C.28. Records Maintenance and Audit Rights

a. Describe the Contractor's methods to assess performance and compliance to medical record standards of PCPs/PCP sites, high risk/high volume specialist, dental providers and providers of ancillary services to meet the standards identified in Section 38.1 "Records Maintenance and Audit Requirements" of RFP Attachment C "Draft Medicaid Managed Care Contract and Appendices."

b. Describe the Contractor's approach to prevent and identify data breaches.

c. Describe the Contractor's approach to conducting Application Vulnerability Assessments as defined in Section 38.6 of RFP Attachment C "Draft Medicaid Managed Care Contract and Appendices."

Passport Highlights: Records Maintenance and Audit Rights

How We're Different	Why It Matters	Proof
Twenty-two (22) years as a trusted steward of confidential Kentucky Medicaid medical records and other sensitive data	• Protecting records is essential to building trust among our membership	• Ongoing compliance with state and federal guidelines, Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH) and Passport policy • Ninety-eight percent (98%) of Passport practitioners exceed the required average compliance score of eighty percent (80%)
Dedicated on-site cybersecurity and threat resolution team	• Data breach prevention and mitigation is key to safeguarding sensitive member, provider, and DMS data • A local team allows for higher integration of system and business process monitoring and immediate response times	• Passport has never had a data breach • Passport has never had a cybersecurity data disclosure • IT security risks and potential incidents are mitigated in under 24 hours

Introduction

Passport has been trusted to serve Kentucky Medicaid recipients for over two decades. As a steward of this trust, we have woven accountability, security and confidentiality in all levels and aspects of the organization. These values are extended into our relationships with providers, employees and contractors to prevent data breaches and ensure safe handling of member information.

C.28.a. Describe the Contractor’s methods to assess performance and compliance to medical record standards of PCPs/PCP sites, high risk/high volume specialist, dental providers and providers of ancillary services to meet the standards identified in Section 38.1 “Records Maintenance and Audit Requirements” of RFP Attachment C “Draft Medicaid Managed Care Contract and Appendices.”

Provider Medical Record Standards

Passport implements medical record-keeping standards that cover confidentiality, organization, documentation, access and availability of records. We have adopted National Committee for Quality Assurance (NCQA) standards, as approved by the Department for Medicaid Services (DMS), as well as those required by the state and federal entities requiring records retention identified within the request for proposal (RFP) and all attachments (e.g., Section 38.1, Records Maintenance and Audit Requirements, of RFP Attachment C, Draft Medicaid Managed Care Contract and Appendices). Passport revises its standards as needed to conform to new NCQA, federal or state, or DMS recommendations. Providers must agree to these requirements in their contract, as included in attachments, such as the provider requirement to forward the medical record of a member when he/she changes primary care provider (PCPs), and the requirement to have ongoing access to Passport’s standards via the Provider Manual (see Section 4.5 of the Passport Provider Manual in **Attachment C.17-2_Passport Provider Manual.**)

Passport ensures medical record confidentiality policies and procedures comply with state and federal guidelines, HIPAA/HITECH and as outlined in **Attachment C.28-1_Policy QI.0333.E.KY Medical Records Standards and Review**. Documentation in the medical records is confirmed to be timely, legible, current, detailed and organized to permit effective and confidential member care and quality review. Complete medical records include but are not limited to medical charts, prescription files, hospital records, provider specialist reports, consultant and other health care professionals’ findings, appointment records, and timeliness of services provided to the member. These standards also apply to specialists, dental providers and providers of ancillary services. We require that the member record be signed by the provider of service. PCPs are contractually obligated to forward member records to a member’s new provider if a member changes his/her PCP. The records must be forwarded to the new provider within 10 days of the member authorizing the transfer with signature.

Passport ensures provider compliance with medical record-keeping standards by performing regular audits. These audits are conducted periodically by Passport’s Quality Assurance team and at least every three (3) years. The team executes on-site reviews of practitioners’ offices, procedures and chart samplings. We also use our internal controls and data reporting to ensure compliance standards and regulatory requirements are being met or exceeded. We transmit our findings through provider interaction meetings, our quality committees and with DMS. These audits typically:

- Demonstrate the degree to which providers are complying with clinical and preventive care guidelines
- Allow for tracking and trending of individual and plan-wide provider performance over time
- Include mechanisms and processes that allow for the identification, investigation and resolution of quality of care concerns
- Include a mechanism for detecting instances of overutilization, underutilization, and misutilization

In addition, we contractually require our subcontractors and providers to comply with record management requirements.

Practitioners must achieve an average score of eighty percent (80%) or higher to be considered in compliance. All findings are logged and maintained in a database to facilitate detailed analysis. Ninety-eight percent (98%) of Passport practitioners exceed the required average compliance score of eighty percent (80%) and are exempt from the review cycle for three (3) years. We monitor practitioners who score less than eighty percent (80%) through a corrective action plan and reevaluation process as outlined in **Attachment C.28-1_Policy QI.0333.E.KY Medical Records Standards and Review**.

Our subcontractors and providers are also contractually required to comply with records management requirements, which are monitored through annual on-site delegation audits that include a review of policy and procedures and record management requirements.

C.28.b. Describe the Contractor’s approach to prevent and identify data breaches.

Prevention and Identification of Data Breaches

Passport takes the use, disclosure and security of our data, specifically personal health information (PHI), seriously. As part of our HIPAA/HITECH-related precautions, we have implemented the following rules and practices to limit data access and exposure:

- All employees who support Passport are required to:
  - Use programmed access cards to enter restricted areas of the Passport campus
  - Never use portable information storage devices, unless specifically approved and arranged by the IT department
  - Dispose all hardcopies of PHI, personally identifiable information (PII), confidential or sensitive information into company-organized shred containers for secure disposal
  - Comply with all applicable password policies and procedures on data privacy and security
  - Follow special guidelines for electronically handling PHI, PII, confidential or sensitive information

- All Passport employees and contractors are trained to:
  - Digitally lock the screen after 15 minutes of inactivity
  - Physically lock away the computers if the workstation is unattended
  - Never share passwords or building access cards
  - Use the provided secure keyword to encrypt all confidential (PHI, PII, etc.) emails
  - Ensure Passport electronic devices, including laptops or mobile devices, are encrypted at all times when traveling and are not left unattended in a visible location or in an unlocked vehicle
  - Immediately report any suspected cybersecurity incidents or lost/stolen equipment to Passport IT and/or Compliance
- All Passport employees and contractors are prohibited to access:
  - Websites that are electronically analyzed and identified to be a security threat
  - File-sharing websites that could easily share unintended data
  - Off-site printers (all printing must take place on Passport premises)
  - Cloud-based email accounts or cloud storage services (i.e., Google, Yahoo, Dropbox, etc.)
  - Administration rights to install software other than software approved by Passport IT
- Other audit oversight controls include:
  - Monthly workstation assessments to confirm no restricted information is at risk of exposure
  - Annual refresher training on privacy and security for all employees supporting Passport
  - Provider data protection education, data handling provisions in the provider agreements and periodic provider data management audits
  - Cybersecurity awareness training

Passport also maintains active breach monitoring through technological tools and vetted processes. We have installed Network Intrusion Detection appliances on both the perimeter and internal Local Area Network (LAN), which are monitored twenty-four (24) hours a day, seven (7) days a week throughout the entire year. In addition to intrusion detection, we also use log correlation and system event monitoring. Our data loss prevention (DLP) technology enforces policy restrictions on data at rest and data in motion. Last, we have protocol filtering on network ingress/egress access points. All of these active monitoring components work together to keep Passport’s systems and data protected.

Handling Accidental HIPAA Disclosures and HIPAA Breaches

If an employee accidentally sends a fax to an incorrect recipient, sends an email containing PHI to the wrong person, or any other accidental disclosure of PHI has occurred, the incident is reported to our Privacy Officer. The Privacy Officer determines what actions need to be taken to mitigate risk and reduce the potential for harm. Specifically, the incident is investigated and a risk assessment is performed to determine the probability of PHI having been compromised, the level of risk to individuals whose PHI has potentially been compromised and the risk of further disclosures of PHI. Following the risk assessment, the risk is managed and reduced to an appropriate and acceptable level. If the Privacy Officer concludes that a breach has occurred, under the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414), the Privacy Officer will ensure, where appropriate, that notifications are sent to DMS, the impacted individuals, a media notice is issued and a report of the breach is sent to the Department of Health and Human Services’ Office for Civil Rights (OCR).

Staff Support for Information and Data Security

Passport's cybersecurity team is also on hand to monitor and resolve data security threats. This on-site response team is trained to react quickly and effectively in the event of sensitive security incidents. In addition to response, the team studies and stays current with the latest security news, trends and training to stay prepared for emerging threats. Passport collaborates with its partners on data security matters and plans to perform compliance and IT-driven tabletop exercises with its partners in which it will simulate threat responses, communications and resolutions of real-world security incidents.

Information protection is a paramount priority for Passport. For this reason, we have a Compliance Hotline that is available twenty-four (24) hours a day to employees or contractors who want to report an actual or potential data exposure.

We also have an on-site compliance team, HIPAA Privacy Officer and security officer who offer an open-door policy when it comes to potential breaches of information or other compliance-related matters. In addition, we have a coordinated effort between Passport's compliance and IT teams for all privacy and security efforts, and we have a coordinated effort between Passport and its subcontractors relative to HIPAA privacy and security matters.

Our prevention and identification protocols include notification to required parties, including:

- Law enforcement as needed
- Mandatory incident management review and remediation
- Other forensic best practices within the data security guidelines
- Additional technical and physical safeguards
- Monitoring of our network, platforms and encrypted data stores

C.28.c. Describe the Contractor's approach to conducting Application Vulnerability Assessments as defined in Section 38.6 of the RFP Attachment C "Draft Medicaid Managed Care Contract and Appendices."

Internal Vulnerability and Penetration Testing and Audits

Passport takes a holistic approach to security and performs multiple levels of vulnerability testing, penetration testing and external auditing procedures. We conduct static and dynamic vulnerability and penetration testing on the entire network infrastructure, including the servers housing the applications. Our security testing model consists of ongoing vulnerability and penetration testing of various layers of our infrastructure, including the underlying applications, and a rotating annual external assessment of our full security program and HIPAA/HITECH risk by qualified third parties. In addition, we have incorporated security testing during our development processes, and it is part of our Software Development Life Cycle (SDLC). Despite not having any off-site web applications processing PHI (for network security reasons), part of this ongoing assessment is performing a full Open Web Application Security Project (OWASP) Top 10 (e.g., Injection, Cross-Site Scripting [XSS], Sensitive Data Exposure) compliance test of our custom web applications.

During the course of security testing, any vulnerabilities discovered, application or otherwise, are remediated based upon severity and risk priority according to the Common Weakness Scoring System (CWSS) classification system. Any changes to production applications are first vetted through our Change Advisory Board (CAB). The CAB consists of various IT leadership roles, including but not limited to security, infrastructure and data leadership. During regular weekly CAB meetings, the CAB reviews the proposed changes for potential risks and chooses to approve or deny the proposed change to the application.

We have a set of policies and procedures related to information security vulnerability and penetration testing guidelines. These policies and procedures comply with the framework established in the HITRUST Common Security Framework (CSF), which ensures compliance with multiple regulations, including HIPAA/HITECH, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000, National Institute of Standards and Technology (NIST), etc. An example of this extensive testing is our assessments performed on the Identifi platform. We have conducted a HITRUST self-assessment to identify our current compliance and use our vulnerability tests to not only identify issues but to remediate items based on severity and risk under our risk management and disaster recovery programs.

Identifi Platform Penetration and Vulnerability Testing

Passport uses the Identifi platform and interfaces for various operational and clinical functions. We execute its external penetration and vulnerability testing through GuidePoint, its web application security vendor.

GuidePoint performs manual penetrations tests (MPTs) annually and automated static code analysis (SCA) quarterly to ensure Identifi is free from common vulnerabilities. The GuidePoint program tracks vulnerabilities and their mitigations across software releases to present a holistic view, over time, of the resilience of the application against various attack vectors as defined by OWASP. Special emphasis is placed on the OWASP Top 10 vulnerabilities, including Structured Query Language (SQL) injection, XSS, and parameter tampering/server-side input validation.

Passport adheres to OWASP guidance for classification and remediation patterns to manage common web application vulnerabilities. Each new release of the Identifi application is assessed by Evolent Health's (a Passport partner and vendor) Web Application Security team to evaluate any impact to the risk profile of the application so that new risks can be mitigated. We scan for vulnerabilities on all systems and perform remediation within thirty (30) days. Application vulnerabilities discovered through our web application security program are remediated based upon severity and priority according to the CWE classification system.

All Identifi application components are currently VL5, the highest level of certification offered by GuidePoint. GuidePoint tests for the following at minimum:

- Injection
- Broken authentication and session management
- XSS
- Insecure direct object references
- Security misconfiguration
- Sensitive data exposure
- Missing function level access
- Cross-site request forgery (CSRF)
- Using known vulnerable components
- Invalidated redirects and forwards

Conclusion

Data security and integrity is at the core of Passport. Our dedicated team employs stringent processes and protected systems to maintain secure, tested and audited medical records and other sensitive data for the ongoing safety of our members. It has been our commitment and responsibility, and a Passport priority in all levels and aspects of our organization. We are proud to say that we have never had a major breach in our twenty-two (22) years supporting the community and our members.

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.