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."

We have methods and safeguards to maintain medical records standards. We require participating providers and subcontractors to maintain clinical and medical records in a manner that is current, detailed and organized and, which permits effective and confidential patient care and quality review in compliance with Attachment C – Draft Medicaid Managed Care Contract, Section 38.0 Records Maintenance and Audit Rights.

Our medical record policies and practices (P&Ps) are consistent with 42 C.F.R. 456 and the current NCQA standards and all other related state and federal laws for medical record documentation. We have well-established internal P&Ps that comply with medical record documentation standards articulated in this contract, Kentucky law and applicable federal laws and regulations.

Through a contractual agreement, we require our network providers to maintain medical records in a detailed and comprehensive manner, which conforms to good professional medical practice, permits effective professional medical review and medical audit processes, and facilitates an adequate system for follow-up treatment. We require medical records to be detailed, organized and accurate, which permits effective and confidential patient care and quality review. We require medical records to be legible, signed and dated.

Records retention procedures will follow the UnitedHealthcare policy on records retention, which is consistent with state and federal laws related to document retention. Training on provider medical record requirements will follow the current process for training and educating providers on record keeping expectations through the health plan and functional partners as we do today and successfully accomplished for more than a decade.

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

Preventing Data Breaches

UnitedHealth Group enterprise information security (EIS) has developed policies and standards to address the requirements for logging and monitoring our environments to prevent vulnerabilities and breaches. UnitedHealth Group's information security operations (ISO) team maintains the operational platforms and procedures for ongoing monitoring and reporting for the information security infrastructure. The EIS security incident response (SIR) team and CD security operations center (SOC) perform monitoring and reporting of security events identified by the devices within the security infrastructure.

UnitedHealth Group's SOC shares responsibility with the SIR team for the overall assessment, response and reporting of cyber-security events. Along with routine reporting, the SOC provides formal procedures for custom and ad hoc reporting. The SOC is responsible for conducting 24 hours a day, seven-days a week monitoring, event triage and analysis. Our SIR and rapid recovery team, coordinate event containment, response and recovery. The Privacy team is part of this process and manages notifications, reporting, and customer and regulatory communications. We are also compliant with Appendix Q. The Cabinet for Health and Family Services Contractor Security Requirements.

We prevent security breaches through our enterprise resiliency program and ongoing vulnerability assessments. The programs encompass ensuring that every employee and contractor sending information from our systems is authorized and trained on HIPAA provisions to safeguard the information they are authorized to obtain, access and use. We will comply with Appendix Q. related to additional security requirements, which also reiterate requirements related to the protection of beneficiary protected and personal health information and resiliency requirements.

Enterprise Resiliency

UnitedHealth Group conducts computer security and privacy incident-response operations under well-defined and formal policies, processes and operating procedures that are documented for consistency and continually updated in response to the changing threat landscape. Our designated security incident response team operates 24 hours a day, 365 days a year to provide oversight for handling security and privacy-related incidents. We appropriately manage reported breaches and thoroughly investigate them by:

- Establishing a discrete network of principal participants, to include our compliance, privacy and security offices with support from EIS staff, counsel and executive leadership, as circumstances warrant
- Identifying a primary incident owner who will facilitate review and investigation of the reported incident with appropriate principles to foster efficient and thorough review of the known facts and to bring the matter to a successful conclusion
- Identifying incident type or root cause (e.g., operational error, system malfunction or malicious intent, by either an internal or external agent), and determine if the incident is a single or global event, which indicates specific procedures for information security incidents, remediation (as appropriate) and related communications
    - Implement response activities or remediation and corrective action plans based upon incident
    - Track the historical response or apply remediation data to reduce risk of repeat occurrences

Our EIS team works in unison with our enterprise resiliency and response team and the local IT team to deploy response mechanisms (including fail-safe procedures) as soon as we become aware of an event that may disrupt our systems. Within minutes of identifying a major threat, we open a bridge line so technical leads can collaborate, understand how the threat may affect our enrollees and stakeholders and determine response options and recovery priorities. The EIS team systematically keeps a log for audit and reporting purposes of access attempts that failed, along with detailed login information such as when the system in question is accessed, by whom and what records are created, viewed, updated, extracted or deleted.

All UnitedHealth Group employees and contractors are required to report privacy and security breaches, whether it involves one individual or affects thousands.

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."

We agree to comply with Attachment C – Draft Medicaid Managed Care Contract, Section 38.6 Application Vulnerability Assessment, to perform a non-intrusive vulnerability assessment on web applications and web services. We conduct both internal and third party penetration tests on externally facing portals on an annual basis. Reports of the penetration tests and identified findings will be provided within 14 days of the audit as required. Our vulnerability testing includes, but is not limited to:

- A. Injection
- B. Broken Authentication and Session Management
- C. Cross-Site Scripting (XSS)
- D. Insecure Direct Object References
- E. Security Misconfiguration
- F. Sensitive Data Exposure
- G. Missing Function Level Access
- H. Cross-site Request Forgery (CSRF)
- I. Using Known Vulnerable Components
- J. Invalidated Redirects and Forwards

We limit access to our network and systems through firewalls, a virtual private network (VPN) and physical separation of processing systems. Firewalls protect our customer service applications. Our firewall defenses observe over 800 million events a day. All enrollee and provider self-service tools accessible through our secure portals are password protected and use secure web protocols (HTTPS).

Proactive Threat Monitoring
Our EIS team has implemented an integrated suite of emerging technologies using machine learning/artificial intelligence and data analytics to definitively assess and proactively monitor entities as they interface with our systems, keeping us at the forefront of threat detection.

Our IT teams work with our national EIS team to protect the confidentiality, integrity and availability of system data. This includes creating, administering and overseeing policies to confirm the prevention, detection, containment and correction of security breaches. **We monitor our systems in real time 24 hours a day, 365 days a year.** The EIS infrastructure services security team uses two network-based intrusion detection technologies to identify the potential risk of security breaches:

- ***Intrusion Prevention System (IPS):*** Allows for “detect” and “deny” action
- ***Intrusion Detection System (IDS):*** Allows for a “detection” action

Configured to detect and protect against malicious traffic, the IPS/IDS systems include real-time alerts and provide detection and prevention of known attack characteristics (e.g., denial of service attacks, worms and viruses) within the scope of all network-based protocols.

We invest significant resources in our information security program, which includes a robust cyber defense program that includes smart cards for computer access, hard drive scanning and remediation for protected information, and phishing awareness. **We also monitor 11 million emails a day from external sources, and we block 90% based upon security.**

This Page Intentionally Left Blank