C.28 Records Maintenance and Audit Rights

REQUIREMENT: RFP Section 60.7.C.28
28. Records Maintenance and Audit Rights (Section 38.0 Records Maintenance and Audit Requirements)
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."

To deliver high-quality, efficient access to care, Molina's approach will ensure all contracted providers, including primary care providers (PCPs) / PCP sites, high-risk/high-volume specialists, dental providers, and ancillary services providers, fully comply with Kentucky Medicaid program medical record standards.

Drawing upon the experience of our 14 affiliated Medicaid health plans, Molina has the expertise to maintain medical record confidentiality policies and procedures. We will monitor for—and ensure compliance with—Commonwealth and federal laws and regulations, including HIPAA, as well as the requirements set forth in Attachment C, Draft Medicaid Managed Care Contract and Appendices, Section 38, Records Maintenance and Audit Rights.

Covering All the Bases

- Comprehensive processes will enable systematic review of provider medical records to verify standards compliance
- Zero-Trust security model will promote greater security throughout our network
- Vulnerability management will quickly detect, report, and remediate security vulnerabilities within the organization

a. METHODS TO ASSESS PERFORMANCE AND COMPLIANCE TO MEDICAL RECORD STANDARDS

Molina will cover specific Contract requirements with providers and delegated providers—including performance and compliance with medical record standards—through our written provider agreements, provider orientations and annual trainings, and Provider Manual. Our Provider Manual, which we will tailor to meet Contract requirements for providers participating in our Kentucky Medicaid network, will clearly stipulate the scope of our providers' administrative, regulatory, compliance, clinical quality, and preventive care performance responsibilities.

Molina also will audit, on a rotating basis, contracted provider practices based on risk considerations, size, and complexity of the provider. We will apply a standard checklist and a variety of effective audit techniques to understand a provider's compliance with the Kentucky Medicaid program requirements stated in the Provider Manual, including adherence to medical record standards.

HOW WE WILL ASSESS FOR PERFORMANCE AND COMPLIANCE

As part of our comprehensive provider network and subcontractor management processes for Kentucky, Molina will apply the analysis methodology described below to systematically review provider medical records and verify standards compliance. If standards are not met, we will draw upon contract stipulations to promptly implement process improvements and other corrective actions to remedy the deficiency. We then will assess the practice site's follow-up plans to improve their compliance with medical records standards and goals.

For the Kentucky Medicaid program, we will apply and maintain methodologies to regularly assess provider performance and compliance with medical record standards across contracted provider types, including PCPs and PCP sites, high-risk/high-volume specialists, dental providers, and ancillary service

© 2020 Molina Healthcare of Kentucky, Inc.

providers. Molina will routinely monitor its network physicians using valid methodologies and perform annual analysis of access data to ensure we provide appropriate Enrollee access to primary care, specialty care, and behavioral healthcare. Compliance and performance rates will be evaluated annually against access standards and goals.

We will conduct physician surveys, examine access-specific grievances, and study applicable CAHPS 5.0 questions as part of our Accessibility of Services Analysis. This effort will enable us to quantitatively analyze and determine performance and the rates of compliance with access standards and goals. It also will help us to qualitatively evaluate and identify necessary improvements. Table C.28-1 provides an example of the data sources and methodology we will adapt for use in Kentucky.

Table C.28-1. Example of Data Sources and Methodology

Data Source	Description
Appointment Accessibility Audits	We will conduct these audits using a phone survey to interview providers and/or their staff, applying quotas established by provider type (e.g., PCPs, specialists, and behavioral health providers). We then will analyze the responses in terms of access standards. Because the survey results are self-reported, we will supplement surveys with analysis of specific CAHPS 5.0H questions and access-specific Enrollee grievances and appeals information.
Access-specific Grievances and Appeals	We will collect grievances and appeals using our core claims administration system, QNXT, and our appeals and grievances application. We will extract the information from the systems by querying for a specific period and sort them by categories (e.g., quality of care, access, attitude/service, billing/finance, quality of practitioner office site). Grievances and appeals will be monitored monthly and reported quarterly. No sampling will be used.
Applicable CAHPS 5.0 Questions	We will collect CAHPS 5.0H data annually using a mailed survey. This data will accurately capture Enrollee feedback and gather information relative to quality of care issues in two age-based groups: • **Adults**—Enrollees 18 years of age and older who are currently enrolled and have been continuously enrolled for at least five of the six months of the measurement year. A random sample of eligible Enrollees will be drawn and processed, so only one adult per household will be included in the sample. • **Children**—Enrollees 17 years of age and younger (as of December 31 of the measurement year) who are currently enrolled and have been continuously enrolled in the plan for at least five of the last six months of the measurement year. A random sample of eligible Enrollees will be drawn and processed, so only one child per household will be included in the sample.

The following examples, drawn from our Accessibility of Services Analysis report, demonstrate how that report will align with the standards and audit activities specified in the Draft Contract.

Provider Compliance with Clinical and Preventive Guidelines

To demonstrate the degree to which providers are complying with clinical and preventive care guidelines, Molina will set appointment standards. We then will compare physician survey results to those standards to determine the level of compliance. We provide examples in Tables C.28-2 and C.28-3.

Table C.28-2. Appointment Standards Example—Physical Health

Physical Health Appointment Types	Standard
Routine, preventive/symptomatic	Within 4 weeks
Urgent care	Within 48 hours
After-hours care	24/7 availability
Specialty care (high volume)	Within 12 weeks
Specialty care (high impact)	Within 12 weeks
Urgent specialty care	Within 48 hours

© 2020 Molina Healthcare of Kentucky, Inc.

Table C.28-3. Appointment Standards Example—Behavioral Health

Behavioral Health Appointment Types	Standard
Non-life threatening	Within 6 hours
Urgent care	Within 48 hours
Routine care	Within 10 business days
Follow-up routine care	Within 30 calendar days
After-hours care	24/7 availability

To further illustrate these examples, we may mandate that practitioners achieve a specific percentage on non-behavioral health access standards and another specific percentage on behavioral health access standards. Those not complying with the performance standards will receive letters notifying them of the findings and the need for corrective action. Then, Molina's Provider Services or Quality Improvement staff will follow up to confirm the deficiency has been corrected.

Quality of Care Concerns / Overutilization, Underutilization, and Misutilization

Table C.28-4 offers an example of how we might document opportunities for improvement as well as planned interventions to ensure improvement is made. It shows a mechanism and process that can be applied to the identification, investigation, and resolution of quality of care concerns. It also may be used when detecting instances of overutilization, underutilization, and misutilization. Our qualitative analysis will allow for the documentation and identification of items that can be recommended to the Quality Improvement Committee, which will review and analyze the identified barriers and opportunities; recommend further actions, as applicable; and approve the report.

Table C.28-4. Example of an Opportunity for Improvement and Planned Interventions

Opportunity for Improvement	Intervention	Date of Action	Priority	Barrier Addressed	Responsible Department
Improved Enrollee and provider communication; review of authorization guidelines, network gaps, and provider online/paper directories to ensure that Enrollees can obtain care as needed	• Provide ongoing updates and revisions • Provide ongoing review and maintenance of our material repository • Update Molina's website • Outline potential improvements to our existing material and potential for additional communication • Drive awareness of our Enrollee self-help tools through our Welcome Calls and Enrollee-facing departments.	Ongoing	High	Barrier 1	Provider Contracting

Provider Site Visits at Time of Credentialing

At the time of provider credentialing, Molina will conduct initial visits to provider sites, including PCPs / PCP sites, high-risk/high-volume specialists, dental providers, and providers of ancillary services, as required by 42 CFR Part 455 Subpart E. Our comprehensive screening will include a structured review and evaluation of each site against our standards, NCQA guidelines, federal and Commonwealth guidelines, and Contract requirements. We will document our evaluation of the medical records and the record-keeping practices at each site for conformity with our standards and with those in our Contract with the Commonwealth.

Molina will conduct routine provider site visits outside of credentialing on a regular basis as dictated by our Contract and/or when a provider situation warrants, such as when we respond to quality-of-service complaints from our Enrollees. If a reported issue seems especially concerning, we will conduct an unannounced site visit to address the matter with the provider office. For comparatively minor issues, we will track and trend the issue. If the same issue continues to be a concern, we then will make an office visit. When providers do not address issues identified in a visit, we will propose a corrective action plan. In cases where a serious concern is not addressed, we will recommend termination from our network.

Our affiliated health plans successfully perform similar medical record standard assessments in coordination and collaboration with respective state Medicaid agencies to ensure providers meet all program and contractual requirements and comply with state and federal laws and regulations. For example, our California affiliate works closely with the state's Department of Healthcare Services to conduct site reviews to ensure all PCP sites contracted in the state's Medi-Cal (Medicaid) program can:

- Provide appropriate primary healthcare services
- Carry out processes that support continuity and coordination of care
- Maintain patient safety standards and practices
- Operate in compliance with all applicable local, state, and federal laws and regulations

In California, MCOs do not maintain member medical records. That responsibility is solely consigned to contracted providers. To monitor this requirement, our California affiliate uses a Department of Healthcare Services-provided tool to conduct regular audits of provider sites that include review and verification of medical record standard compliance.

Third-party Requirements

Our commitment to medical record standards will further extend to our subcontractors. We will require an extensive information security requirements agreement to ensure compliance with medical record standards and security of data. A sampling of these requirements is provided in Table C.28-5.

Table C.28-5. Information Security Requirements

Requirement	Details
Network Security	Subcontractor will agree to maintain network security that, at a minimum, includes hardware and software protections such as network firewall provisioning, intrusion, and threat detection, and regular third-party vulnerability assessments, and policies and procedures enforced as part of a robust information security program including access control limitations and review, physical security controls, and personnel training programs that include phishing recognition and proper data management hygiene. Subcontractor will agree to maintain network security that conforms to generally recognized industry standards and best practices that subcontractor shall apply to its own network in conformance with the families of controls found in National Institute of Standards and Technology (NIST) Special Publication 800.53, 800.171, and ISO/IEC 27001.
Data Security	Subcontractor will agree to preserve the confidentiality, integrity, and accessibility of client data with administrative, technical, and physical measures that conform to generally recognized Industry standards that subcontractor then will apply to its own processing environment. Maintenance of a secure processing environment will include, but not be limited to, the timely application of patches, fixes, and updates to operating systems and applications as provided by subcontractor or open source support.
Data Storage	Subcontractor will agree that any and all client data will be stored, processed, and maintained solely on designated target servers and that no client data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of subcontractor's designated backup and recovery processes and encrypted.

© 2020 Molina Healthcare of Kentucky, Inc.

Requirement	Details
Data Encryption	Subcontractor will agree to store all client backup data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Subcontractor further will agree that all client data constituting personally identifiable information stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption, a 1024 (or larger) bit key length for asymmetric encryption, and FIPS PIB 140-2.
End-of-agreement Data Handling	Subcontractor will agree that upon termination of the Agreement and upon client's written approval, it shall erase, destroy, and render unrecoverable all client data, and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the client's request, whichever shall come first. At a minimum, a "clear" media sanitization will be performed according to standards enumerated by the NIST Guidelines for Media Sanitization, SP800-88, Appendix A.
Right to Audit	Client or a client-appointed audit firm (hereafter "auditors") will have the right to audit the subcontractor and the subcontractor's subcontractors or affiliates that provide a service for the processing, transport, or storage of client's data. Client will announce its intent to audit subcontractor by providing at least 10 business days' prior notice to subcontractor. A scope document along with a request for deliverables will be provided at the time of notification of an audit. If the documentation requested cannot be removed from the subcontractor's premises, the subcontractor will allow client and/or auditors access to the subcontractor's site or share on the desktop screen in an audio–video conference. Where necessary, subcontractor will provide a personal site guide for client and/or auditors while on site. If a site visit is necessary, subcontractor will provide a private workspace onsite with electrical and Internet connectivity for data review, analysis, and meetings. Subcontractor will make necessary employees or contractors available for interviews in person or by phone during the audit period. In lieu of client or its auditors performing their own audit, if subcontractor has an external, independent audit firm that performs a certified SOC or HITRUST review, client will have the right to review the controls tested as well as the results and the right to request additional controls be added to the certified SOC or HITRUST review for testing the controls that have an impact on client data. Audits will be at client's sole expense, except where the audit reveals material non-compliance with contract specifications, in which case the cost will be borne by subcontractor.
Right to Conduct Assessments	Subcontractor will agree to fully cooperate with any due diligence security assessments performed by client and/or any designated representative or vendor. Client will agree to promptly provide accurate and complete information with respect to such due diligence security assessments. If client performs a due diligence/security assessment of subcontractor, the subcontractor will: • Warrant that the services provided pursuant to the Agreement will comply with generally recognized industry standards and as provided in subcontractor's response to the client's due diligence/security assessment questionnaire • Agree to inform client promptly of any material variation in operations from what was provided in subcontractor's response to client's due diligence / security assessment • Agree that any material deficiency in operations from those as described in the subcontractor's response to the client's due diligence / security assessment questionnaire will be deemed a material breach of the Agreement
Industry Standards	Generally recognized industry standards include, but are not limited to, the current standards and benchmarks set forth and maintained by the following: • NIST Special Publications 800-53 Rev.4 and 800.171 Rev. 1, or as currently revised: http://csrc.nist.gov • HIPAA and HITECH • Federal Risk and Authorization Management Program

Requirement	Details
Implementation of Cybersecurity Measures	Subcontractor shall implement appropriate administrative, technical, and physical measures to protect and secure the information systems and non-public information that are accessible to, or held by, the subcontractor. Subcontractor must have, and permit, client to audit via written request, the cybersecurity measures, safeguards, and standards used by the subcontractor, including, but not limited to, policies, procedures, and practices: • Delineating access controls, including multi-factor authentication, to limit access to client's information systems and non-public information accessible to or held by the subcontractor • Using encryption to protect client's non-public information, in transit and at rest, accessible to or held by the subcontractor • Ensuring the security of client's information systems and non-public information accessible to or held by the subcontractor
Records	Subcontractor shall maintain records concerning all cybersecurity events for at least five years from the date of the cybersecurity event or such longer period as required by applicable laws and produce those records upon client's demand.

As described throughout the remainder of this section, Molina will take an active stance in the prevention and identification of data breaches to maintain the confidentiality of records and protect the integrity of our systems against unauthorized access.

b. APPROACH TO PREVENT AND IDENTIFY DATA BREACHES

In today's landscape, data breaches are alarming both for their frequency and the span of their occurrence. ***That is why our parent company has embraced and invested in an advanced and contemporary security model known as Zero-Trust, which, by default, maintains strict access controls that question the presence of even those who already have access to a network, thereby promoting greater security throughout the network.*** Our parent company's rationale for such a significant paradigm shift comes from the realization that the old model to protect healthcare networks by building a "fortress wall and moat" with a hard network perimeter has not worked. For example, adversaries now use techniques such as email phishing to infiltrate otherwise secure networks**.**

Our parent and affiliated health plans have not experienced any major security breaches of their own computing environments.

Additionally, our parent has taken steps to increase the governance over cybersecurity and elevate issues associated with these risks. A dedicated board-level Cybersecurity Committee oversees management's cybersecurity and IT risk efforts. The committee meets on a semiannual basis and requires the attendance of our parent's chief information officer and a formal written assessment by their chief information security officer.

HOW WE WILL PREVENT AND IDENTIFY DATA BREACHES

Employee Awareness. Molina strongly believes the best way to prevent security incidents is to ensure that our employees are trained and aware of the threats and risks we face within our industry. Our company-wide security awareness and education training program includes but is not limited to, new hire training, onsite presentations, security awareness website(s), and timely hints to detect threats and risks. Every quarter, a fake phishing email is sent to every employee, and click-through rates are monitored with repeat offenders required to complete phishing training. The PhishMe tool is used to manage this awareness campaign, which allows our organization to compare our performance against other healthcare organizations that have completed the same phishing email campaigns.

© 2020 Molina Healthcare of Kentucky, Inc.

Policies and Standards (NIST CSF and 800-53). Enterprise wide, we promote policies and standards that have been mapped to NIST 800-53 and state regulations such as the NY DFS cybersecurity rule and also mapped to control procedures. These control procedures will be adapted as needed to meet any specific Kentucky Medicaid program security requirements. Employees and contractors will be made aware of their security and privacy obligations (includes HIPAA training) when they commence employment and on an annual basis.

Continuous Security Transformation. Our parent company has undergone a security transformation over the last two years, investing heavily in new contemporary security technologies while confirming the basics are operating effectively. For example, our parent company maintains a non-emergency daily and weekly patch security cycle that strives to keep outstanding patches to no later than 30 days. Also, systems are automatically monitored for their compliance with NIST 800-53 controls and our parent company's chief information security officer and chief information officer have a daily dashboard (CyberGaze) to identify areas of non-compliance or trends. Molina believes transparency on the efficacy of controls implemented is important to combat cyber criminals. Therefore, in addition to making available the annual HIPAA security and privacy assessments for Kentucky Medicaid, as well as an independent Ernst & Young SOC 2 report, we will be committed to sharing relevant security metrics pertaining to the Commonwealth at regular intervals via a dashboard that includes the status of any internal corrective actions.

Cyber Defense and Security Operations. Our centers work together to prevent and identify data breaches 24/7/365. Functioning as a certified threat hunting team, they work continuously to review event logs and audit trails for malicious activities, malware, unauthorized intrusion, and phishing attempts. Additionally, our parent company has invested in a variety of security tools to prevent and detect incidents and potential breaches. The following are examples of our organization's various prevention and detection methods and tools:

- Employee Security Awareness
- Data Encryption and Masking (Vormetric)
- Email Security (PhishMe, SPAM protection, FireEye)
- Two Factor Authentication (Microsoft 2FA, Symantec VIP)
- Azure Cloud Security Model (Azure Security Center, Redseal)
- Privilege Access management and Multifactor (PAM)
- Data Loss Prevention (Symantec DLP)
- Security Information Event Management (Splunk, RSA, Symantec MSS 24x7x365)
- Data Access Gateway—Leakage Protection and Data Governance (StealthBits)
- Database and Data Lake Access Protection (Blue Talon)
- Web Security (Symantec Cloud SOC / Akamai WAF)
- Identity Management (SailPoint, Azure IDaaS)
- Threat and Vulnerability Management / App Security (Nesus Tenable, Whitehat, Fortify)
- Endpoint Security (Symantec Endpoint Protection, Tanium)
- Secure File Exchange (sFTP, Msoft OneDrive, PGP, Secure mail)
- Network Security and Intrusion Detection (SourceFire—IPS/IDS, Palo-Alto Firewalls)

APPROACH TO CYBERSECURITY COMPLIANCE

Molina attests that all our systems and processes will comply with all federal and Commonwealth privacy and security provisions. We will receive, create, access, store, and transmit all health information data in a manner that is compliant with HIPAA standards. Furthermore, all systems and processes will comply with HITECH. If a breach or other security incident occurs, Molina has a tested Security Incident Response plan to mitigate potential Enrollee harm and meet Commonwealth and federal reporting obligations. We will comply with all applicable Commonwealth and federal laws, rules, and regulations governing the handling of Enrollee privacy and PHI. ***The Molina EDI Gateway complies with all EDI and HIPAA requirements for data transfer and acquisition.*** Highlights of our compliance Molina EDI Gateway include:

- **Compliant Security Processes and Tools.** We employ advanced security technology and policies to protect our member data enterprise wide, including security and antivirus systems.
- **HIPAA Security and Privacy Training.** We train all employees on PHI, including HIPAA security and privacy, as part of our overall efforts to promote a culture of compliance and awareness.
- **Business Continuity and Disaster Recovery.** We have established processes, policies, and procedures to recover IT systems and operations after a declared disaster event. To review a draft of our plan, see Proposal Section E., Emergency Response and Disaster Recovery Plan.
- **Periodic Audits.** We engage in annual internal and external audits and several state audits that oversee IT controls for administrative, physical, and technical security. We also leverage those audits to identify areas to improve both our security and our operational posture.
- **5010 and ICD-10 Compliance.** We are 5010 and ICD-10 compliant.

Our Compliance Record

- We comply with NIST 800-53, HIPAA, state regulations, and PCI.
- We make available to state partners an independent SOC 2 AIPCA report in which Ernst & Young attests to systems control efficacy.
- We have a record of being compliant with state and federal regulations; most recently, we satisfied the NYDFS Cybersecurity Regulation.
- We encrypt all PHI at rest.
- We require two-factor authentication.
- We require third parties to comply with security requirements: approximately 215 vendors have been audited in the last twelve months.

Our management information system will allow access to all Enrollee health information in a secure and confidential manner. To ensure the accuracy of Enrollee information, we have engineered and implemented an eligibility data management methodology and technology solution for the resolution of discrepancies that may exist between Enrollee eligibility files and internal Enrollee records.

We also apply security measures across our health plans and applications. For example, our affiliated health plans' members must register to log into our member Web portal and, once registered, are provided with a unique username and password. Members are only able to see their health information after logging on. Furthermore, once a member has logged on, our Web portal features a local session timeout that requires reauthentication after a period of inactivity.

© 2020 Molina Healthcare of Kentucky, Inc.

c. APPROACH TO CONDUCTING APPLICATION VULNERABILITY ASSESSMENTS

Molina's Application Vulnerability Management Process meets the Department's Application Vulnerability Assessment requirements as defined in Draft Contract, Section 38.6, Application Vulnerability Assessment. With oversight by our Security Team, our vulnerability management process will detect, report, and respond to security vulnerabilities within the organization and effectively remediate identified security vulnerabilities timely. Our approach is predicated on the inclusion of a security testing process within the Azure DevOps Continuous Integration / Continuous Deployment (CI/CD) pipeline, which we call SecDevOps. SecDevOps automates the previously manual security testing of developed code and deployment of hardened servers/infrastructure. We use a variety of specialized tools to test the security of our applications: WhiteHat Dynamic Application Security Testing (DAST) scans, MicroFocus Fortify Static Application Security Assessments of all applications custom code (SAST), and Black Duck Structured Composition Analysis of the developed code (open source review). We also use third-party security assessment vendors to confirm systems are secure from unauthorized access or disclosure. Additionally, all Internet-facing systems are scanned daily on a rotational basis, and a comprehensive weekly security scan is performed for all Web portals. Any identified issues are prioritized and remediated in a timely manner, usually within two weeks for non-critical issues.

SecDevOps—Application Security

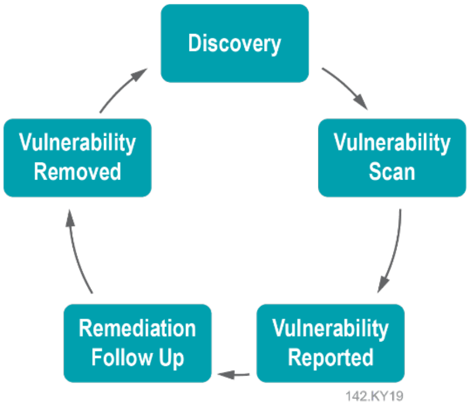
- All applications are security assessed.
- Vulnerabilities are fixed before applications are deployed.
- Build Security In Maturity Model (BSIMM) coupled with CMMi is used to benchmark maturity.

ANNUAL INCIDENT RESPONSE EXERCISE

Annually, Molina will undergo an incident response exercise conducted by a third party. We will work with the Commonwealth as needed to identify incident escalation and emergency response protocols beyond Molina's standard procedures. We will welcome the opportunity to conduct simulated incident response exercises with the Commonwealth and partners.

Our Partnership with the Commonwealth of Kentucky. We believe that cybersecurity, privacy, and disaster recover / business continuity planning will be stronger when we share best practices with our affiliated health plans, state partners across the enterprise, and providers. In coordination with the Commonwealth, we will welcome an opportunity to tailor an engagement plan to share best practices, solutions, and ideas and facilitate subject matter expert discussions through webcasts and hosted in-person symposiums.

Our Approach to Data Protection. Given that a key risk area will be the protection of our Enrollees' PHI, we will implement a series of prevention and monitoring controls to protect data while in motion and at rest. For example, a data loss prevention tool (Symantec) will monitor and block PHI that is not encrypted from leaving the network via email or other protocol. Other tools such as Vormetric will encrypt data at rest in databases, and masking tools such as Blue Talon and Delphix masking solution will mask data from individuals who should not be able to view PHI. PHI at rest within non-production environments will be masked, and no PHI data may be used for testing or development outside of production-ready environments where encryption and access controls have been deployed. Our organization has also implemented an advanced data access gateway solution that manages access to unstructured data repositories such as directory shares, Microsoft SharePoint, and Microsoft OneDrive. Molina will use the StealthBits tool to perform user behavior machine learning (UEBA) to understand and block unusual access to PHI.



Page Intentionally Left Blank

© 2020 Molina Healthcare of Kentucky, Inc.