truly integrated medical management model. Rich member profiles combine member demographic and contact information, claims, labs, biometrics, program eligibility, Continuity of Care Documents (CCDs), admission, discharge and transfer (ADT) data, care gaps, risk scores and other data. Automated workflows trigger follow-up action items for UM staff in a single, integrated platform and provide the ability to share UM requests with physicians and team members for review. Work queues prioritize follow-up actions based on SLA-configured requirements.

Intelligent workflows based on proprietary NCQA-certified UM programs and SLA-driven work queues eliminate manual tracking of SLAs. Full integration with Identifi Care enables real-time visibility into the status of all UM requests for care management (CM) staff and status of care management programs for UM staff, as well as enables joint UM/CM responsibilities. Integration with InterQual enables evidence-based decision support for each UM review line. Our UM model also includes pharmacists who support both pharmacy and medical UM development and operational functions. This type of integrated pharmacy model brings clinical pharmacy expertise to optimally manage cost and utilization of trend-driving, physician-administered specialty medications. Providers will be able to submit requests for physician-administered drugs as well as outpatient medications through Identifi Practice or by fax, phone, email and mail. The electronic prior authorization solution in Identifi Practice allows providers to receive a status on the submitted prior authorization or nonpreferred exception request and submit additional supporting documentation, as necessary. Identifi Review shares authorization request data with the Identifi Health Plan Claims Adjudication module to streamline processing when the claim is submitted after the service.

Identifi supports highly configurable auto-authorization rules that reduce administrative burden and reduce the time a provider must wait for a decision. These rules can be configured according to a variety of member (e.g., age, gender, diagnosis code), procedure and provider (requesting, attending, rendering) data elements. Passport uses machine learning and other analytics on historical authorization data and trends to identify potential auto-authorization rules to configure in Identifi. Our platform also supports integration of service authorization determinations with our claims processing system to support timely claims payments.

In addition to UM, Identifi Review includes management of auth-based as well as stand-alone appeals (e.g., claims appeal, lock in appeal). Appeals functionality includes an SLA-driven task-based workflow, an appeal-specific reference number for easy identification, and the ability to edit most data fields. The task queue includes sending a communication (e.g., acknowledgment, decision) and making a decision. In addition, auth-based appeals can be linked to the related auth request for quick reference/access.

Our UM system also has extensive reporting capabilities that allow us to monitor and report timeliness of review and determination within the required Commonwealth turnaround time frames. Standard UM and appeals reports available to Identifi Review include but are not limited to:

- Authorization Dashboard
- Inpatient Dashboard
- Request and Procedure Dashboard and details reports (e.g., request details, review details, care note, communications)
- Readmissions reports
- Productivity Dashboard and details reports
- SLA summary and details reports
- Appeals reports, with supporting care notes and communications details reports

The reports in **Exhibit C.6-13** will be produced from information housed in our Utilization Data Subsystem as required in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices.

Exhibit C.6-13: Utilization Management Program Reports

Report Number	Report Name	Frequency
72	*Prior Authorizations*	Monthly
73	*Utilization Report*	Quarterly
74	*Utilization of Subpopulations & Individuals with Special Health Care Needs*	Quarterly
75	*Behavioral Health Services In/Out State Facility Utilization*	Monthly
76	*Utilization Management Program Annual Evaluation*	Annually

Identifi Care is Passport's NCQA-compliant care management workflow and performance management application that enables the Passport care team to efficiently and effectively engage members in the care management process. The application supports multidisciplinary care teams in triaging members, conducting assessments, developing care plans and managing their list of prioritized action items in a guided workflow that aligns with the clinical model. Cross-functional collaboration within the application helps to engage the broader care team (physicians, pharmacists, dieticians, social workers, care advisors and care coordinators) on a common set of problems, goals and interventions, thereby maximizing ROI on care management by focusing on high-risk members. Identifi Care leverages the same longitudinal member profile available in Identifi Review (see Identifi Review section above).

Identifi Care prioritizes members for care management applications using a best-in-class intelligence engine that leverages proprietary predictive modeling algorithms to identify the most "impactable" members with high precision and then determine the most appropriate clinical program for those members. These predictive models leverage all available information about a specific member including claims and clinical data, as well as other social data sources (e.g., public housing data, consumer data) to stratify

members based on their likelihood of experiencing specific impactable outcome within the next six (6) to nine (9) months, such as an ambulatory care-sensitive hospital admission.

As noted earlier, one of the most frequently cited measures of predictive performance is the model's c-statistic (the measure of the area under a ROC curve). A c-statistic of 0.5 indicates a random chance at predicting a future event (e.g., a coin flip), while a value of one (1) is a perfect predictor. A model with a c-statistic of 0.8 or higher is considered to have strong predictive ability. The MIS' c-statistic is 0.82, significantly higher than the rest of the industry and indicative of strong predictive ability. The Identifi PHM system's suite of stratification predictive models targets "impactable" future members, events and medical expenses as further summarized in **Exhibit C.6-3** presented earlier in the MIS section.

Identifi Care was purpose-built both to ensure strong alignment with care management operations and to drive maximum clinical impact, all while reducing the cost of care. The module supports a member-centered, holistic approach to assessing, planning and implementing personalized care plans aimed at improving members' physical and behavioral health, functional status and overall quality of life. Identifi Care is preloaded with proven longitudinal and episodic clinical programs as well as a full suite of NCQA-compliant assessments that prompt care advisors with evidence-based intervention recommendations. These recommendations are supplemented by the Care Advisor's clinical judgment to create a personalized care plan for the member.

Identifi Care also supports collaboration across all members of the care team, including pharmacists, social workers and other clinicians. All documentation can be shared across care team members, and individual users can create and assign action items to other care team members as needed. Care notes and care plans can also be shared with physicians through Identifi Practice.

Identifi Care has embedded workflow solutions for common tasks managed by the care team:

- Gaps in care are identified by a configurable rules engine that leverages all the available data for a member. Identifi Care users can view currently open care gaps and the history of closed gaps (based on claims data or user intervention). Care gaps can also be closed based on information collected from the member. The latest status of care gaps is shared with Identifi Review and Identifi Practice users.
- The member's medications can be reconciled, combining data collected from claims with member-reported data (e.g., for over-the-counter medications). Medication status can be updated on a recurring basis.
- All Identifi Care users can document and contribute to a history of communications, including any materials sent to the member or extended members of the care team. Identifi Care also retains a history of care notes for the specific care management program.
- Identifi Care users can document the PCP who is coordinating care for the member (which may be different than the assigned PCP based on eligibility files).

Identifi Care includes embedded reporting that summarizes an individual Care Advisor's member panel, highlighting members who require intervention. Manager-level views also support performance management across individual care advisors, focusing on actions that drive the most impact based on evidence-based analysis.

Identifi Practice (Practice) is Passport's provider-facing portal that supports utilization/quality improvement. Practice is designed to inform providers about actionable opportunities within their member panels by surfacing information about care gaps, active care management programs, and cost and utilization metrics. Practice integrates with provider EHR systems to promote data exchange, improving care efficiency and the accuracy of our risk stratification models.

Practice includes several pre-built member rosters that can be further customized by providers and their staff. The Total Members roster includes a snapshot of all members attributed to a provider or practice, detailing the risk of impactable ED visits and inpatient admissions, status of care management programs (based on activity in Identifi Care), the number of open care gaps for each member, and chronic conditions identified for each member. A more focused roster highlighting members with care gaps identifies all the open care gaps within a provider's panel.

Providers can also obtain additional details by drilling into a specific member from one of the rosters or by searching for members individually. Once on the member profile page, providers can view problems, goals and interventions for members enrolled in care management or view the complete care plan provided by the Care Advisor to the member. Providers can also access details about open care gaps for that member, as well as close care gaps based on education provided to the member or electronic medical record (EMR) chart review.

Practice also includes detailed interactive reports that highlight compliance with quality measures relative to targets or additional details about their panels, including recent medical and pharmacy service history. Quality measure compliance is calculated by a customizable rules engine that includes both NCQA-certified Healthcare Effectiveness Data and Information Set (HEDIS) measures and "HEDIS-like" measures that include some variation from HEDIS specifications (e.g., relax continuous enrollment requirement). Member-, provider- and practice-level results are available to providers/practices through Practice, but Passport can support broader quality improvement initiatives through access to the complete data set. This allows Passport staff to define quality improvement initiatives that target specific measures and/or providers/practices based on current and historical performance.

Practice also allows providers and their staff to submit prior authorization requests (inpatient, outpatient, durable medical equipment (DME)) directly to the Passport UM team. Providers and practice staff can edit requests after initial submission and upload supporting information electronically. The status of authorization requests is available in real time to Practice users (based on their security profile).

The flexibility and modular design of the system has allowed Passport to easily adapt to the requirements of the Kentucky statewide plan. In fact, the system was recently upgraded to enhance scalability and the ability to provide data in a structure for DMS' needs.

The reports in **Exhibit C.6-14** will be produced using information housed in our Quality Improvement Subsystems as required in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices.

Exhibit C.6-14: Quality Reports

Report Number	Report Name	Frequency
32	*Report of Quality Improvement Activities; Monitoring Indicators, Benchmarks & Outcomes*	Annually
33	*Quality Assurance and Performance Improvement (QAPI) Status Reports*	Quarterly
34	*34 QAPI Annual Report*	Annually
35	*Performance Improvement Projects Status Reports*	Quarterly
36	*Audited HEDIS Reports*	Annually
37	*Other Quality & Performance Measurements Reports*	Quarterly & Annually
38	*Member Satisfaction Survey Report*	Dependent on Survey Timing
39	*Provider Satisfaction Survey Report*	Dependent on Survey Timing
40	*Member Appeals & Grievance Activity*	Monthly
41	*Provider Appeals & Grievance Activity*	Monthly
42	*KY HEALTH Grievance Activity: Members and Providers*	…

Member-Facing Mobile Application

Passport members who are actively enrolled in care management programs have access to the **Identifi Engage** (Engage) mobile application to facilitate two-way (chat) communication with their care team. Chat messaging supplements traditional telephonic and in-person communication, allowing frequent and convenient communication between members and care advisors to maintain program engagement while limiting interruptions in members' daily lives. Engage also provides an additional channel that provides directions and interventions to the member (e.g., links to resources, recipes, etc.). Engage is available via the iOS and Android app stores.

Passport Member-Facing Mobile Application Expansion

For the proposed contract period, Passport intends to expand smartphone application availability to the full plan membership. In this model, the smartphone app will be freely available to all members regardless of prior engagement with Care Managers or other plan staff. Upon downloading the app from iOS or Android stores, members will be able to perform a wide variety of core health plan functions, including:

- Registering for the app and managing their login/password
- Validating their coverage history including effective and termination dates
- Viewing status of claims submitted and any accumulators
- Searching in provider directories

C.6.a.viii. Surveillance Utilization Review Subsystem (SURS)

The Passport SURS incorporates our FWA detection tools. Our claims processing system, leveraged through Identifi HPA, uses a custom-designed FWA program from ClarisHealth. In turn, ClarisHealth utilizes a suite of analytics designed to identify aberrant claim patterns with a comprehensive claim and case management platform, enabling efficient tracking and reporting of all recovery activity. It also includes claims editing to identify potentially wasteful or fraudulent claims and can pend claims from providers or for services to members who are being investigated for potential FWA.

SURS incorporates industry-leading anti-fraud technology, allowing for substantive surveillance utilization review. It also includes case tracking, data manipulation and visualization tools, ad hoc and scheduled analyses, and claims editing to identify potentially wasteful or fraudulent claims. In addition, it can pend claims from providers or for services to members who are being investigated for potential FWA. By leveraging built-in FWA capabilities, Passport can conduct claims reviews to identify patterns that may be indicative of FWA on a prospective and retrospective basis. Together, these tools are used to identify potential FWA, such as overutilization; up-coding; high-dollar claims; unusual patterns by subscribers, providers or facilities; unusual dates of service; excessive time units for time-based codes; unusual claims volume by providers or members; unbundling services; incorrect reimbursement to providers, members, facilities and/or pharmacies; and incongruous procedure code, prescription and diagnostic code combinations.

Passport works diligently with other subcontractors on FWA efforts. For example, our dental and pharmacy administrators run targeted algorithms to detect potential fraud and identify anomalies for further review. The way that SURS leverages ClarisHealth grants the ability to analyze claims data to identify potential member and provider FWA.

Exhibit C.6-15 lists the reports produced using information housed in this system, adhering to the Program Integrity Reports outlined in Appendix D–Reporting Requirements and Reporting Deliverables.

Exhibit C.6-15: Program Integrity Reports

Report Number	Report Name	Frequency
65	*SUR Algorithms*	Monthly
66	*Provider Fraud, Waste & Abuse*	Quarterly
67	*Member Fraud, Waste & Abuse*	Quarterly
68	*Medicaid Program Lock-In Report*	Monthly
69	*Medicaid Program Violation Letters & Collections*	Monthly
70	*Explanation of Member Benefits (EOMB)*	Monthly
71	*Overpayment Recoveries*	Annually

Member/Provider Services & Telephone Management

Member/provider services, communications and support are intrinsic to our mission, with Identifi HPA managing the call centers where incoming calls are routed through an automatic call distributor to the first available customer service representative and then logged in Identifi HPA for tracking/reporting. To expedite routine eligibility verification calls, we use interactive voice response (IVR) technology, so that providers or members can verify eligibility by entering the member's identification or social security number when prompted. Once the member's ID is entered, the IVR system provides the member's status as either eligible or not eligible for benefits as well as the member's PCP and office visit copayment amount. Our call centers have the following features:

- System routing, tracking and reporting capabilities to ensure smooth transitions, management of information and operational reporting for internal teams as well as DMS
- Management of Customer Service Representative (CSR) teams to allow workload balance through skill level assignments
- Live dashboard monitoring of queues so real-time adjustments can be made based on volume
- Live call-monitoring capabilities
- Record retention, where calls are recorded and maintained for no less than ten (10) years
- Ability for auditors to use both recorded and live calls for quality monitoring
- Storage of quality auditor score sheets
- Automated reports that allow management to track daily and month-to-date SLAs
- Phone number for members that routes to a call center representative, where the only option a member has to choose is English or Spanish
- Phone number for providers that allows the option of an IVR or live call center representative (providers can also select an option to be routed to a live representative from the IVR if they need further information).

Subcontractor Management Information Systems

Passport contracts with highly qualified vendors to manage specific portions of the services rendered through the managed care program. CVS/Caremark (CVS), Beacon Health Options, and Avēsis use sophisticated management information systems that work in concert with our core system, allowing us to effectively manage and oversee member service delivery.

CVS/Caremark

CVS fully owns and maintains a proprietary, integrated claims processing suite of systems called RxClaim, which has been operational since 1995. CVS owns the source code, enabling quick changes to the software based on Passport's needs. The system is scalable, flexible and continuously enhanced to keep pace with Passport's requirements, enterprise system enhancements and ever-changing market needs, including state and federal requirements. Passport leverages shared interfaces and integrated file transfers with CVS to manage and oversee the delivery of pharmacy benefits to members.

RxClaim is designed to allow flexibility in the administration of multiple plan designs in Passport's prescription drug program. Anticipating needs, the suite of systems is designed without upper-limit boundaries, and system hardware is upgraded before current bandwidth or CPU cycle allocations/capacity levels are exhausted.

System Architecture

CVS uses IBM's most advanced technology: Power8System model 880 hardware and 64-bit reduced instruction set computer (RISC). Redundancy is built into every aspect of the claims processing computer systems, including primary and secondary processors for production, a processor for development and fully redundant disk storage systems. IBM system model 880 employs five (5) notable system concepts:

- *Hierarchy of microprocessors*. The system features a large number of microprocessors in addition to the main system processor. Each input/output device type on the system has its own microprocessors, enabling data to be written or read while the main processor executes another application.
- *Layered machine architecture*. This architecture insulates users from hardware characteristics and enables migration to new hardware technology without impacting the application programs.
- *Object orientation*. Everything that can be stored or retrieved on the machine is known as an object, and objects exist to make users independent of the internal structure of the machine.
- *Operating system*. The operating system is a single entity that fully integrates all the software components (e.g., relational database, communications, networking) needed to support claims processing.
- *Single-level storage*. Main storage and disk storage appear contiguous by implementing a device-independent addressing mechanism when an object is saved or restored on the system. This means extra storage can be added without affecting applications.

All systems are supported by uninterruptible power supply systems and diesel-driven power generators to ensure operations twenty-four/seven (24/7). Because it is predicated on scalability, the CVS system's

architecture is designed to accommodate significant increases in processing requirements. CVS maintains a multiplicity of technology systems, with primary functional areas of integrated claims adjudication, data warehousing and decision support. Each functional area requires specific technologies to address its particular systems requirements.

Data Warehousing

The EDW facilitates storage, linkage and rapid retrieval of prescription information and other health data and advanced tools, such as statistical analysis system software, which allows large amounts of data to be accessed faster than ever before. While traditional reporting gives the user a historical perspective, CVS provides intelligent reporting—reports with built-in interactive features that enable Passport to manipulate data with future projections and understand how to influence and shape those developments.

CVS's data warehousing technology employs a combination of proprietary and third-party-developed software systems in a client/server environment. This system provides access to ad hoc queries and reports (e.g., clinical, administrative, financial). Highlights of the CVS data warehousing systems include:

- More than 220,000 pharmacy entities with name, address and classification information
- Multiple therapeutic classification systems
- Online data resources that currently include nearly 16 million drug pricing records with historical information spanning more than seven (7) years
- Oracle, Teradata and Hadoop
- Proprietary enhancement data sets

Integrated Claims Adjudication

CVS's integrated retail and mail service claims adjudication network consists of a varied infrastructure composed mainly of WAN/LAN architectures and a drive for customer service. The WAN media involve dedicated point-to-point private lines services, multiprotocol label switching (MPLS) using both traditional T-1 and new flexible WAN ethernet to provide greater access to additional capacity and new features. The LAN services are one (1) Gb and ten (10) Gb ethernet on dedicated internal hardware to isolate adjudication service from other traffic types. This ensures the highest level of availability and performance for claims adjudication services.

Reporting

The CVS claims processing suite of systems offers a comprehensive set of automated reports and customizable reporting capabilities that provide the key financial and utilization statistics essential to analyzing and managing Passport's pharmacy benefit program.

Beacon Health Options

Beacon's FlexCare360 information management system is efficient and flexible in supporting the diverse services and capabilities necessary for Kentucky Medicaid. The system provides meaningful and user-friendly reports on quality, utilization, administration, provider performance, finance, and complaints and grievance

indicators, as well as the ability to pay claims timely, accurately and in accordance with HIPAA transaction requirements.

FlexCare360 is a modular system, with all the modules fully integrated and working in concert to provide users with high quality functions and data. It is comprised of six (6) main modules that have a system of checks and balances built into their programming to ensure reliable performance and accurate data reporting. The modules function as follows:

- The **member/customer service module** carries out customer service-related tasks and is the point of entry into the system for member information. Data such as member demographics, current and historical eligibility information, call history, complaints, grievances and appeals information resides in this module.
- The **plan management module** serves as the "benefits administrator." It stores and maintains all contract/plan-specific information, such as distinct plan definitions, specifications, level-of-care criteria, performance standards and fee structures.
- The **provider management module** affords users with network management functions and handles provider information, such as provider credentialing and specialties at the individual and provider organization levels. It works seamlessly with the plan management module to fully integrate items such as fee structures from various contracts.
- The **clinical management module** allows users to conduct case and UM activities. It is the point of entry and maintenance vehicle for case management information, such as treatment history, linkages with PCPs, external agency involvement, and service authorization data, treatment goals and outcomes. This module also maintains information regarding the utilization review management and service authorization activities. Additionally, it maintains the most up-to-date clinical symptoms and members' historical clinical data, along with integrated person-centric, level-of-care criteria, to enhance clinical decision-making.
- The **claims processing module** provides users with all claims processing and payment functions. It integrates data from the case management and provider management modules and allows for claims data entry to occur via various mediums, including manual as well as electronic entry. Tasks such as claims data validation and adjudication are performed in this module. In addition, this module handles all fund disbursement features, such as check printing and EFT.
- The **reporting/analytics** function of the overall FlexCare360 architecture provides all required and ad hoc reporting capabilities. FlexCare360's reporting architecture provides for a dedicated reporting data warehouse that is distinct from our transactional database. Transactional data is replicated to this data warehouse on a nightly basis, where data goes through an ETL process and is prepared at an atomic level for reporting and analysis. In addition, the data is aggregated and summarized on a weekly and monthly basis for the data marts and cubes in Microsoft business intelligence (BI) tools. From there, the data will be available for reporting and analysis via the Microsoft self-service portal.

The FlexCare360 system offers built-in checks and balances to ensure highly reliable performance and accurate claims processing. The system is designed to be highly configurable per the unique business needs of Passport, especially related to unique member identifiers; products offered to members and their related benefit limits; out-of-pocket maximums; and network participation by product and benefit limits.

Some examples of integrated system checks include:

- Eligibility data uploaded into FlexCare360 through data files received from Passport
- Coverage and benefits (maximums and minimums)
- Authorization requirements from the clinical management module
- Provider contracting status in relation to the procedure/revenue code being billed
- Validity of diagnosis codes, submitted NPI number and other data
- Sophisticated hierarchical adjudication logic

Claims Payment and eServices

Beacon uses FlexCare360 to adjudicate claims, and to make administrative requirements more efficient and user-friendly, the system also offers web portal capabilities. Through Beacon's eServices provider web portal or EDI gateway, electronic claims are uploaded and run through FlexCare360's claims adjudication engine for processing and entered into the claims processing module. The system accepts national 837I (UB-04 equivalent) and 837P (CMS 1500 equivalent) electronic as well as paper formats. Paper claims are either entered from scanned images upon the day of receipt or an 837 is created from the paper images submitted to FlexCare360. Once in the system, claims are run through FlexCare360's claims adjudication engine and tracked.

All claims information remains available in eServices for future reference, and users can view claim status here, regardless of how the claim was submitted. In most cases, claim status is posted on eServices within two (2) hours of electronic submission of the claim. Alternatively, providers can use EDI, which is also available twenty-four/seven (24/7) to providers and supports electronic submission of claim batches in HIPAA-compliant 837P and 837I formats.

Finally, while paper submission of claims is discouraged, providers can submit them manually by using the national standard format CMS 1500 or UB-04 claim form. Beacon has consolidated and streamlined operations by outsourcing paper claim processing to Fidelity National Information Services (FIS). By partnering with FIS, an industry-leading organization headquartered in Jacksonville, Florida, Beacon is able to improve the consistency, quality and timeliness of paper claims. All paper claims will be received and scanned by FIS, which will then generate an 837 to be sent to Beacon and accepted into FlexCare360 for adjudication.

FlexCare360 includes adjudication edits and logic for claims processing. It also contains standard code tables with HIPAA-compliant codes for diagnosis, procedures, decisions and place of service. During claims adjudication, the system uses these tables for adjudication processing, in turn validating industry standard codes. Specifically, FlexCare360 claims logic checks for erroneous payments, including duplicate payments, incompatibility between gender and procedure code-diagnosis edits, gender code-diagnosis edits and payments for services that do not correspond with the pricing schedule on file for the date of service.

Avēsis

Our dental and eye care benefits administration subcontractor, Avēsis, uses BridgeGate Health's technology solutions for all extract, transform and load (ETL) functions. We exchange data and files through the

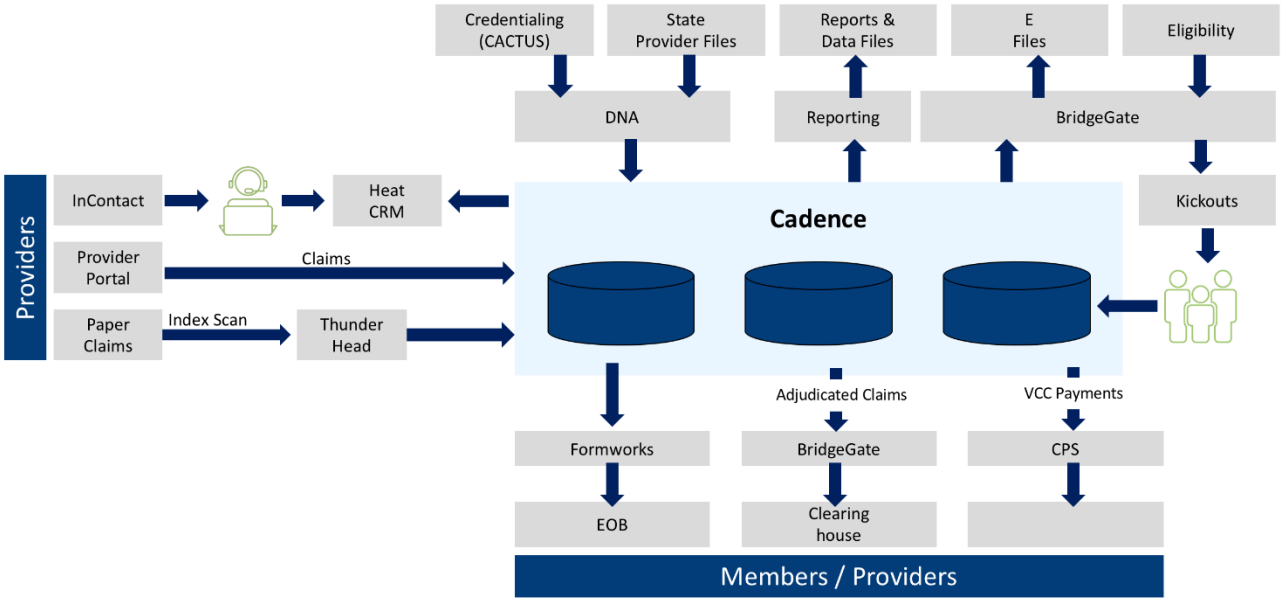
Axway/Secure file transfer protocol (FTP) system, where on both a scheduled and ad hoc basis, BridgeGate picks up and processes files using our custom business logic. BridgeGate also extracts data from the Cadence system and pushes it into Axway/Secure FTP systems, where it is then transferred into our system or set for pick-up by a team member. For data safety and reference purposes, all the data Avēsis receives from Passport is archived in an archive file server.

In addition, Avēsis has a provider web portal that uses secure interfaces to:

- Offer online (a) client eligibility verification, (b) secure claims submission, including batch uploads and batch viewing, (c) prior authorization request submission and (d) claims appeals, complete with electronic signature capabilities
- Offer an online credentialing process
- Offer an online process to obtain electronic remittance advice (graphical user interface (GUI), EDI or other)
- Include an electronic process to obtain EOP statements and other reports in PDF
- Provide information on submitting an appeal for recoupments due to eligibility changes

Finally, Avēsis uses a third-party software-as-a-service (SaaS) customer relationship management (CRM) solution called Heat from Ivanti. Heat interfaces with the claims system to support provider and member calls. The call center uses soft phones via InContact in a SaaS model as illustrated in **Exhibit C.6-16**.

Exhibit C.6-16: Avēsis Software-as-a-Service CRM Solution



Avēsis' MIS includes four (4) secure interfaces with external tools to provide comprehensive benefits administration as illustrated in **Exhibit C.6-17**.

Exhibit C.6-17: Avēsis Software-as-a-Service CRM Solution

Name/Unique Identifier	Type of Interconnection (e.g., SFTP, HTTPS, Web Services, etc.)	Interaction Details and Security Considerations
BridgeGate	SFTP	Commercial EDI transformation engine
InContact NICE	Hypertext Transfer Protocol Secure (HTTPS)	Member self-service through XML gateway (interactive voice response)
Thunderhead	HTTPS	Member/provider correspondence generation and printing
CPS	SFTP	Secure provider payment system

Avēsis is thoughtfully laying the groundwork to replace its claims system by 2024, one (1) year before the contract term is due to expire. Avēsis will work closely with the selected platform vendor and Passport to ensure there is no disruption to services through thorough planning and testing. As work continues in the current system, Avēsis is continually investing in staff and technology to provide the newest and most efficient administrative and reporting systems available.

Passport Management Information System Reporting Capabilities

Passport complies with all current DMS reporting requirements. We have reviewed all reporting requirements outlined in Section 37.0 of the Draft Medicaid Managed Care Contract and Appendices and are prepared to develop and submit all required reports in accordance with DMS specifications and timeframes, respectively, as outlined in **Attachment C.6-1_DMS Report Summary**. Passport fully supports the opportunity to collaborate with DMS and other contracted MCOs to establish report templates for a comprehensive reporting package that meets the needs of the Kentucky Medicaid Managed Care Program. A description of our robust reporting infrastructure is detailed below.

Data and Technical Solution to Meet Reporting Requirements

The Identifi EDW serves as the primary source of data to support operational, clinical, financial and ad hoc reporting in compliance with DMS, CMS, state and other federal agency requirements. The reporting stack leverages a wide range of data types, including clinical data, SDoH, partnerships with external data sources, EMRs, EHRs, third-party resources, administrative (payor) data and claims data. Our data validation process allows all external data loading (batch or real-time messages) of the aforementioned data types to go through a series of loading steps involving multiple staging tables of increasing complexity, moving clean data into the final data mart for reporting purposes and ensuring that the data elements required to produce the required reports are captured within our member-centric data warehouse.

The Identifi EDW allows for automated reporting and analytical needs as well as ad hoc report queries. The reporting subsystem uses a MicroStrategy backbone to provide robust reporting and business intelligence capabilities, including advanced visualization and dashboard options to present data in the most intuitive manner. The MicroStrategy semantic layer is connected to the Identifi EDW, allowing business intelligence users to access the data to create ad hoc reports, along with a complete palette of graphical widgets to present the data in the most understandable manner possible. With this pairing of EDW integration and visual insight capability, users can slice, dice, roll up and drill down with ease. The Identifi Platform's high configurability also allows for any necessary customization to respond to DMS-specific rules, workflows and data requirements, including prescribed reporting formats and frequencies as part of a comprehensive reporting package to address all requirements of Appendix D–Reporting Requirements and Reporting Deliverables.

In some instances, accountability for compiling specific DMS reports lies within a specific Passport operational area. In these cases, the Passport Compliance Department works closely with the functional area to ensure that reporting specifications are clearly defined and understood and that submission timeframes are met. Examples of these reports include NAIC annual financial statements, audit and internal control reports, marketing activities reports, QAPI status reports and audited HEDIS reports. As appropriate, functional report owners can use the Identifi Platform directly for a specific data set or to request more complex analytics and reporting through the analytics and reporting team. In both cases, the emphasis is on close collaboration, clear handoffs and quality control to realize the highest degree of efficiency and accuracy.

Passport can provide several report templates to DMS, CMS and other state and federal agencies at the appropriate submission cadence. It utilizes Identifi software's "canned" reporting, which is more operational in nature and focuses on daily routine monitoring, such as census, numbers of newly identified members and more; batch file requests that involve large data sets and claims-based activity summaries; and/or unique reports that result from database queries in an executable program language, typically statistical analysis system (SAS) and/or standardized query language (SQL) as further outlined in Section 27, Contractor Reporting Requirements.

Capabilities to Address a Broad Spectrum of Reporting

In addition to the above types of reporting templates and types of reporting platforms used, Passport is able to delineate its reports into qualitative (descriptive in nature, focused on processes and used to uncover trends), quantitative (ability to collect and report on measurable data to formulate facts and uncover patterns) or a combination of both.

For financial reporting, Passport's Financial Services department uses a combination of SAGE 50, Microsoft Excel and Microsoft Access to deliver reports to the financial management teams. The data for this reporting is generally sourced from our financial subsystem and the EDW, and as such, we are able to generate reports

to support cash management, funds flow, general ledger accounting, pro forma and financial statement generation, budget analysis and other financial requirements.

For population health and operational reporting, Passport's Data Analytics department leverages all claims, provider and eligibility data to support a robust reporting capability, including a suite of analytics services, embedded platform capabilities and configurable business intelligence and reporting tools to surface insights and drive improvement. As outlined above, our analytics capabilities are built on the MicroStrategy business intelligence platform. We geocode all members, providers and sites of care on the Identifi Platform, which allows for geospatial analytics, including maps of high-risk members and their attributed PCPs.

Identifi users can export reports and files in structured and unstructured formats, including Excel, PowerPoint, Word and/or PDFs, as well as configure existing formats to better meet their presentation needs. The reports within Identifi modules are designed to provide interactive, visual reports for optimal output within the module (e.g., targeted dashboards for providers in Identifi Practice) and can also be exported in structured and unstructured formats depending on the report.

Financial data elements corresponding to premium, capitation, incentives, etc., can also be stored in the data warehouse for use in reporting and analytics. The analytics team builds out financial summaries and generates reporting stacks that answer questions on plan profitability (MLR), trend components, drivers and opportunities. Reporting is flexible, so users can slice and dice the data by rate cell, provider hierarchies, service delivery area, etc., and highlight key cost and utilization metrics.

Quality as an Integral Component to Reporting

Passport places a strong emphasis on both quality and compliance. We never consider a report fully "canned" or completely automated. Each report that we produce, regardless if it is a one-time ad hoc report or a cadenced standing monthly report, is subjected to the same quality assurance (QA) check for completeness and accuracy, including data validation, reliability, comprehensiveness of the information requested, and format and presentation per DMS-defined requirements.

Passport's analytics and reporting team regularly reviews reports as part of a continuous improvement and quality control cycle to ensure that requirements are accurately reflected in the reports produced. While this process is essential for reports already delivered to DMS, it also provides an agile review cycle that allows for the modification and potential expansion of the numerous dashboards and preexisting data elements used for internal measurement purposes, operations and quality. Using the same workgroup that is developing comparable and sustainable reporting efforts across the MCOs to determine the most practical list of existing reports also ensures consistency in this effort, as well as contributes to version control. Passport uses these agreed upon and shared reports as a means to develop continuous quality improvements in response to trending, goal/objective performance and system change.

Existing processes are in place that will allow us to respond to new DMS requests and quickly utilize key operational metrics that are already built out. Any new report developments will adhere to the report development process steps described in Section 17 and will adhere to the same rigorous QA and control standards implemented across the entire reporting function.

Passport Management Information System Testing Infrastructure

The Identifi Platform is rigorously tested and validated to ensure compliance with DMS' testing and Kentucky Medicaid program requirements. The platform maintains separate environments as each release matures closer to production, with the development (DEV), QA, user acceptance testing (UAT) and production (PROD) environments helping to ensure that each change is thoroughly tested and validated prior to release. These tests help to ensure that system changes and updates do not adversely affect other systems, including those operated by Passport and its subcontractors, as well as that older programming still works with new changes.

Evolent continually updates and enhances the Identifi Platform, rigorously testing and validating updates prior to release to ensure compliance with Kentucky Medicaid program requirements. Passport's testing capabilities meet DMS' unique system requirements and include any and all required testing as directed by DMS. As previously noted, Passport was proud to serve as the Kentucky showcase MCO to CMS. We worked collaboratively with both DMS and contracted vendors to demonstrate our readiness to execute new Medicaid program requirements. Our comprehensive testing plan required 900 hours of partner integrated testing and dry run calls with DMS and contracted vendors to ensure adherence to required results and outcomes for critical program requirements, such as 834 consumption, plan mapping for the Kentucky HEALTH population and automated delivery.

Passport welcomes the opportunity to participate in joint application development sessions for system or policy changes upon request by DMS, ensuring that the system is enhanced and updated collaboratively and then tested to DMS requirements. The Identifi Platform also goes through several iterations of internal tests, including integration testing, end user capabilities testing and Identifi Platform security testing as further outlined below.

Identifi HPA

Identifi HPA software code is managed in Microsoft's Team Foundation Server, a product that provides source code management (either with Team Foundation Version Control or Git), reporting, requirements management, project management (for both agile software development and waterfall teams), automated builds, and testing and release management capabilities. It covers the entire module lifecycle and enables DevOps capabilities. The Support Team regularly applies fixes to all versions where a bug may exist, including the current "in-progress" branch.

The development team utilizes an agile-scrum software development life cycle (SDLC) and releases service packs every ten (10) weeks that include new system enhancements and bug fixes. The ten (10)-week releases consist of five (5) sprints, each two (2) weeks long. Each new enhancement is tested and validated by QA and the product owner at the end of each sprint. The fifth sprint in each release is identified as a "hardening" sprint, where no new code is introduced but full regression testing, manual and automated, is performed on the system.

After successful acceptance testing is completed, a release is promoted to P during well-communicated, nonpeak processing times between the 2:00 a.m. to 6:00 a.m. block.

All product patches and releases are handled by a central group for a repeatable process. Each release is numbered as **Rel. N.XX.YY**, where "N.XX" is the denotation of a master release, and ."YY" is the version number. The Identifi HPA system has a fully dedicated UAT environment for each release, and changes are typically provided within thirty (30) days of acceptance testing in that environment. Test times can vary based on the complexity of a particular release and the potential impact of the feature changes to Passport.

Comprehensive test beds have been created that can be modified to suit Passport's specific testing requirements. Business owners and internal stakeholders define the content of the test cases to be executed and subsequently help to define the expected results. Reusable test beds are comprised of applicable EDI files and data loads that execute specific test cases for Passport. Files from the reusable test beds can be used for all future testing efforts, which gives Passport a consistent testing approach.

The job scheduler function in the core payor system is leveraged to load the files from reusable test beds and run additional jobs to execute other required test cases (e.g., invoicing). Test cases that cannot be executed through a scheduled job will be executed with a manual test case. There are some instances where the software functionality must be tested through the UI: these test cases will also be executed during the manual test case execution. For example, the best and most realistic way to test the member profile functionality is through the UI, but the member used for this test could be loaded through an 834 eligibility load.

Negative test cases are also handled. A negative test case can be defined as ensuring the software gracefully handles unexpected input and data variables, for example, the system should not allow a user to save a "letter" in a date field. Some examples of eligibility and claims regression testing are shown below.

Non-automation eligibility regression testing:

- Load/processing
- ID card generation
- Invoicing (if applicable)
- Effectuation (if applicable)

Non-automation claims regression testing:

- Top 50 providers
- Top 50 procedure codes (by frequency)
- Top 50 procedure codes (by dollars)
- Top 20 diagnosis codes (by frequency)
- Top 20 revenue codes (by frequency)
- Top 20 revenue codes (by dollars)

Identifi Population Health Management (PHM)

The Identifi PHM system enhancement configuration is managed through environment-specific configurations and acts as a controlled change management process for deploying code to production. All deployments to the PROD environment are managed through an enterprise release management (ERM) process. Thorough post-production deployment validations check for module and data consistency.

Major releases of the Identifi PHM system go out on a quarterly basis (every ninety [90] days), on the last Sunday of a predetermined month. Each release contains a predetermined scope that is identified via feature tagging in Identifi's source code management system (including numbers showcasing the approved change and/or enhancement requests). Once the code has been completed, the build process is engineered such that only the specified features tagged as being in scope for a specific release are built in the module binaries for production release. This prevents code that has not been through the certification processes from being included in any production deployment. Our ERM team builds a feature checklist and sequence of events for each release to ensure that the change management process is followed. Only a very limited team of system administrators have rights to perform the actual deployment to production.

Changes and enhancements are approved by business owners based on UAT. Both QA analysts and business owners validate and approve production deployments prior to turning the new version over to end users. All source code is maintained and versioned in a code repository. When the code version has been approved in a QA environment, the code is moved to a UAT environment. Business users test in UAT, and once testing is complete and any issues are addressed, business sign-off is received. Once this version is deployed to production, business and IT users validate the changes in production. Upon the successful completion of validation, the system is made available for external users. Identifi users are notified in advance of any changes to the UI, and training is provided for any changes in the process/business workflow. This training may be provided in various forms (including job aids and webinars), depending on the scope of the update.

The Identifi module development team uses the GitHub code versioning tool to track and maintain all code versions, and the TeamCity module is used to build and deploy module code based on the business-approved version targeted for the production release as outlined above. The code version is displayed on the UI to ensure visibility of the deployed code version.

Identifi maintains separate environments as each release matures closer to production: DEV, QA, UAT and PROD environments ensure that each change or enhancement is validated prior to promotion. A combination of manual and automated regression testing helps to ensure the quality of each release. Our testing team maintains a library of more than 1,500 test cases in Microsoft's Test Manager to validate candidate releases. We also use Microsoft's Team Foundation Server to track the execution and status of all targeted test cases for each production release. Release notes are published with each release.

Each new release of the Identifi module is assessed by the web module security team so that new risks can be mitigated. For production checkout, a checklist is utilized to verify that all required functionality has been executed prior to QA sign-off. After successful testing and a production checkout is executed, the

enhancement and/or change release is promoted to production during the 1:00 a.m. to 6:00 a.m. block, to minimize impact to users.

Integration Testing

As outlined above, both components in the Identifi Platform (HPA and PHM) utilize multiple environments in the development cycle. The DEV, QA, UAT and PROD environments help to ensure that each new change or enhancement is validated prior to promotion. The separation of environments allows any issues or problems to be isolated and remediated before they are promoted to the next environment in the queue, potentially jeopardizing existing code and modules. In the event issues are discovered during the change management process, they are assessed by the agile-scrum SDLC team for business impact. The scrum team's product owner will communicate the issue to the impacted business units and negotiate a solution based on business needs and objectives, as well as any technical constraints that may exist. Once resolution is obtained, the code is reevaluated in its respective environment, and once it is confirmed to be issue-free, it is promoted to the next environment. All code must be fully validated and pass all exit criteria before it is promoted to the next environment in the queue.

Development teams use a combination of manual and automated regression testing to ensure the quality of each release. Regression testing is the process by which we test any changes and/or enhancements or updates to the Identifi Platform to ensure that system changes and updates do not adversely affect other systems, including those operated by Passport and its subcontractors, as well as that older programming still works with the new changes. Our testing team maintains a library of more than 1,500 test cases in Microsoft's Test Manager to validate candidate releases. Of these 1,500 test cases, roughly 600 are dedicated solely to regression testing, both manual and automatic. Our regression testing ensures that system changes do not impact system components that have not been changed for a release.

End User Capabilities Testing

The end user capabilities testing process starts with the design of Passport-specific workflows that reflect a spectrum of configurations and considerations. From this, a master test plan is formulated to include testing scope, scenarios, team and timeline. The scope and scenarios outline the Identifi module features, functionality and Passport-specific configuration to be tested. Based on these, a series of step-by-step scripts are written to conduct the testing, which is then performed by QA testers, the implementation team and a selection of Passport end users.

During testing, if issues are identified, they are logged in a formalized issue tracker by the implementation team, where they are further evaluated for triage to the appropriate area for resolution. If it is a technical issue, the Support Team is notified. If it is a configuration issue, the implementation team will address it. Testing results are communicated throughout the testing process in test plan design meetings, in-person testing sessions, test issue logs and master plan documentation. At the end of the testing session, a report on status is provided to everyone involved.

Identifi Platform Security Testing

The Identifi Platform has been developed in accordance with industry-standard secure coding guidelines as published by Open Web Module Security Project (OWASP). Throughout the SDLC, developers run module code through code analysis engines to discover any vulnerabilities that may have been introduced into the code base for immediate remediation, adhering to OWASP guidance for classification and remediation patterns to manage common web module vulnerabilities. Emphasis is placed on the OWASP Top 10 vulnerabilities, including SQL injection, XSS and parameter tampering/server-side input validation. The Identifi Web Module Security team ensures module code moved to the PROD environment is free of commonly encountered security vulnerabilities, using an assessment process consisting of static code analysis (SCA) and manual penetration testing (MPT). A third-party security firm performs MPTs annually and automated SCAs quarterly to ensure the platform is free of common vulnerabilities. The program tracks vulnerabilities and their mitigations across software releases to present a holistic view of the resilience of the module against various attack vectors as defined by OWASP. Vulnerability definitions are updated by the third-party security firm as new threats are discovered.

To mitigate new risks, the information security team regularly evaluates any impact to the risk profile of the MIS. We scan for vulnerabilities on all systems and perform remediation within thirty (30) days for any critical-, high- or medium-severity findings. Vulnerabilities discovered through our information security program are remediated based on severity and prioritized according to the common weakness enumeration (CWE) classification system. Identifi's most recent MPT was performed by GuidePoint Security between May and July 2019. There were no critical-, high- or medium-level severity findings post-remediation. Identifi's latest SCA test was conducted November 7, 2019, yielding a score of ninety-nine percent (99%). Passport will provide a copy of the module vulnerability assessments within fourteen (14) business days of its completion. In the event remediation needs to take place, Passport will provide a remediation plan that meets risk assignment and is in agreement with the Commonwealth.

Passport Management Information System Hardware and Architecture

Identifi Health Plan Hardware and System Architecture Specifications

The Identifi HPA system contains the modules that support core DMS subsystem requirements in a SaaS platform hosted in a high availability, secure, private data center. The hosting environment consists of two (2) distinct geo-redundant storage locations for our primary and disaster recovery sites. The disaster recovery site also hosts production support systems. In the event IT systems are down, breached, corrupted or otherwise subject to a disaster-related event, the Identifi HPA system will employ fully redundant systems to ensure failover capability both within our production site and at our disaster recovery site. A backup plan is in place to ensure that exact copies of electronic personal health information (ePHI) are retrievable. In the event of an outage that is expected to last more than twenty-four (24) hours, we implement our BC/DRP.

Module Architecture

Passport's Identifi HPA system is architected to scale horizontally and vertically across the infrastructure to handle ever-increasing system demands and store large amounts of data for data analysis as well as standard and ad hoc reporting. Tools like SolarWinds and other monitoring technology check the system for availability, performance and load. Identifi servers are Hyper-V virtual machines that allow us to scale the infrastructure if system load exceeds current peak system capacity. There is no upper limit on the number of users, lives or platform capacity.

The Identifi HPA system is built entirely on the Microsoft technology stack. All Microsoft SQL database servers are installed on servers running MS Windows server 2008 R2 or 2012, and they can be supported with either the MS SQL server 2008 R2 or the MS SQL server 2014 database platform. The Identifi HPA system employs a three (3)-tier architecture delivered via our SaaS platform as outlined in **Exhibit C.6-18**.

Exhibit C.6-18: Identifi Health Plan Administration Platform Architecture

Tier	Description
User Interface	The Identifi UI is hosted within Microsoft Internet Explorer and requires no module code to be installed for the user. The UI is built with Microsoft web technologies and JavaScript for client-side validations and improved usability. Although the UI can be navigated with a mouse, it can also be fully utilized without requiring a mouse to speed up the more intensive transactions.
Services Tier	The middle services tier is hosted on Microsoft IIS and is exposed via both RESTful and SOAP-based web service endpoints. The middle tier module code utilizes the .NET framework and is written in C#.
Database Tier	The backend database tier is deployed to Microsoft SQL server 208R2 and utilizes online transactional processing (OLTP) and online analytical processing (OLAP) components to provide all commonly used database objects, including stored procedures for complex database operations. It uses Microsoft SSIS for batch processing.

Hardware Requirements

Because the Identifi HPA system is a SaaS module, it does not need to be hosted on DMS and/or Passport premises. No specific hardware requirements have been defined, and no client-side downloads or other client modules must be installed at Passport to use the module. Recommendations for the minimum desktop requirements are a dual-core, two (2) GHz or higher CPU; four (4) Gb minimum of RAM (eight [8] Gb preferred for optimal performance, particularly if multiple other modules are also in use); 1366 x 768 or higher screen resolution; and a stable network connection (interruptions in network connectivity will cause errors in the Identifi module). The only desktop software necessary to use the full breadth and functionality of the Identifi PHM system is Internet Explorer. It is understood that, if requested, DMS shall be provided with log-in credentials to allow access to the claims and customer service systems on a read-only basis

during normal business hours as outlined in Section 15.4 of the Draft Medicaid Managed Care Contract and Appendices. All access will comply with HIPAA's minimum necessary standards and any other applicable Commonwealth, DMS or federal law.

Identifi Population Health Management (PHM) Hardware and Architecture

The Identifi PHM system that contains the modules supporting the core DMS subsystem requirements is a cloud-based SaaS platform hosted in Azure, a high availability, secure, cloud environment provided by Microsoft. The Azure environment is available in three (3) distinct geo-redundant storage locations for our primary site, our disaster recovery region and our backup storage region. In the event IT systems are down, breached, corrupted or otherwise subject to a disaster-related event, the Identifi EDW will employ fully redundant systems to ensure failover capability both within our EDW and at our disaster recovery site. A backup plan is in place to ensure that exact copies of ePHI are retrievable. In the event of an outage that is expected to last more than twenty-four (24) hours, we implement our BC/DRP, which will stand up a new environment in a nonaffected US region and attach the new environment to geo-redundant encrypted storage. In the event of a disaster, we can use automated tools such as Desired State Configuration to deploy our module to an unaffected region. Once deployed, we attach the Identifi module to the geo-redundant storage, test and release our module for public consumption. Predefined scripts are also used for rapid deployment of servers and restoration of data from an unaffected alternate data center.

Module Architecture

Passport's Identifi PHM system and its modules are architected to scale horizontally and vertically across the infrastructure to handle ever-increasing system demands and store large amounts of data for data analysis as well as standard and ad hoc reporting. Elasticsearch, Logstash, Kibana (ELK) stack log aggregation and monitoring technology check the system for availability, performance and load. Identifi servers are Azure Hyper-V virtual machines that allow us to scale the infrastructure if the system load exceeds current peak system capacity. There is no upper limit on number of users, lives or platform capacity.

The Identifi HPA system is built entirely on the Microsoft technology stack. All Microsoft SQL database servers are installed on servers running MS Windows server 2008 R2 or 2012, and they can be supported with either the MS SQL server 2008 R2 or the MS SQL server 2014 database platform. Identifi HPA contains more than 800 tables, 3,300 procedures, 160 functions and 100 automated jobs. The Identifi Population Management System components employ a three (3)-tier architecture delivered via our SaaS platform as outlined in **Exhibit C.6-19.**

Exhibit C.6-19: Identifi Platform Architecture

Tier	Description
User Interface	The Identifi UI is hosted in supported browsers. The UI is built with Bootstrap and Angular and adheres to the single-page module design pattern.

Tier	Description
Services Tier	The middle services tier is hosted on Microsoft IIS and is exposed via RESTful web service endpoints. The middle tier module code utilizes the .NET framework and is written in C#. The middle tier is completely stateless.
Database Tier	The backend database tier is deployed to Microsoft SQL Server 2012 and utilizes OLTP and OLAP components to provide all commonly used database objects, including stored procedures for complex database operations and Microsoft SSIS.

More complex reports are delivered using the Identifi analytics and reporting module, which is architected on the MicroStrategy BI layer. Data is accessed via stored procedures or dynamic SQL.

Hardware Requirements

Because the Identifi PHM system is a SaaS module, it does not need to be hosted on DMS and/or Passport premises. No specific hardware requirements have been defined, and no client-side downloads or other client modules must be installed to use the module. Recommendations for the minimum desktop requirements are a dual-core two (2) GHz or higher CPU; four (4) Gb minimum of RAM (eight [8] Gb preferred for optimal performance, particularly if multiple other modules are also in use); 1366 x 768 or higher screen resolution; and a stable network connection (interruptions in network connectivity will cause errors in the Identifi module). The only desktop software necessary to use the full breadth and functionality of the Identifi PHM system is a web browser. Identifi currently supports Google Chrome (current version plus the two [2] previous major versions); Firefox (current version plus the two [2] previous major versions) and Internet Explorer v11. Chrome is preferred for optimal module performance. It is understood that, if requested, DMS shall be provided with log-in credentials to allow access to the claims and customer service systems on a read-only basis during normal business hours as outlined in Section 15.4 of the Draft Medicaid Managed Care Contract and Appendices. All access will comply with HIPAA's minimum necessary standards and any other applicable Commonwealth, DMS or federal law.

General Network Connectivity Requirements

During the data readiness/onboarding phase, a secure HIPAA-compliant EDI is used to exchange the administrative (payer), clinical, provider and specific data feeds needed to drive the Kentucky Medicaid Managed Care program on the Identifi Platform. As a part of the current implementation, Passport has facilitated the data exchanges required to ensure we have attained successful and secure connectivity and the appropriate DMS, administrative (payer), clinical, provider and self-submitted data domains flow into our EDW for operational performance and use.

Passport recognizes that DMS requires bi-directional and/or unit-directional electronic data submission for certain information in commercially acceptable formats to facilitate and expedite eligibility validation, capitation reconciliation, fee-for-service reimbursement and encounter submissions specific to the Kentucky Medicaid Managed Care Program as outlined in Section 15.3 of the Draft Medicaid Managed Care Contract and Appendices. Passport has existing business continuity policies to ensure that structured redundancy around electronic data submissions is maintained. Our EDW employs fully redundant systems to ensure

failover capability both within the data center and at the disaster recovery site in the event IT systems are down, breached, corrupted or otherwise subject to a disaster-related event. A data backup plan is in place to ensure that exact copies of ePHI are retrievable as well:

- System snapshots are backed up and stored in an encrypted geo-redundant storage container
- Database logs and backups are also stored in an encrypted geo-redundant storage container
- Customer files transmitted via EDI are copied on separate encrypted storage located in a different region

The EDW supports industry standard (including ANSI-compliant) health care data and message formats and standards, including HL7 (v2 and v3), HL7 FHIR, CCDA, National Council for Prescription Drug Programs (NCPDP), X12, IHE, DICOM, XML, binary, delimited and legacy formats. It also supports the use of transmission control protocol (TCP) over virtual private network (VPN), FTP, SFTP, FTPS and HTTPS protocols for processing files. SFTP network connectivity is supported for data exchange; we also support encrypted transmission of files via encryption over VPN and secure web services for data exchange. These HIPAA-compliant EDIs allow us to provide information in accordance with the format and file specifications for all data elements as specified by DMS in Appendix G–Management Information Systems Requirements. It also transmits all data directly to DMS and in a format specified in accordance with 42 C.F.R. 438.

Passport MIS Configuration Management

Custom Configurations to the Identifi Platform

The Identifi Platform's configurability supports a faster and more agile implementation and provides flexibility in adjusting to continue to meet the requirements of Kentucky's Medicaid Managed Care Program, including the ability to quickly address any current and upcoming DMS waivers. Through system configurations, we can accomplish modifications such as operational reporting layouts to conform to contract-specified requirements; reporting data extraction methods/coding; stratification/rules configuration specific to target populations; fee schedules, provider and benefit plan configurations; and UM requirements to support specific Kentucky Medicaid requirements. As configurations and possible customization requirements emerge (if applicable), any new scope including business, platform and user-driven requirements will be defined to meet DMS and Passport's unique environment and needs.

DMS-Directed Modifications, Changes & Enhancements

Any major system changes or implementations that Passport or DMS require or that are anticipated as part of the platform's product roadmap are communicated to the appropriate Passport and DMS staff via email at least ten (10) days prior to the planned change or implementation (including any DMS-directed waivers and any changes relating to Evolent and subcontractors) as outlined in Section 15.1 of the Draft Medicaid Managed Care Contract and Appendices. It is understood that all major system changes are subject to DMS desk reviews and onsite reviews of our facilities as necessary to test readiness and functionality prior to

implementation. Passport will also participate in workgroups and regular calls related to the MIS platform, as convened by DMS.

It is Passport's understanding that DMS will communicate required Medicaid Managed Care Program changes directly to Passport, including but not limited to established expectations, processes and timelines for DMS-directed modifications, changes and enhancements. Passport will then work with applicable subcontractors to ensure timely completion of the changes. A dedicated team of module and engineering, IT, and data developers and analysts (including technical and project managers) will be formed. This collective team will be present in meetings and will partner directly with DMS on solutioning and implementing the requested changes or enhancements. Our team will leverage existing DMS-dictated project tracking systems that align with our own internal project portfolio management PPM and development tracking solutions, ensuring both parties are synchronized during the change/enhancement process. Managing an MIS is continuous, and the change control process below will be utilized to manage all modifications, changes and enhancements throughout the life cycle of the contract in a streamlined and agile manner as directed by DMS or Passport.

We will use an internal change management process designed to provide a single point of engagement for the intake, communication, management and resolution of any modification requests, ensuring that relevant parties are notified of status/progress throughout the entire change process and life of the contract. Requested changes adhere to our module security program, which encompasses our SDLC, to ensure that all publicly-facing Identifi Platform module components are free of commonly found security vulnerabilities and that all module deployments follow the change management process. This ensures that changes to the platform are introduced in a controlled and coordinated manner, reducing the possibility that unnecessary changes (or worse, faults) will be introduced. The goal of this process is to minimize disruption to our products, member and provider communities, reduce back-out activities and utilize our resources cost-effectively when implementing requested changes.

Identifi change requests go through a documented approval, testing and validation process that includes module code management, module QA, module UAT, module security vulnerability assessments and ultimately module production deployment that will align with required DMS project tracking system protocols. These phases document artifacts for Passport and DMS, including what aspects of the MIS will change, dates of agreed upon and planned implementation, how these changes will affect the provider and member communities, if applicable, and what communication channels will be used to notify these communities. They also include a detailed implementation plan and schedule of proposed changes, and contingency plans in the event of downtime or substantial non-performance of the MIS.

DMS-directed modifications and enhancements to any existing systems are managed and completed within a collaborative and mutually agreed upon timetable within DMS-specified guidelines in accordance with scope and required level of effort. Changes that fall within the Identifi HPA system include changes to eligibility and enrollment; benefits management for covered services; member and provider services; COB; EDI/clearinghouse interface and claims management; and member and provider portals. Changes that fall

within the Identifi PHM system include changes to provider and network management; CM workflows; reporting; analytics and business intelligence; and UM workflows.

Changes requested by Passport or DMS will follow SDLC and change management processes that account for, but are not limited to, SDLC and change management policies, our Identifi HPA and PHM system change control processes, system integration and end user testing, module code management, QA, UAT, security vulnerability assessments, off-cycle releases, procedural back-out policies and our standard release schedule.

As part of the response, include information about the following:

C.6.i. Required interfaces, how the system will share and receive information with the Department, how the Vendor's system will use files provided by the Department, Subcontractors, providers, and other supporting entities.

Required Interfaces

Passport has successfully and securely exchanged data with DMS, its subcontractors and business partners for twenty-two (22) years. Secure interfaces are of the utmost importance and we ensure our processes are consistent with industry best practices and the latest technology. **Exhibit C.6-20** summarizes current DMS interface transactions.

Exhibit C.6-20: Passport Health Plan Data Exchanges with DMS

Inbound/Outbound	Description	Frequency
Inbound	*820 Capitation Payment*	Monthly
Inbound	*834 file Benefit Enrollment Daily*	Daily
Inbound	*834 file Benefit Enrollment Recon*	Twice a month
Inbound	*834 file Benefit Enrollment Monthly*	Monthly
Inbound	*TPL Resource Daily*	Daily
Inbound	*TPL Resource Recon*	Twice a month
Inbound	*TPL Resource Monthly*	Monthly
Inbound	*TPL Carrier*	Monthly
Inbound	*Prior Authorization Medical*	Daily
Inbound	*Prior Authorization Pharmacy*	Daily
Inbound	*Provider Master extract*	Daily
Inbound	*Twenty-four (24)-Month Inactivity and Termination Report*	Quarterly

Inbound/Outbound	Description	Frequency
Inbound	*License Renewal Report*	Weekly
Inbound	*MCO Provider Member Auto-Load Error Report*	Daily or as delivered
Inbound	*Annual Disclosure of Ownership Notice Report*	Weekly
Inbound	*Annual Disclosure of Ownership Shutdown Report*	Weekly
Inbound	*277U Claims*	Daily
Inbound	*277UESC Encounters (description of 277U errors)*	Daily
Inbound	*277U Pharmacy*	Daily
Inbound	*NCPDP Acknowledgement (ACK)*	Daily
Inbound	*999 ACK*	Daily
Outbound	*Encounters (837P/I/D, NCPDP)*	Weekly
Outbound	*TPL Resource Data Match*	Monthly
Outbound	*Provider Network File*	Monthly
Outbound	*Cost Share File*	Daily
Outbound	*Member Level of Care File*	Daily
Outbound	*Member Level of Care Error File*	Daily
Outbound	*MCO Member File (daily)*	Daily
Outbound	*MCO Member File (monthly)*	Monthly
Inbound	*MCO Member File daily error file*	Daily
Inbound	*MCO Member File Monthly recon error file*	Monthly
Inbound	*Policies Added/Updated from TPL Resource Data Match*	Monthly
Inbound	*Policies Added/Updated Error Report from TPL Resource Data Match*	Monthly
Inbound	*Policies Added/Updated Member Mismatch Report from TPL Resource Data Match*	Monthly
Inbound	*Encounter Submission Statistics Detail Report*	Weekly
Inbound	*Encounter Submission Statistics Summary Report*	Weekly
Inbound	*Provider License Shutdown Report*	Weekly
Inbound	*Managed Care Lock-in Report*	Monthly
Inbound	*Consolidated Omnibus Budget Reconciliation Act (COBRA) files Part A & Part B*	Daily
Outbound	*MCO Member Count*	Weekly

Inbound/Outbound	Description	Frequency
Inbound	*Member Mismatch Report*	Weekly
Outbound	*Member Mismatch Report-MCO Response*	Weekly
Outbound	*Capitation Payment Request*	Monthly
Inbound	*230 Report Response*	Monthly
Outbound	*Capitation Adjustments Request*	Monthly
Inbound	*250 Report Response*	Monthly

Sharing and Receiving Information

We focus on stringent protocols and support multiple HIPAA compliant file formats—and require the same from our trading partners. Data exchanges between DMS, providers and vendors occur through dedicated point-to-point connectivity or secure virtual private networks or encrypted secure sockets layer (SSL) connections over the Internet.

Passport uses the MoveIT DMZ and MoveIT Central products to perform job scheduling, automation, status monitoring, exception alerting, logging and reporting of secure file transfers inside the organization and between other organizations. This software suite allows for extensive file transfer automation capabilities to support business functions twenty-four (24) hours a day, seven (7) days a week.

The architecture of this solution is highly resilient and offers robust control. The current integration model we support is fully scalable to accommodate whatever integration is required, and our repository of jobs can scale to meet future growth. We are proud to have served as the Kentucky HEALTH showcase MCO to CMS–working collaboratively with both DMS and contract vendors to demonstrate our readiness to execute new Medicaid program requirements, which includes new interfaces. For example, Passport developed solutions and frameworks to consume new program indicators in the eight hundred thirty-four (834) to identify member's cost share and program status for Kentucky HEALTH as well as automated delivery and monitoring for required data shares/extracts to share eligibility information and trigger ID cards and welcome kits.

All interfaces are well documented and include defined data elements, formats and file layouts including input and output job schedules with backend reporting and data reconciliation. Passport routinely self-audits performance, security and operational controls and participates in DMS and regulatory audit processes annually. Requests for access or documentation are processed within prescribed timeframes and any subsequent follow-up or suggested actions will be agreed upon and executed.

Using Data

DMS interfaces support key health plan processes and include loading of eligibility into all subsystems to enable unimpeded member access to health services; fulfillment of member enrollment materials, including ID cards; member PCP assignment, as appropriate; utilization management work activity; and provision of care management services for members. Data from DMS is also used to perform reconciliation of DMS payment to Passport, to correct erred encounters as well as aid in the submission of encounters (e.g., Provider Extract File provides KY Medicaid ID numbers) and supplement member TPL information to ensure KY Medicaid/Passport is the payor of last resort

Many intersystem interfaces provide authorization, lock-in program eligibility, cost share, referrals, county codes, level of care, cost avoidance data, and more to comply with all DMS requirements, including reporting, to support Passport clinical and operational activities. For example, lock-in program eligibility data is used to supplement reporting on these members. Please see **Exhibits C.6-21** and **Exhibit C.6-22** for key subcontractor and business partner EDI transactions, and how this data supports Passport operations and Kentucky Medicaid program requirements.

Exhibit C.6-21: Key Inbound Subcontractor and Business Partner EDI Transactions to Passport

Transaction/ Description	Sender	Frequency	Health Plan Activity
Encounter	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Encounter submission to DMS
Encounter Response	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Corrected encounter submission to DMS
Claim	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Care management
835	Provider Payment Vendor	Daily	Provider payment
837	Clearinghouse	Daily	Claim processing

Exhibit C.6-22: Key Outbound EDI Transactions to Subcontractors and Business Partners

Transaction/ Description	Recipient	Frequency	Health Plan Activity
Eligibility	BH, Vision, Dental and Pharmacy Subcontractors	Daily	Provision of health care services
Encounter Response	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Corrected encounter submission to DMS

Transaction/ Description	Recipient	Frequency	Health Plan Activity
COB	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Claim processing
TPL	BH, Vision, Dental and Pharmacy Subcontractors	Weekly	Claim processing
Provider	Provider Directory	Daily	Provider directory updates
ID Card	ID Card Vendor	Daily	ID Card production and member enrollment materials

C.6.ii. Capability to store and use large amounts of data, to support data analyses, and to create standard and ad hoc reports.

The Identifi HPA reporting SAS infrastructure consists of eight (8) physical server nodes, providing redundant analytical capacity. Each server has a private, five (5) TB, all-solid state drive (SSD) working space on a dedicated EMC Unity 550 array. Each node also connects via redundant Strongest devices to a shared eighty-five (85) TB storage environment hosted on a NetApp all-SSD solution. There is capacity available on the NetApp solution to double the SAS shared storage, if required. The environment resides in a Tier III data center with redundant one (1) GB circuits providing connectivity to both the Internet and MPLS. The environment is kept in locked cages within a private pod in a co-location facility.

Passport's MIS PHM component and its modules is architected so that the solution can scale horizontally and vertically across the infrastructure to handle ever-increasing system demands and store large amounts of data for data analysis and standard and ad hoc reporting. ELK stack log aggregation and monitoring technology monitor the system for availability, performance and load. Identifi servers are Azure Hyper-V virtual machines that allow us to scale the infrastructure if the system load exceeds current peak system capacity. There are no upper limits on the numbers of users or lives, or platform capacity. In fact, Passport has recently made significant investment in the technical architecture underlying the application platform to enhance stability, improve performance, and provide for data, usage growth and expansion. Within the past nine (9) months, Passport has installed a new NetApp storage platform, adding over one hundred twenty-four (124) TB of SSD storage in the production data center, added six (6) additional servers (close to three [3] TB of memory), and expanded the production web server environments.

The Identifi PHM platform uses a combination of Azure Cloud infrastructure and Hadoop Big Data capabilities to create a platform with elastic scaling capabilities. The Identifi Platform has been tested to onboard data in the data warehouse from multiple sources and is capable of processing eligibility data related to 600,000 lives, 33 million historical and current medical claims datasets, and 8 million historical and current pharmacy claims datasets. The data warehouse is also able to process clinical data in real time

and in batch-processing mode, handling 22 million, 8 million and 5 million ADT, lab and CCD transactions per month, respectively. The Identifi Platform also runs monthly measure compliance calculations on members based on new data received—processing 6.5 million members every month to measure compliance across 1,400 measures. The Identifi Population Health applications undergo performance and stress testing with every release of the application. This best practice has enabled the Identifi applications to support average daily transaction volume of 1.14 million transactions, peak daily transaction volume of 1.9 million, and total monthly transaction volume of 29.6 million, with an average transaction response time of 0.176 seconds.

As previously detailed, the Identifi EDW serves as the primary source of data to support operational, financial and ad hoc reporting in compliance with DMS, CMS, state and other federal agency requirements. The reporting stack leverages a wide range of data types that converge in the Identifi EDW for operational, financial and ad hoc reporting, including: clinical data, SDoH, partnerships with external data sources, EMRs, EHRs, third-party resources, administrative (payer) data, claims data and EDIs. Our Identifi EDW allows for automated reporting and analytical needs as well as ad hoc report queries.

Passport employs a rigorous process facilitating the intake of requests for standard and ad hoc reporting. A tight cross-collaboration and clear hand-offs between functional groups ensures a seamless and efficient approach to receiving requirements, review and assessment of the requirements, and report development as well as subsequent testing and production (see Section C.27 for detailed Passport Report Development Process). Standard reports, usually operations-focused, are defined by the ability to reproduce the report, faithfully modifying just a few input variables as needed, for example, time period and membership. These reports utilize the Identifi Platform and analytics functions to produce ad hoc or repeat instances of "canned" reports. More complex ad hoc requests, requiring a unique database query in an executable program language, for example, SAS and/or SQL, and analytics are received through the Passport Compliance Team, prioritized and then produced, in a process including several QA cycles to ensure accuracy of the ad hoc report. The resulting report product typically is presented in widely accepted office software platforms, such as Microsoft PowerPoint, Excel, Word and/or PDF. More detailed information on reporting capabilities is provided above in our response to 6a, *Reporting*.

C.6.iii. Extent to which these systems are currently implemented and integrated with other systems, internal and external, and the Vendor's approach for assuring systems that are not fully implemented and integrated will be ready to begin operations on required timeframes.

The Passport MIS, along with its corresponding subsystems and modules, is fully operational, implemented and integrates with all required internal and external systems to support the new 2021 contract. The MIS is currently configured to meet or exceed all Kentucky Medicaid Managed Care Program subsystem requirements and is functioning within the guidelines and specifications of the Commonwealth, including all required interfaces. This ensures continuity, as reimplementation of systems and interfaces is not required with Passport.

One of the keys to continually improving the care provided to our members involves changes to current systems and interfaces. Whether the changes are based on new methods of care or upcoming DMS waivers, the Identifi Platform's vast configurability supports a faster and nimbler implementation and provides flexibility in adjusting to continue to meet the requirements of Kentucky's Medicaid Managed Care program. When a larger system or programmatic change is called for, Passport's development team utilizes the Agile-Scrum Software Development Lifecycle, providing rapid development and deployment, while ensuring a problem-free implementation.

Passport System Readiness for Commonwealth Initiatives

As an example, in preparation for the Kentucky HEALTH initiative, Passport was the only MCO selected by DMS to demonstrate readiness, making all necessary system changes to meet requirements.

Examples of the systemic solutions and frameworks that Passport developed in preparation for Kentucky HEALTH are summarized in **Exhibit C.6-23**.

Exhibit C.6-23: Solutions and Frameworks

Framework or Solution	Solution Details
834 Consumption	Passport updated this process to identify the following Kentucky HEALTH indicators: • Coverage type, Medically Frail, deductible, suspension and penalty reasons, community engagement exemption reasons and hours, fast track, and monetary amount (premium amount) • Considers copay and cost share met and program status codes • Features fast file ingestion with deep monitoring (as noted in Section C.26–Enrollee Eligibility, Enrollment and Disenrollment) *Quality Assurance oversees the consumption of the files to support up-to-date, accurate eligibility status.*
Corresponding Plan Mapping for Kentucky HEALTH Populations	This process will support the intended benefit module for varying eligibility categories relative to cost-sharing requirements and layers into the plan assignment approach (*as detailed in Section C.26 and the attached Plan Product Scenarios Kentucky Health (KYH)*). Passport has created a plan mapping structure including a consistent indicator in its naming convention for easy identification of cost share status. *This indicator has been shown to be helpful to providers.*
Automated Delivery and Monitoring	This solution was applied to: • Share required data extracts with eligibility information • Trigger ID cards, deductible statements and invoice generation • Send welcome kits

Framework or Solution	Solution Details
New Member Portal Launch–"MyPassportPlan"	Passport's portal features the following information: • Deductible tracking • Premium payment status • Plan type • Federal Poverty Level (FPL) level • Cost share (copay or premium) • Community engagement requirements • My Rewards status Links are also included to our payment vendor CareEnroll for any payment functionality and detailed balance information.
Provider Portal Changes	This update features: • New medically frail attestation • Mirroring the member-level detail described above for the member portal

C.6.b. Provide a description for and list of potential risks and mitigation strategies for implementing new information systems and changes to existing systems to support the Kentucky Medicaid managed care program.

Passport strives to continuously improve information technology systems in support of its mission to improve the health and quality of life of its members. As a long-standing incumbent for the Commonwealth, we do not expect to implement new information systems during the length of the contract. However, we anticipate enhancements or modifications to the existing MIS will occur routinely to continue to bring the latest technology and advancements to bear. While our system has the needed capabilities and functionality to operate the Kentucky Medicaid Managed Care Program, we do anticipate minor configurations and modifications in the event, for example, that new lines of business are added or when there are new program and operational requirements from the Commonwealth. These include, but are not limited to, new operational reporting layouts; reporting data extraction methods/coding; stratification/rules configuration specific for the target populations; fee schedule updates; provider and benefit plan configurations; and UM requirements. Our strategies to mitigate potential risks for any change, enhancements and/or modifications to the system are implemented carefully according to a comprehensive change control process. If requested by DMS, Passport will participate in joint application development sessions for system or policy changes.

Potential Risk Factors with Implementation of New Systems/Changes to Existing Systems/Mitigation Strategies

As previously noted, in 2016, Passport embarked upon an effort to transform its business model, system infrastructure and employee talent to better serve its members. We proudly transitioned to the Identifi Platform, an MIS designed to support health plan administration via Identifi HPA and population health via the Identifi PHM system.

Our Passport leadership acknowledged that business transformation was necessary to make our operations, including MIS, more scalable and agile to improve the quality of care. Today, Passport operates a robust MIS. The MIS and its subsystems are fully operational, already configured to meet the needs of DMS, and are currently functioning within the guidelines and specifications of the Commonwealth.

System implementations and changes often have many interdependent components and modifications in one component can easily affect another function. Potential risks for any system implementation or changes to existing systems include tight timeframes. For proper configuration, testing, deployment and change control management of any adjustments, sufficient time is needed. Mitigation of this risk includes proactive and routine communication with the Department on anticipated changes with as much runway as possible.

Unclear requirements also present a risk to new implementations and changes. In such a complex system, detailed and comprehensive requirements are necessary. Incomplete or unclear requirements can jeopardize both the project plan and expected results. Risk mitigation includes detailed requirement gathering with internal and external stakeholders, and sufficient time to allow for iterative review as well as sign-off by stakeholders.

Control Processes in Place to Mitigate Risk with System Enhancements and Modifications

The Passport MIS is a highly configurable SaaS platform. Any configurations to the MIS, rules, workflows and data are managed. Configurability supports a faster and more agile process and allows the ability to adjust to continue to meet the requirements of the Commonwealth and to optimize the performance of our systems to better support our work to improve the health and quality of life of our members.

Enhancement and change requests go through a documented approval, testing and validation process. Upon receipt of any such modification requests (from the Commonwealth or internally), an entry is created within our centralized intake form for change management documentation. Each request will receive a unique identifier that can be noted for later retrieval purposes and to track the change request throughout the entire change management process from request to production. Enhancement and change requests are then reviewed by the Cross-Functional Review Board to analyze the high-level impact of the change request relative to other contractual commitments, our product roadmap, and resource availability to deliver on the request and communicate a plan for including the change in a scheduled system update. The Cross-Functional Review Board schedules commitments based on capacity and cross-client priorities, escalating to an outside Executive Operations team as needed. This ensures a collaborative and mutually agreed-upon timetable within DMS specified guidelines in accordance with scope and required level of effort (LOE) is achieved. The team provides leadership visibility and oversight for macro-level client communications. Further details of custom configurations to the Identifi Platform and DMS-directed modifications, changes and enhancements is outlined above in the Custom Configurations to The Identifi Platform & DMS-Directed Modifications, Changes & Enhancements section of the response to Question C.6.a.

Software Development Cycle

Enhancements and changes include the following procedural steps as further outlined above in the Custom Configurations to The Identifi Platform & DMS-Directed Modifications, Changes & Enhancements section of the response to Question C.6.a: (1) module code management, (2) module QA, (3) module UAT, (4) module security vulnerability assessments, and ultimately, (5) module PROD deployment.

Communications Process for Systems Updates

Effective communications are critical to the change control process. In addition to the communication referenced throughout the process descriptions above, additional communications protocols are included. Identifi Platform users are notified via an e-mail communication from the Identifi Support and Release Management team in advance of patch and fix deployments and change enhancements. Planned downtime includes MIS updates, including major releases and hot fixes, and is typically done during our maintenance window. Unplanned downtime could be the result of an Internet outage or another disruptive event. In the case of planned downtime, the MIS Support Team sends an e-mail communication to all Identifi Platform users about one (1) week prior to the downtime (or in the case of a hot fix, as soon as we know that we need to take the system down for maintenance). The Support Team sends another e-mail communication before the system goes down, and follows up with an e-mail communication to users when the system is again available. With regard to unplanned downtime, the Support Team will communicate with all users as soon as possible. We will provide updates on expected return to service, and a final e-mail communication when the system is back up, as well as some explanation of the root cause of the outage.

MIS users have access to a system that is free of recurring errors or failures on the backend. We proactively monitor the platform for errors and resolve any issues as part of the SDLC within the change control process. Each software release will contain several iterations, known as sprints, to complete all deliverables identified for the release. The MIS has been developed in accordance with industry-standard secure coding guidelines as published by OWASP. Throughout the SDLC, developers run module code through a static code analysis engine to discover any vulnerabilities which may have been introduced into the code base for immediate remediation. In the event any issues are discovered during the change management process, they are assessed within the aforementioned team for business impact where they will communicate the issue to impacted business units and negotiate a solution based upon business needs and objectives, as well as any technical constraints which may exist. These issues are also communicated to the Commonwealth.

Internal Testing Processes

As outlined in the Testing section of the response to Question C.6.a.viii, we utilize formal integration testing, end-user capabilities testing, security testing and full manual and automated regression testing as part of our change control process to ensure that changes to the product or system are introduced in a controlled and coordinated manner. It reduces the possibility that unnecessary changes will be introduced to a system without forethought, introducing faults into the system or undoing changes made by other users of the software. The ultimate goal of the change control process is to minimize disruption to our products, reduce back-out activities and ensure cost-effective utilization of resources involved in implementing

change. Coupled with previous quality assurance and testing activities, enhancements and changes are thoroughly tested and validated to ensure the proper code is released to production. The most important testing safety net is our combination of manual and automated regression testing, by which we test any changes and/or enhancements or updates to the Identifi Platform to ensure that system changes/updates do not adversely affect other systems, including systems operated by the client and subcontractors' systems, as well as ensuring that older programming still works with the new changes. Our regression testing ensures that system changes do not impact system components that have not been changed for a release.

Emergency ("Off-Cycle") Changes

There is an established process by which emergency changes are requested. Emergency (or "off-cycle") changes still go through the same process as routine changes (documentation of requirements, testing and sign off, etc.). The only difference between changes that are made through the normal change management process and the emergency change management process is that items that are requested as emergency changes are evaluated to ensure they meet emergency change requirements (e.g., there is an impact on member care) and there is a strong case to be made for why the change should be made outside of the regular deployment cycle.

Procedural Code Back-Out Process

In the event a change does not test successfully after production implementation and a fall-forward remediation is not feasible, the release-management back-out procedure will be implemented. The back-out procedure consists of the following:

1. Restoring the database backup that was captured as the first step of the deployment.
2. Redeploying the previous production version of the code from TeamCity.
3. QA certification of the previous production version, indicating a successful back-out.
4. Site is made available for use on the previous version.

These processes mitigate risks arising from any changes, enhancements and/or modifications to the systems to ensure positive, expected results are achieved, commitments made to the Commonwealth are realized, and both members and providers are not adversely affected.

C.6.c. Describe the Vendor's current and planned use and support of new and existing technology in health information exchange (HIE), electronic health records (EHR), and personal health records (PHR)

Maintaining Existing Standards While Striving for Continued Innovation

Passport remains committed to the use and support of new and existing technologies for HIE, EHR and PHR for the Commonwealth and to our mission for its members and providers.

Passport has been working collaboratively with DMS since 2011 to contribute detailed information on its members to the Kentucky Health Information Exchange (KHIE). We met with the deputy executive director and KHIE staff in the fall of 2019 to work together on establishing a data exchange between Passport and KHIE. When KHIE systems are ready, we will be capable of a sending a continuous feed of Passport data to the KHIE system.

Passport has chosen to implement KHIE using a secure web service that serves CCDs to the KHIE. We have developed a standard-based C132 Continuity of Care document that retrieves clinical information in real time with response times of less than three (3) seconds. The transaction for requesting and responding meets all KHIE requirements. It uses web services (WS) security over an unsecure Hypertext Transfer Protocol (HTTP) connection following the KHIE web services description language (WSDL) with an X.509 certificate, as per KHIE specifications, and responds to a Query T-12 request from KHIE that passes a Kentucky Medicaid number. The response is provided in an encrypted DOC T12 containing a CCD (Healthcare Information Technology Standards Panel (HITSP) C32) that follows all KHIE nomenclature requirements (e.g., NDC, ICD-9, etc.). We are prepared to test this through the KHIE portal when it becomes available.

It is also noteworthy that Passport's CCD payload to KHIE will include a rich and timely set of clinical data on the member that is accessible in real time. This includes current dispensed medications; recent ED, inpatient and ambulatory visits; diagnoses; problem lists; and gaps in care for preventive health screenings and chronic disease management. A comprehensive set of data rules are in place to screen out prohibited data related to human immunodeficiency virus (HIV), substance abuse, and mental health-specific diagnoses, procedures and medications. This data will be used to improve case management services.

Passport's transaction will go through extensive testing with KHIE including connectivity, development, CCD compliance and end-to-end testing. Our KHIE transaction will be built on a flexible and extensible clinical information sharing technology infrastructure. As KHIE expands its document types, moves to later versions of HL7, considers a direct exchange model, and evolves to stay current with health care technology advances, we will continue to demonstrate our ability to keep pace with KHIE advancements. We will use state-of-the-art technology to improve member access to quality care.

Passport Network Providers

Connected to KHIE

~**73%** of KHIE participants are current Passport network providers, which totals nearly **80%** of Passport membership.

This improvement in care also hinges on providers utilizing EHR, so all providers have access to the most accurate and timely treatment information available through KHIE. Most hospitals and large practice groups currently utilize an EHR system, however, smaller practices often do not have the technical abilities or resources to adopt an EHR system, which puts them and the members they treat at a disadvantage. For that reason, connection and use requirements will vary based on the type of provider.

Providers and hospitals in Passport's network will be required to connect and utilize the KHIE and an EHR system to promote the facilitation of real-time data usage and improved care coordination. Exceptions will be evaluated if it imposes too great a financial burden on the provider. Hospitals will be required, at a minimum, to exchange applicable public health reporting data and ADTs, whereas non-hospital participating providers will have contractual requirement for connection and use of KHIE to exchange applicable public health data. The requirements for use of KHIE and EHR systems will be explained by our Provider Relations team and detailed in Passport's Provider Manual. They will also be encouraged to exchange a much broader range of data, to improve the overall member treatment data set.

Our strategy for encouraging providers to fully adopt the use of the KHIE and EHR is extensively detailed in **Section C.8. Kentucky Health Information Exchange (KHIE) and Electronic Health** Records

The Identifi PHM platform can ingest CCD and ADT data to support building a comprehensive profile of each member and stratifying profiles into risk levels. Notification of admissions, discharges and transfers, in particular, can trigger enrollment in care management programs for the members with the highest risk of readmission. This functionality has been implemented in conjunction with other state HIEs, and Passport will continue to collaborate with KHIE to leverage data in Identifi as KHIE develops mechanisms to make that available to MCOs and other entities.

Current Use/Planned Use: Provider Communication and Clinical Operations for Holistic Support of our Members Served

There are continuous opportunities to provide automated information for a holistic record through the various clinical programs administered for Passport members and collaboration with the providers serving these members. For example, the Identifi PHM used for care management (Identifi Care) integrates workflows across the care management continuum; automates workflows intelligently based on business rules; enables identification, stratification and engagement of members, including high-risk members; and facilitates multichannel communication and collaboration between individuals, providers and stakeholders. This care management software is licensed, with a base platform containing over twenty (20) different functions and optional modules. Using this system, our Care Managers can view an individualized record of every service provided to a member–including all data for services covered by Passport (including our subcontractors and providers).

The software can deliver PHRs, member decision aids, health management tools, clinical content for health education, and decision support tools at the point of care.

Other examples of clinical program utilization are the health coaches who work to close a member's care gaps through coordination of needed services; member education and help accessing and completing specific appointments or refilling medications; and through collaboration with the member's PCP and specialist(s). The member's PCP also receives care gap alerts and urgent notifications when a member's condition indicates a need for an urgent care visit with the PCP or treating provider. Periodic reports, as well as information provided through the local care management team or embedded Care Managers, also helps keep PCPs up-to-date on their member's progress. Messaging transmitted to the providers EHR or by fax alerts the PCP and specialist the member's Action Plan is available in Identifi, or by hard copy upon request

The presence of Population Health Managers boosts the ratio of health plan staff focused on provider engagement. While local field representatives are focused on operational issues such as claims payment and network contracting, Population Health Managers analyze PCP practice data and identify opportunities to improve performance, and help PCPs make full use of data available through the provider portal and EHR to help drive care enhancements by supporting practices' workflow improvements via plan do study act (PDSA) cycles.

Current Use/Planned Use: Electronic Health Record Integration

Passport understands that providers want workflows that are seamless and uninterrupted when delivering member care. This means staying in one tool, the EHR, whenever possible. Passport's MIS gives providers that adopt and use EHRs an almost automatic enhancement to their ability to better care for Passport's members through its EHR Integration services. Identifi was designed to work with and enhance our provider's EHR investments through integration solutions that keep clinicians in their usual EHR workflow. Passport providers continue to enter member clinical directly in the EHR, and Identifi EHR integration solutions will deliver insight into their members' care-management and/or population-health activities directly within their existing EHR workflows. This lessens the data entry administrative burden for providers while enabling access to more comprehensive member information.

To date, Identifi PHM has integrated with the following EHR systems that may already be familiar names to Passport providers: Allscripts, Amazing Charts, AthenaHealth, Cerner, Centricity, eClinicalWorks, e-MDs, Epic EMR, GE Centricity, Greenway PrimeSuite, NextGen, Practice Fusion, ReliMed and Quest Care360.

There are several EHR Integration solutions to support our providers in the sharing and use of information to best care for Passport's members.

- **Single Sign-on (Unidirectional into Identifi Practice from EHR):** Allows the provider to easily navigate into Identifi Practice directly from their EHR to access member data critical for value-based care. The single sign-on passes user log-in as well as Passport member identification information so that the EHR user can transition into Identifi Practice workflows.
- **Identification of Risk Lives (Unidirectional into EHR):** Flagging whether a member is an attributed risk life, listing the types of population health management program(s) he/she is enrolled in, and providing contact information for the member's care manager.

- **Care Gap Identification and Closure (Bidirectional):** Provides a proactive approach to flagging and closing care gaps before and at the point of care that increases efficiency, reduces duplicative tests/procedures, and ensures appropriateness of care.
- **Care Manager Notes and Physician Messaging (Unidirectional into EHR):** Sharing clinically relevant care manager–member interactions in the EHR in the form of a care manager encounter and Care Note, with the option of sending a tailored message to the member's PCP.
- **Intelligent, Guided Hierarchical Condition Category (HCC)/Risk Adjustment (RA) Documentation and Coding (Bidirectional**): Provides a logic-driven form within the usual member visit workflow to enable providers to easily capture the most accurate RA score for value-based members and assist physicians with documentation of the supporting notes and visit-level diagnoses.
- **Care Plan: (Unidirectional into EHR):** Enables users to share and update Care Plans.

Current Use/Planned Use: Innovations

As part of our Identifi PHM Systems & Module, there are plans to bring enhanced functionality via Passport's piloted Identifi Engage mobile module which allows for a daily check-in to be sent to the members who are already enrolled in Engage. This provides further opportunity to connect with members in another way that may provide alternatives for further increased engagement to support our mission. A brief description of the future enhanced capabilities is outlined below:

- To be eligible to enroll in Identifi Engage, members need to have both active eligibility in the health plan and be in a care program in either "enrolled" or "engaged" status. They will then be able to download the Identifi Engage app from their phones' module stores (supported on iOS and Android platforms) and register as users. This is a multistep, secure process and ensures secure messaging between the members and their respective care teams.
- Current functionality is simple messages. Enhanced functionality will allow members to complete daily check-ins. There are five to ten (5-10) questions, which address such items as "How are you feeling today?" and "What is your blood-pressure?" that will allow the users to take active ownership of their symptom management.
- Alerts will go to the Care Team member (a Care Advisor or Care Coordinator) and they will have the ability to see their current and past answers. This will allow the Care Team to reach out to its member or provider accordingly.
- Alerts will come to Identifi Care in the notification section.
- All information is stored within Identifi Care and becomes part of their record. Anyone who works on this member currently or in the future would be able to see the responses to the check-in questions as well as the chat history.

Passport will continue to deliver uninterrupted health information/records while planning for innovation and strategies to develop further connectivity for the Commonwealth, providers and members served.

C.6.d. Describe the Vendor's approach to assessing integrity, accuracy, and completeness of data submitted by providers and Subcontractors.

Data Onboarding and Validation Process and Procedures

Established systems and processes help to ensure data received from DMS, providers, members and subcontractors, including administrative (payor) and clinically relevant data across multiple sources and standard data types, is accurate and complete.

Robust System-Driven Data Validation

The Passport MIS ensures that data received from DMS, providers, members and subcontractors, including administrative (payor) and clinically relevant data across multiple sources and standard data types, is accurate and complete. It does this by verifying, through edits and audits, the accuracy and timeliness of reported data; screening the data for completeness, logic and consistency; collecting service information in standardized formats, including secure information exchanges and technologies; compiling and storing all claims and encounter data in a data warehouse in a central location in the MIS; assuring edits and audits comply with NCCI; resolving all reporting errors in transaction submission and reconciliation; and successfully transmitting required data to the Department as outlined in Section 15.2 of the Draft Medicaid Managed Care Contract and Appendices. Data validation allows all external data loading (batch or real-time messages) to go through a series of loading steps, involving multiple staging tables of increasing complexity (data validation, deducing, and aggregation) and quality assurance. In turn, the system loads clean data into the final data mart destination to be exposed to the BI layer and the data consumers. All these processes have robust logging, exception handling (data rejection), and auditing frameworks. There are error resolution screens and/or error reports available to assist operations as they work through the data errors. The QA team is involved during every step of the process to ensure a quality output from the data validation process, and performs extensive system integration testing to ensure the accurate implementation of the Identifi ETL process.

The ETL processes are built on top of an SQL server technology stack. A combination of SQL server integration services (SSIS), SAS and Orion Rhapsody tools are used within our ETL process for orchestration and implementation of business logic to ensure that the data is loaded from source to destination in multiple phases. This process makes it possible to map, normalize and validate administrative (payer), clinical and provider data provided by a variety of national, regional and local vendors, facilities and payers in both proprietary and EDI standard layouts/formats. We conform to HIPAA standards for the data sets, and apply multiple validation controls, both through initial data profiling as well as robust in-line data quality checks.

Data quality is measured at numerous checkpoints along the data integration pathway. Initial data profiling is also performed using commercial data profiling tools as well as customized data profiling code developed internally. The team is also responsible for producing data-quality assessment reports to alert to gaps in the

incoming data. The QA team also coordinates the UAT phase. The data providers participate in the UAT phase, and validate:

- That the data onboarding meets documented requirements for data exchange.
- The integrity of the data onboarding process, by checking against control totals for membership, claim counts, claim dollars, etc.
- The accuracy of the clinical output of data (e.g., lab results).

These validations are performed by exchanging reports as a part of the testing phase before completing implementation. After implementation, the Support Team performs quality checks to ensure system input is valid. Within Identifi, required fields, input validations and business rules are all enforced within the module itself.

We require that all data feeds include control totals to ensure the reconciliation of counts and aggregates for intake auditing and validation of load. The counts are validated at each load stage, and any error trapping is reconciled against the total loaded. In addition, when applicable, we utilize available administrative (payor) data summary reports to further validate the data load and final load disposition into the Identifi EDW, after applying the necessary business rules and subsequent transformation. These comparisons and validation reports are stored as part of the overall data quality tracking for each data load.

The Support Team has a series of monitoring processes in place where various files and datatypes from our data sources are checked for quality and accuracy. Data types monitored include, but are not limited, to (1) administrative (payor) data such as claims and eligibility; (2) transactional clinical data such as ADT, CCD, Lab and Biometrics; (3) other flat files such as health assessment survey (HAS), health risk assessment (HRA) etc. Any issues with operational data are logged via tickets, assessed by Tier-2 analysts, and escalated to the appropriate Tier-3 parties where required.

All incoming data is loaded through four (4) separate databases before it is ready for consumption. The data quality and standardization of the data increases at each level as outlined below:

1. **Staging:** Data is in client-specific format, with one table for each data type.
2. **Common Format:** Data is in a specified format. Data is transformed from client format in Staging to common format (CF) through the mapping requirements document and coding.
3. **Preload:** Data is prepped for loading into the EDW. Keys are assigned to prepare for star-schema normalization.
4. **Data Mart:** Final and centralized data repository. Data Marts are subsets of the EDW. Data is stored in transaction fact tables that link to reference dimension tables.

The four (4) databases are replicated in three (3) separate environments, DEV, QA and PROD, allowing for data transactions to be tested, verified and approved as data moves toward execution in production.

Data loading begins in the DEV environment, where the development team creates and tests their code(s). Once verified and free of any errors or vulnerabilities, the team promotes it up into the QA environment. Code pushes from DEV to QA happen twice daily. The QA environment is where functional testing occurs to test the mapping requirements, the developer's coding, client data quality and any special transformation logic(s). Once testing is completed in the QA environment, the code is slotted for promotion into PROD as part of a scheduled release.

We utilize and maintain separate environments including DEV, QA, UAT, Training and PROD to ensure each change is separated and validated prior to promotion. Identifiable data is available in the Staging and PROD environments. Masking and de-identification of any identifiable data is done in the UAT, QA, DEV, Training and Demo environments. The Identifi EDW is a member-centric data warehouse. The data marts that have member personal health information (PHI)/ePHI go through a de-identification process to make sure that the members' demographics and other identifiable information are masked. Internal identifiers like the Master Member ID (MMID) and TPA member numbers are maintained to help tie the admin and clinical data back to the member. DEV, QA, UAT, Training and PROD environments are deployed to different subnets, servers and databases. User accounts are specific to each environment.

The Identifi Web Module Security team has over six hundred (600) test cases that are updated and executed for each major release. Tests are maintained in Microsoft Test Manager, storing the results of each test for audit purposes. Code versions must pass the threshold of all severity (SEV) 1 through SEV 3 defects being resolved as exit criteria for promotion to higher test environments.

Performance testing, UAT and security testing are all required before a data code version may be deployed to production.

Data Aggregation and Normalization

Our MIS uses custom configuration and rules to derive the confidence level for matching members that are already present in the MIS. New members are assigned new Enterprise Unique IDs. All incoming data is run through the Enterprise Master Patient Index (EMPI) so that the data is aggregated at the member level and the platform has access to the member's longitudinal clinical record.

The EDW can create a Longitudinal Patient Clinical Record with a unique identifier for the MMID, which is updated as new information about the member is received. The data warehouse has a member record de-duping and aggregation process and utilizes "Smart" Delta Sensing Technology for processing efficiency. When aggregating data from disparate sources, the data platform utilizes industry-standard formats and coding for its data, including, but not limited to, International classification of diseases (ICD-10), SNOMED CT, logical observation identifiers names and codes (LOINC), CPT-4, CPT2, HCPCS, RxNorm, generic product identifier (GPI), vaccube administered (CVX), NDC and model output report (MOR) file HCCs.

Our MIS utilizes NextGate for enterprise-wide member matching and EMPI creation for all incoming member records across various sources (payor, EMR, etc.), ensuring that each member is represented only once across various sources by:

- Collecting a standard set of demographic information and member identifiers for each member, from various data sources, including, among others, EMR medical record numbers, health plan member numbers and health insurance claim numbers.
- Creating a "Single Best Record" for each member that is a composite of the most current information available for that member across the systems.
- Creating a unique identifier for the member, the MMID, to represent that member in the enterprise.

Deterministic scoring is used, based on configurable field-by-field "match analysis" that computes the total "match score" for the member record. The rules-based intelligence matching allows partial scoring, exact match or similarity rules to be applied on a field level. All exceptions below the threshold are manually reviewed to ensure accurate member match.

Working with Providers and Subcontractors for Data Accuracy, Timeliness and Completeness

Provider Claims Data

Claims are submitted by providers via EDI methods or on a paper claim form, which is converted to electronic format, through a clearinghouse. The clearinghouse performs base edits to ensure inbound claims are structurally valid. Upon receipt from the clearinghouse, all claims are processed by the Edifecs Smart Trading Platform, which performs WEDI/SNIP data validations. Edifecs is an industry leader in ensuring EDI transactions are fully populated and HIPAA-compliant, enabling Passport to maximize efficiency of claim adjudication processes. Health plan-specific business rules are also enforced within Edifecs, and claims not meeting HIPAA and health plan requirements are rejected back to providers via acknowledgment files. Clean claims are processed through our claim system, which verifies the completeness and accuracy of provider numbers, member ID numbers, diagnosis codes and procedure codes. Claim acknowledgments are returned to providers via the clearinghouse daily. A control process ensures all claims received are acknowledged. Discrepancies are identified, researched and corrected promptly.

Internal quality audits are performed frequently, and discrepancies are investigated promptly. Quality and independent audits are conducted by sampling claims and encounters processed by the Passport systems. Queries are written and preapproved by an auditor. Specific data elements may be requested (e.g., provider national provider identifier (NPI), procedure, diagnosis codes, bill amount, payment amount, etc.). Query results are provided to the auditor to verify the samples against internal systems.

Subcontractor Claims and Encounter Data

All subcontractor data is submitted in accordance with 42 CFR 438. In addition to its claims processing system, Passport also processes and supports encounters data submissions, contemplate rate capitation, program oversight and meeting DMS-specific reporting requirements. For twenty-two (22) years, we have remained firmly committed to our members in improving their health and quality of life–it is our mission.

Our encounter management and reporting system and process is comprised of four (4) key components:

Component 1. Intake/Preprocessing: Adjudicated medical (institutional, professional) claims are extracted from our core claims system (Identifi HPA) on a daily basis and loaded into the Edifecs EM platform in a proprietary comma separated values (CSV) file format. During the intake process, data is validated and subsequently converted into a common data format within the EM platform and made ready for encounter creation.

Component 2. Encounter Creation: To ensure accuracy, during the encounter creation process the EM system validates each encounter record against Kentucky-specific configured rules and edits based on DMS encounter reporting requirements and other data integrity validation, including HIPAA and other syntactical and structural data validation checks. Encounter accuracy and validation checks include, but are not limited to:

- Business edit validation
- Compliance validation
- Provider validation
- Kentucky-specific business edits
- Validation exception (duplicate check, NPI, etc.)
- Voids/replace for denials or accepted encounters

Encounters passing all business and compliance edits are generated and made ready for submission to DMS based on predetermined submission frequency. Records that do not pass all edits are systematically identified as “exceptions” and are logged for review and remediation, as applicable, prior to submission.

Component 3. Encounter Submission: The Edifecs platform generates outbound encounter extract files in accordance with DMS encounter file submission specifications, eliminating the need for manual manipulation of the files prior to submission. In accordance with DMS requirements, the encounter file is submitted to DMS on a weekly schedule (on Sundays). In addition, the encounters platform queues and tracks the claims that have been extracted for submission and reconciles the acceptance, failure or warning status upon receipt of response files from DMS.

Edifecs supports flexible submissions scheduling, allowing for both prescheduled and on-demand encounter transmissions, and utilizes tracking and reporting functionality to allow for the ability to quickly work and resubmit any rejections received from DMS at any time.

Component 4. Response and Reconciliation: Upon transmission of encounter files, response files are received from DMS and are subsequently uploaded to the EM system, and are systematically reconciled against submitted encounters. The system will update the disposition of each submitted record with an appropriate status (Accepted/Rejected/Warning) based on the response file received from DMS.

Encounter record errors are reconciled, and a detailed reconciliation report is submitted to DMS within thirty (30) days of the transaction or file error. Passport understands the requirement that encounter file transmissions not exceed a five percent (5%) threshold.

Converting Paper Claims to Encounter Data

Special attention is paid to gathering encounter data from claims that are submitted on paper. We employ a rigorous process for converting paper claims, first to an electronic 837 file, and then to encounters using the same process that is used for electronic claims. Passport works with SDS as our vendor to manage intake of paper claims and converting them to electronic 837 ANSI transactions, including attachments related to the claim to aid in adjudication. SDS uses a combination of optical character recognition (OCR) and manual data verification to ensure that the maximum amount of data is pulled from each document with in-line process screening against a number of control checks, such as format validation, claim completeness, CPT validation and more.

Validating That All Encounters Have Been Submitted

Subcontractor and provider encounter files are validated in depth during implementation process. The process for capitated providers to submit information sufficient to report encounters is reviewed during the provider orientation process. In production, the encounter submission process performs a basic X12 WEDI SNIP level four (4) verification to assess submitted information completeness before file submission to the division.

The Passport Edifecs Encounter Data Management platform tracks all encounters submitted from all sources to ensure an appropriate response is received for each file submission. Our encounter submissions are also routinely compared to the paid claims file to identify whether there are paid claims for which an encounter should have been submitted.

Providing Subcontractor Oversight

Passport utilizes subcontracted service providers for the delivery of pharmacy, behavioral health, vision and dental services. Each subcontracted vendor adjudicates claims via its respective internal systems, employing specific edits and validations to ensure that the required claim data elements are present and correct prior to payment and in compliance with DMS requirements. The resulting claim encounters are securely transmitted electronically to Passport in the format prescribed by DMS. Subcontracted vendor files are received by Passport on a predetermined submission schedule. The DMS-ready files are then transmitted to DMS and loaded to the Encounters Management platform for visibility and tracking.

Each subcontractor is held to a ninety-five percent (95%) acceptance rate minimum. Passport closely monitors this standard through weekly Acceptance Rate Reports. We work very closely with our subcontractors on identified issues to ensure timely and accurate submission of encounter data. The Encounter team and Data Operations team maintain a subcontractor contact list for any issues that occur during encounter submission (e.g., host connection issues, file non-receipt, file validation failure, etc.). Inbound data is proactively monitored against expected delivery dates and frequencies. Any deviations are logged from expected receipt schedules and promptly investigated for root cause and remediation. The data quality and integrity are monitored at receipt of data and throughout processing. Key volume and metric

trends are also monitored on an ongoing basis, measuring against historical trend and upper/lower control limits to monitor for consistency and completeness in inbound data. These monitoring procedures and alerts are used to ensure that timely and accurate encounter data submissions are received from subcontractors. Encounters Analysts meet weekly with each subcontractor to discuss encounter data and provide error resolution prior to submission of data to DMS. We work with our subcontractors on identified issues to ensure timely and accurate submission of encounter data. All data from providers and subcontractors is also collected in an easy, standardized format, screened for accuracy and compliance with the NCCI, and stored at our data warehouse.

C.6.e. Provide a description of the Vendor's data security approach and how the Vendor will comply with Health Insurance Portability and Accountability Act (HIPAA) standards including the protection of data in motion and at rest, staff training and security audits.

Data Security and Privacy Management Methodology

Passport's data security and privacy management policies commit to securing the confidentiality, integrity and appropriate availability of all PHI/ePHI of the health plan's members that Passport creates, receives, maintains or transmits, as required and prescribed by the HIPAA Security Rule, and the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the ARRA of 2009. Security of PHI/ePHI is a basic member and provider right, and it is intrinsic to the trust that Passport establishes with its members and providers. Security policies and procedures concerning minimum necessary standards and the privacy of PHI/ePHI address not only administrative requirements, but technical and physical safeguards to verify compliance with HIPAA Privacy Rules and the Security Rules.

HIPAA Standards

It is the policy of Passport to commit to securing the confidentiality, integrity and appropriate availability of all electronic protected health information of the client's members that Passport creates, receives, maintains or transmits, as required and prescribed by the HIPAA Security Rule, and the HITECH act, part of the ARRA of 2009.

Passport ensures that all policies, procedures and business plans protect against any reasonably anticipated threats or hazards to the security or integrity of its electronic protected health information. These policies and procedures address all aspects of its information security program—including administrative, physical and technical safeguards to protect the security, confidentiality and integrity of the health information in Passport's possession—whether on-site or through its vendors. As required under Section 13402 of the HITECH Act, Passport actively monitors its electronic systems. In the event of any breach of unsecured protected health information, Passport performs all required notifications.

Passport also protects against any reasonably anticipated uses or disclosures of such information that are not permitted or required and requires that all departmental policies and procedures comply with all the elements of the HIPAA Security Rule, as applicable to each department's functions and workforce and as identified through an ongoing Corporate Compliance Program.

Passport's Information Security Management Program, as well as corresponding documentation, including policies and procedures, is updated no less than annually. Passport reviews these programs and security policies to account for environmental or operational changes and must amend the policies or adopt additional security policies or measures to facilitate the security of PHI/ePHI.

Passport complies with all requirements of applicable federal and state laws and regulations concerning security of PHI/ePHI and nonpublic personal information. Departmental policies and procedures concerning minimum necessary standards and the privacy of PHI address not only administrative requirements, but technical and physical safeguards to verify compliance with HIPAA Privacy Rules and the Security Rules.

Passport requires that all departmental policies and procedures comply with all elements of federal and state laws, regulations and standards governing privacy of health care information that are applicable to managed care companies and health plan sponsors, including HIPAA Privacy Rules; the HITECH Act, the Gramm-Leach-Bliley Act (GLBA), and NCQA accreditation standards as identified through our Corporate Compliance Program.

Passport maintains the confidentiality, integrity and availability of data within the Identifi Platform through the following: routine vulnerability scanning of code; role-based access control; logging, monitoring and alerting of events; backups and recovery; replication and disaster planning; SDLC management; annual penetration testing; and annual risk assessments. Access to any production data is tightly controlled per HIPAA guidelines where system users are provisioned based upon the level of user access requested, adhering to the HIPAA "minimum necessary" requirements. All data in motion is also encrypted, adhering to HIPAA and HITECH regulations.

Protection of Data in Motion and at Rest

Passport utilizes full disk encryption across all facets relating to PHI/ePHI protection. Data is stored in an SQL server within the cloud infrastructure using Microsoft Azure's storage encryption. Data is de-identified in the QA, training and demo environments. Access to production data is tightly controlled as per HIPAA guidelines. The servers are protected within the corporate firewall and access to servers is limited to administrative-level access and to outside users who are authorized to access data under required business associate agreements (BAA).

Data residing in Exchange Online and SharePoint Online are encrypted using disk-level encryption. Microsoft utilizes Advanced Encryption Standard (AES) with 256-bit keys and is Federal Information Processing Standard (FIPS) 140-2 compliant. For any data in motion over a public network, such as the Internet, Identifi supports HTTPS on TLS 1.2. TLS encryption is used both opportunistically and policy-enforced with partners that frequently exchange sensitive information. Office 365 Message Encryption uses Rights Management Services (RMS) as its encryption infrastructure, which supports RSA 2048 for signature and encryption and supports SHA-256 for signature.

Passport ensures that any information stored in databases/datastores or on issued desktops, laptops and other portable computing devices and removable media is encrypted. Passport also utilizes pretty good privacy (PGP) encryption to protect data stored on any issued removable media devices. The system supports strong encryption only, resulting in a score of A+ from SSL Labs.

Passport also maintains logs of any cryptographic, encryption and data key management activities. Passport has policies in place that separate encryption of private and data keys. Private keys, which perform encryption themselves, are stored in encrypted locations. Data keys are stored separately from private encryption keys.

By utilizing Azure's Key Vault, Passport is able to manage its own cryptographic keys while Azure provides the secure hardware platform. Through the Azure Key Vault, Passport can create, revoke, authorize users or modules, and configure and/or monitor keys or shared secrets. Passport data is encrypted in transit and at rest through configurable and standards-based providers using a variety of protocols. This includes BitLocker, AES-256 (in Azure Media Services), IPsec (VNets), and others. Microsoft has policies, procedures and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Azure service. Cryptographic controls are used for information protection within the Windows Azure platform based on the Windows Azure Cryptographic Policy and Key Management procedures. Azure supports strong cryptography using standard, validated formats including AES-256, IPSec, 1024-bit Perfect Forward Secrecy (PFS), and FIPS-140-2.

Staff Trainings

Passport has an annual security awareness training for both existing and newly hired employees. All members of Passport's workforce must participate in security awareness training to enable them to properly protect ePHI. Security awareness training is based on job responsibilities and customized to focus on issues regarding use, confidentiality and disclosure of ePHI. Security reminders may also be part of other annual compliance programs.

Initial security awareness training for staff and users includes, without limitation, education regarding virus protection (including the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected), the importance of monitoring log-in success or failure and how to report discrepancies, password management including rules to be followed in creating and changing passwords and the need to keep them confidential, and user education in incident reporting procedures. Training for users who are granted remote access addresses vulnerabilities related to remote access, including, without limitation, the inadvertent downloading of information into temporary files, the recording of user account information by software modules, and other potential security breaches. Training also addresses, at a minimum, clear and concise instructions for accessing, storing and transmitting ePHI; password management procedures; Remote Access Device and media protection measures; and avoiding the downloading of ePHI to public access computers. Only users with proper authorization and training are granted remote access.

Our Privacy Awareness Training covers HIPAA compliance, PHI and ePHI protection, user authorizations and access (adhering to the HIPAA "minimum necessary" requirements), social media, social engineering, the use of technology and company-issued hardware/devices and systems, the proper handling and sending of PHI/ePHI, proper disposal of paper documents (that may contain PHI), password management and creation, auditing and monitoring of systems, data storage and backup procedures, the disposal of company-issued laptops/portable devices, mobile devices, and the steps to reporting security and privacy incidents. Our HelpDesk also communicates out monthly security awareness e-mails to all employees regarding changes to security policies/procedures.

Employees must attend a minimum of one (1) security training session per year or as necessary to train them on updates to the security policies. Privacy and security awareness training is reviewed and updated annually or as needed by the Privacy Office and the Privacy and Security Officer in collaboration with the Compliance team and the Learning and Development Department. A record of all security awareness training is maintained as documentation evidencing an employee's understanding of the security policies, the security training and acceptance of responsibility. The Security Policies Acknowledgment Form must be updated after each periodic security awareness training session attended by an employee. The Security Policies Acknowledgment Form is permanently retained in the employee's personnel file.

Security Audits

An audit of all of Passport's existing security policies, procedures and standards, and technical controls is done annually during the HIPAA Risk Assessment. This also covers the full BC/DRP, penetration and vulnerability testing, business impact analysis and risk assessments from both a corporate and Identifi Platform perspective. The aforementioned also includes any suppliers or critical hardware, network services and structures, and facility services. Security documentation is updated no less than annually. The security policies are reviewed to account for environmental or operational changes and the policies must be amended to adopt additional security policies or measures to facilitate the security of ePHI.

Passport conducts internal and delegate risk assessments and audits on an annual basis. Although this is an annual activity, as necessary, the Compliance Department will complete an assessment if processes change or are identified as being deficient. Third-party (external) audits are also conducted under the supervision and the authority of the Compliance team. The Compliance and Regulatory Affairs Committee is notified of the outcomes from the risk assessment process.

As outlined above, Passport engages in various internal and independent (external) audits of our information security policies and our security controls. The internal audit process:

- Defines the scope and audit universe
- Performs a risk assessment as outlined by our Risk Management Program
- Conducts interviews
- Reviews established processes, procedures and policies
- Performs formal auditing

- Performs remediation of any risks, vulnerabilities and deficiencies
- Closes the internal audit

Internal audits include walkthroughs, access management audits, change management audits, internal/external penetration testing, module vulnerability assessments, HIPAA/HITECH standards audits, and operational controls assessments. If gaps are identified during the HIPAA Risk Assessment, a remediation plan is initiated and executed prior to completion of the risk assessment. This action is followed by a second audit to confirm that the discovered gaps are addressed and remediated.

The Identifi Platform also undergoes an annual service organization control (SOC) (2) audit during our HIPAA Risk Assessment period.

C.6.f. Describe any proposed system changes or enhancements that the Vendor is contemplating making during the anticipated Contract Term, including subcontracting all or part of the system. Describe how the Vendor will ensure operations are not disrupted.

System Changes

At this time, there are no proposed system changes for the Passport MIS that would disrupt existing operations. Identifi Health Plan and Identifi Population Health will continue as the primary system for the proposed contract. As a proprietary system owned and operated by our partner Evolent, no modules or subsystems within Identifi will be subcontracted. We acknowledge the ever-changing needs of health care and that the Kentucky Medicaid program requirements will be revised as well–prompting standard changes to our MIS. Although there are no system changes planned, Passport will notify DMS at least ten (10) days in advance of any implementation that may impact the integrity of the data, including such changes as new claims processing software, new claims processing vendors and significant changes in personnel.

Passport can provide value in terms of implementation speed and provide a more robust solution by dint of having already implemented the Identifi Platform. Passport's MIS and its subsystems and modules are already configured to meet the needs of the DMS and are currently functioning within the guidelines and specifications of the Commonwealth. The MIS meets or exceeds all requirements of the Kentucky Managed Care Program, including member services, third-party liability coverage, provider, reference, encounter/claims processing, financial, and utilization/quality improvement.

The existing secure HIPAA-compliant data exchanges and EDI feeds that currently connect Passport and DMS to drive the Kentucky Medicaid Managed Care program on the Identifi Platform do not need to be reimplemented as part of our proposed solution. Another inherent advantage of leveraging the existing Identifi Platform is that the disparate data sources that are already aggregated and normalized as a part of our existing implementation would not require any data conversions or data migration efforts for elements already integrated. In addition to not needing to reintegrate with the existing data or reimplement existing functionality, leveraging the Identifi Platform solution would provide continuity for end users, providers and members alike.

Identifi is offered as a SaaS solution and as such, Passport provides all required hosting, support and monitoring and any upgrades requested by DMS. In the event waivers, changes or enhancements are to be

made, these upgrades are released seamlessly into the client instance after receiving signoff from DMS, which means that Passport will never be left with an outdated system that no longer meets industry standards and best practices.

Proposed Enhancements

Passport is regularly evaluating enhancements to the platform to improve member and provider experience, as well as to improve the efficiency and quality of its subsystems. Enhancements that Passport is considering during the contract term include the following:

- **Improve Tracking of Authorized Units in Claims Adjudication** (*Claims Processing Subsystem*) to improve ability for claims to be auto-adjudicated based on linking multiple claims to units authorized in the original prior-authorization request. This enhancement would also clear links with authorization requests when claims are voided.
- **Enhance Fraud Waste and Abuse** (*Surveillance Utilization Review Subsystem [SURS])* detection prior to claims payment, including automation of claim denials prior to payment, pending claims for additional manual investigation, and denying/releasing claims for payment once an investigation has been marked as completed. Improving detection prior to payment will reduce the need for recovering payment already made to providers.
- **Enhance Identifi Practice and Identifi Review** (*SURS*) to provide additional feedback to both requestors and Passport staff on what services are covered benefits and what services require prior authorization requests. This enhancement will ensure that members receive covered services and members/providers are not waiting for authorizations for services that do not require prior authorization requests. This enhancement may also include service-specific guidelines on what supporting documentation providers must include with prior authorization requests, thereby reducing the time required to review requests.
- **Deploy Precision Pathways** – a web-based point-of-care tool that empowers providers with the latest science, innovative new therapies and clinical compendia to identify the most effective, least harmful and least expensive treatment options for Passport members with cancer and heart disease (*Surveillance Utilization Review Subsystem)*. Additional details are discussed in Section C24. Population Health Management (PHM) Program
- **Enhance insights/reporting delivered to providers in Identifi Practice** (*Utilization/Quality Improvement Subsystem*). Proposed enhancements to allow providers to better manage their panels include adding supplemental data related to care gaps and quality measures (e.g., last date of qualifying service, due date for next service), quality performance trending, risk-adjusted cost and utilization performance.

Any planned system changes or enhancements, including major releases of the Identifi PHM system, go out on a quarterly basis, on the last Sunday of a predetermined month, while releases within the Identifi HPA system go our every ten (10) weeks on Fridays (after business hours). Minor updates to the Identifi PHM system are also released every second and last Friday of the month in accordance with the Release Management Cycle. Most production releases are completed within a four-to-six (4-6)-hour time frame and happen during our already-established maintenance windows outside of business hours to minimize

disruption to users, including providers and members. Passport recognizes that DMS requires notification of any significant changes to the system that may impact the integrity of the data, including such changes as new claims processing software, new claims processing vendors and significant changes in personnel at least ten (10) days prior to its implementation as outlined in Section 15.1 of the Draft Medicaid Managed Care Contract and Appendices.

Passport has anticipated concerns around disruption to existing operations in the event sourced systems and workflows are changed and enhanced. The Identifi Platform module development teams use a combination of manual and automated regression testing to ensure the quality of each release. Regression testing is the process by which we test any changes and/or enhancements or updates to the Identifi Platform to ensure that system changes/updates do not adversely affect other systems, including systems operated by the client and subcontractors' systems, as well as ensuring that older programming still works with the new changes. Our testing team maintains a library of over 1,500 test cases in Microsoft's Test Manager that are used to validate candidate releases. Of the 1,500 test cases, roughly six hundred (600) are dedicated solely to regression testing, and they are executed both manually and automatically. Our regression testing ensures that system changes do not impact system components which have not been changed for a release.

Conclusion

Passport operates a robust MIS. The MIS and its subsystems are fully operational, already configured to meet the needs of DMS, and are currently functioning within the guidelines and specifications of the Commonwealth. Our MIS stands ready to execute on current and future program requirements.

Passport has been honored to serve the Kentucky Medicaid and foster care populations for 22 years and will continue to comply with all provisions of the Medicaid Managed Care Contract and Appendices (including Kentucky SKY) as we continue to serve them in the future.