C.	**Technical Approach**

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."**

Humana understands that consistent, current, and complete documentation in the medical record is an essential component of high quality patient care. For more than 20 years, Humana has conducted medical record reviews across our Medicaid, Medicare, Commercial, and TRICARE lines of business. In 2018, we collectively reviewed 367 medical records and 139 providers across all lines of business to determine their compliance with applicable medical records standards. Similarly in 2019, we reviewed 409 medical records and 179 providers across all lines of business to determine compliance with applicable medical records standards, in addition to our Kentucky medical record compliance reviews. In 2020, we plan to review approximately 400 medical records for compliance with applicable standards. Our experience has allowed us to develop methods to ensure that our provider network is performing at the highest standards possible and in full compliance with the contractual requirements identified in Section 38.1 Records Maintenance and Audit Requirements of RFP Attachment C - Draft Medicaid Contract.

ASSESSING PERFORMANCE AND COMPLIANCE TO MEDICAL RECORD STANDARDS

Medical Record Reviews for Primary Care Provider (PCP)/PCP sites and High-Risk/High-Volume Specialists

We have a standardized review process and record documentation review tool to assess performance and compliance to medical record standards for PCP/PCP sites and high-risk/high-volume specialists. Our Humana Quality Operations Compliance and Accreditation (QOCA) department conducts medical records reviews annually and uses the audit tool to review randomly selected groups of providers. We check provider files for compliance with medical record standards and guidelines. We also conduct medical record audits at any provider site with a pattern of complaints or poor quality outcomes. The medical record review tool includes review of the following medical record elements:

Table I.C.28-1 Medical Record Review Elements

Element	Description
Patient Identification	Gender, Date of Birth (DOB), Patient ID card, and Patient name
Provider Identification	Name, National Provider Identification (NPI), Tax ID
Dates	All medical entries must be dated
Legibility	The medical record must be legible to someone other than the writer
Allergies	Must be documented in a uniform location on the medical record. Medication and other adverse reactions must be listed if present.
Past medical history	For patients seen three or more times, past medical history should be easily identifiable and include serious accidents, operations, illnesses, and familial/hereditary disease

Table I.C.28-1 Medical Record Review Elements

Element	Description
Completion of a Physical exam	All body systems should be reviewed within two years of the first clinical encounter, including head, eyes, ears, nose and throat (HEENT), lungs, neck, heart, neurology, back, and extremities. Height, weight, blood pressure, and temperature must be documented on the initial visit.
History and physical	Subjective and objective information should be obtained and noted regarding the presenting complaints
Working diagnosis	The working diagnosis should be consistent with findings (i.e. the physician's medical impression)
Records	These include consultation, discharge summaries, and emergency department (ED) reports. All reports are required to be filed in the medical record and initialed by the PCP, thereby signifying review. Past medical records and hospital records (e.g., operative and pathology reports, admission and discharge summaries, consultations, and ED reports) should be filed in the medical record.
Authorizations(e.g., consultation, therapy)	Authorizations should be filed in the medical record
X-ray/lab/imaging	Records should show documentation of lab, X-ray, imaging, or other studies ordered. Results should be filed in the medical record and initialed by the PCP thereby signifying review. Abnormal X-ray, lab, and imaging study results should have an explicit notation in the medical record regarding follow-up plans and notification to patients of all results (positive and negative).
Smoking	For patients seen three or more times, a notation concerning cigarette use must be present
Alcohol	For patients seen three or more times, a notation concerning alcohol use must be present
Substance abuse	For patients seen three or more times, a notation concerning substance abuse must be present
Immunization record	A current record of immunizations should appear in the patient chart
Advance directives	For patients ages 21 and older only, there should be evidence that the patient has been asked if he or she has an advance directive (written directions about healthcare decisions), and a yes or no response should be documented. If the response is yes, a copy of the advance directive must be included in the medical record.

The purpose of the QOCA's medical record audit is to assess compliance with adopted medical record documentation guidelines and evaluate physician adherence regarding those guidelines. QOCA checks that at minimum, the record complies with the standards set forth by the State and any other federal regulatory standards. The minimum passing score is 85% compliance with the guidelines, with a goal of 90%. We communicate the score to the provider along with any recommended corrective actions in an effort to improve performance. We make these medical record guidelines available online for our providers. They may also request a printed copy at any time. We include aggregate results of the audit in our annual Quality Improvement Evaluation (QIE).

All information, records, and data collected by Humana, including medical records, are protected from unauthorized disclosure as provided in 42 C.F.R. Section 431, subpart F, KRS 194.060A, KRS 214.185, KRS

434.840 to 434.860, and any applicable State and federal laws, including the laws specified in Section 40.15 of the Health Insurance Portability and Accountability Act (HIPAA). However, Enrollee medical records and other service records are available to the Department for Medicaid Services (DMS) upon request. Authorized representatives of DMS, the Office of the Inspector General, and other authorized Commonwealth and federal agencies can access physical facilities, equipment, and records for financial and medical audit purposes both during and after the term of the provider contract. All Enrollee medical records and other service records are available to DMS upon request. Authorized representatives of DMS or other Commonwealth and federal agencies can access physical facilities, equipment, and records for financial and medical audit purposes both during and after the term of the provider contract.

Medical Record Reviews for Dental Providers and Providers of Ancillary Services

For dental providers and providers of ancillary services (i.e., subcontractors), we assess performance and compliance with medical record standards and guidelines through our delegation compliance audit tool. Our oversight activities of delegated entities, including our dental partner Avēsis, consist of **onsite visits, audits, and reviewing required reports and all relevant documentation** related to specific delegation functions for compliance to Humana, regulatory, and accreditation standards. Oversight of delegation activities is an ongoing process.

Humana's Subcontractor Oversight Committee (SOC) maintains a comprehensive, collective view of performance across the approved Kentucky subcontractors, with specific focus on oversight and monitoring activities and key performance matters of interest. The SOC provides oversight of services provided by DMS-approved Kentucky subcontractors through a comprehensive, plan-wide system of ongoing, objective, and systematic monitoring. The SOC ensures that delegated services meet the Contract standards for care and customer service, including reporting. The SOC's responsibilities also include but are not limited to:

- Establishing appropriate oversight mechanisms, procedures, and tools
- Overseeing delegated services by reviewing subcontractor activity, performance metrics, and reports
- Reviewing pre-delegation and annual delegation audit findings through monthly summary reporting
- Monitoring progress in the resolution of Corrective Action Plans (CAP) as appropriate
- Performing annual evaluation of the monitoring and oversight program and recommending enhancements
- Completing a self-evaluation annually, with feedback by the Quality Improvement Committee (QIC) and market leadership, to ensure it remains current and relevant including the program structure, scope, and effective leadership

We forward summaries of subcontractors' performance to the Kentucky QIC each month and present matters meriting broader engagement to the Executive Steering Committee quarterly. Humana maintains and retains accurate records of such monitoring activity for a minimum of 10 years.

IMPROVING COMPLIANCE WITH MEDICAL RECORD STANDARDS AND GUIDELINES

Contracting

To promote provider compliance with medical record standards, Humana includes specific language in all provider contracts regarding adherence and compliance with both State and National Committee for Quality Assurance (NCQA) medical record standards. Included in our contract language are mandatory provisions acknowledging that we will audit provider records for medical record compliance. Additionally, our provider contracts include requirements to ensure that medical records are transferred appropriately, accurately, and in compliance with the Draft Medicaid Contract when an Enrollee changes their PCP.

Provider Education

Humana includes medical record documentation training in our standard onboarding training, as well as annual refresher training courses. Providers access education through their Provider Relations representatives, using our online and self-service resources or through our written materials, such as the Provider Manual. We will leverage the provider and Provider Relations representative relationship to ensure that all providers in our network are able to adhere to the expected medical records standards mandated by State and federal guidelines.

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

ROBUST SYSTEM CAPABILITIES

Humana has an established **Enterprise Information Protection (EIP) Program** and supports numerous Humana policies and standards addressing Enterprise Information Protection and Security, including the protection of human capital; company assets; and Humana internal, restricted, and confidential information. Humana has a key policy document, "Policy – Enterprise Information Protection," that provides the framework for Humana Information Protection. Using this key policy and all of Humana's EIP policies and standards, Humana identifies, minimizes, and manages risks and vulnerabilities to the enterprise while also establishing safeguards to maintain the confidentiality, integrity, availability, and accountability associated with information and assets. Humana follows all federal and State laws and regulations. Our EIP forms an umbrella of protection for our Enrollees, associates, and business partners. EIP promotes information security by:

Humana devotes significant resources to information security. [redacted]

- Hiring and retaining more than 350 highly educated, dedicated security associates
- Creating, updating, and streamlining security processes
- Purchasing and maintaining current security software and hardware for physical, administrative, and technical controls that protect the confidentiality, integrity, and availability of our interests and those of our Enrollees

Humana's overall EIP strategy is based on **managing real risks** as the primary means to drive meaningful compliance to a myriad of government- and customer-driven requirements. This ensures that we can proactively prevent and identify data breaches. Our approach includes the following components, which we discuss in detail in the narrative that follows:

1. Information protection
2. Security audits
3. Penetration tests
4. Administrative safeguards
5. Physical safeguards
6. Network and system safeguards
7. Endpoint protection
8. Portable media security
9. Mobile device security
10. Wireless security

1. INFORMATION PROTECTION

To protect the confidentiality, integrity, and availability of Humana resources, we have created the **Humana Integrated Control Framework (HICF)**, a collection of control objectives and guidance. It is primarily based on the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), which consolidates numerous regulations, industry standards, and best practices to create, access, store, or exchange Protected Health Information (PHI) safely and securely. Humana will use and disclose PHI in compliance with the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") (45 C.F.R. Parts 160 and 164) under the HIPAA. Some of the regulations and standards that are consolidated include ISO 27002, HIPAA, Payment Card Industry Data Security Standard (PCI DSS), Centers for Medicare and Medicaid Services (CMS), and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF).

Dedicated Information Security Personnel: Aman Raheja is Humana's designated Chief Information Security Officer (CISO). Mr. Raheja, a Senior Vice President in the company, has more than two decades of experience in information security and Information Technology (IT). He collaborates closely with leadership across the enterprise in addressing information protection. Mr. Raheja oversees Humana's Information Protection Security strategy, policy, risk, governance, and compliance and is the leader of the EIP organization. As CISO, his responsibilities include the following:

- Managing risk to protect confidentiality, integrity, and availability of Humana's information assets
- Setting governance, risk, compliance, and policy
- Ensuring enforcement of security policies
- Evaluating compliance with State and federal regulations
- Integrating information protection into operations and culture

Mr. Raheja meets with the Humana Board of Directors at least twice a year and with senior leadership at least monthly.

Humana's EIP establishes and aligns to best practices, regulatory, federal/State, and international laws where applicable in an effort to mitigate risks and protect the business needs of the organization. One component of the Information Protection Program is policy management. Leadership approves these policy documents, which we publish and communicate to all associates and relevant external parties. **We review Information Protection Policies and Standards annually** or if significant changes occur to ensure their continuing adequacy and effectiveness. EIP policies, standards, and procedures are accessible to Humana associates on the Humana intranet.

Training on Information Security: **Humana's Annual Ethics and Compliance training for associates and contractors** consists of mandatory annual web-based training that must be completed within 30 days of hire and annually thereafter. We track annual web-based training for every associate. Topics include but are not limited to:

- Privacy and Information Protection Policies including the Acceptable Use Policy
- Role of EIP and the Privacy Office
- Key definitions and concepts and social engineering tactics such as phishing
- Physical safeguards
- Security incident and privacy breach reporting

As part of the annual mandatory training, all associates and contingent labor must also agree to the terms of the **Individual Information Security Agreement**. To remind associates of their responsibilities and upcoming security and compliance events, we use the following communication tools:

- Periodic postings using electronic message boards strategically placed in lobby areas
- Monthly emails sent to the enterprise
- Enterprise-wide, semi-monthly lunch-and-learn series
- News articles posted on the company's intranet

We also distribute specific communications prior to launching major security and compliance initiatives to apprise associates and subcontractors of changes and to raise awareness of these objectives.

In addition to the communications and trainings, **Humana holds an annual Cyber Security Awareness event** each October for the enterprise. This event is a weeklong focus on all things "information protection." Renowned information security experts share their knowledge throughout the week with presentations, expo halls, and interactive activities.

2. SECURITY AUDITS

Humana undergoes numerous internal and third-party security audits each year. We describe the results of our latest security audits below:

- Health Information Trust Alliance (HITRUST): As of July 2018, after an extensive audit, Humana was certified by third-party HITRUST auditors as being compliant with the HITRUST Common Security Framework (CSF). Humana completed the HITRUST Interim Review in 2019 and has received an interim letter stating that we continue to meet the requirements of the HITRUST CSF v9 Certification Program Criteria.
- Payment Card Industry Data Security Standard (PCI-DSS): Humana was also audited by third-party auditors and certified to be compliant with PCI DSS in December 2019.
- System and Organization Controls (SOC 2 Audits): Humana successfully completed a SOC 2 Type 1 point in time assessment earlier in 2019, and we are currently working on achieving SOC 2 Type 2 compliance by the first quarter of 2020.

Certificates of compliance mentioned here are available for review upon request. Humana is SOC 1 compliant, but this certification can only be provided to those companies that meet certain requirements (details of which we can provide upon request). Humana additionally participates in multiple State Department of Insurance (DOI) audits each year.

3. PENETRATION TESTS

Humana undergoes annual penetration (pen) testing to ensure that our cloud security meets the highest industry standards. Pen testing is a simulated real-world attack on a network, application, or system that identifies vulnerabilities and weaknesses and is part of an industry-recognized approach to identify and quantify risk. Pen testing actively attempts to exploit vulnerabilities and exposures in our infrastructure, databases, and applications so that we can develop effective countermeasures. The specific objectives of **Humana's EIP Pen Testing Program** are to:

- Identify Humana's cyber surface and potential threat surface
- Reduce the number of exploitable vulnerabilities in the Humana environment
- Provide Humana leaders with metrics and transparency around pen testing
- Meet customer contract requirements for pen testing
- Meet federal and State regulatory requirements for pen testing
- Perform cyber-attack simulation exercises

The pen testing program includes ongoing testing based on risk as well as pre-production testing of solutions to provide feedback prior to moving into production. In 2019, we completed 30 production pen tests, 58 pre-production pen tests, and two red team exercises.

4. ADMINISTRATIVE SAFEGUARDS

Humana's information security policies, standards, and procedures begin with the high-level "Humana Information Protection Policy," which is our keystone document for administrative safeguards to information protection. We have continued to develop more specific and defined documents to address the details provided in this keystone policy. Policy Source is Humana's portal for associates to obtain and review policies, standards, and procedures. Each EIP document contains the date it was created and the date that it was last updated. All such documents are required to be updated on an annual basis; we also store older versions to meet the strictest retention standards.

Humana's policy, standard, and procedure structure is based on ISO 27001, PCI, HIPAA, NIST, and HITRUST CSF requirements. This enhances the organization of our documentation, eases maintenance, and makes it easier for associates to find documentation dealing with topics of concern. Many of our administrative safeguard documents deal with access control and areas relating to access control, including granting of access, password management, and access removal after termination and transfers. **Humana has an Identity and Access**

Management team that continues to enhance and mature our already robust access management controls and safeguards.

Humana's EIP structure includes a Crisis Management team, Business Continuity (BC) Planning team, and a Disaster Recovery (DR) team supporting further administrative safeguards including but not limited to **contingency planning, continuity planning, disaster recovery, and backup and restoration of information**. These teams ensure these safeguards, plans, and documents are continually updated and tested throughout the organization.

5. PHYSICAL SAFEGUARDS

Humana's Safety and Security Fusion team governs physical security of Humana facilities and assets. This team creates, documents, and employs safeguards that secure Humana workplaces (including our data centers), protects company assets (including PHI and other protected information), and helps foster an environment where associates, contractors, and visitors feel comfortable and safe.

Humana uses electronic access controls for controlling physical access to our data center facilities.

We require facilities to maintain an electronic or manual system of positive associate and visitor identification and logging; some facilities have biometric access controls. Personnel are required to wear photo identification badges, which are color-coded to indicate access authorization levels, while on Humana premises. **Unescorted access is generally prohibited for all but Humana associates**, with very stringent requirements for any exceptions. Our data center facilities are equipped with access control and alarm systems. We also **use digital closed-circuit (CCTV) systems at ingress and egress locations** to enhance the physical security. Data from the CCTV are kept for a risk-appropriate period of time.

Humana continually references and adapts to forward-looking regulatory impact studies to ensure we are on the forefront of innovation, safety, and security.

6. NETWORK AND SYSTEM SAFEGUARDS

ROBUST SYSTEM + CAPABILITIES +

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

7. ENDPOINT PROTECTION

Endpoint protection is a system for network security management that focuses on network endpoints or individual devices from which a network is accessed. Endpoint protection is important to Humana as it allows for the secure use of mobile devices, laptops, workstations, and other devices that hold sensitive company data. **At Humana, we implement detection, prevention, and recovery software on all devices to protect against malicious code**. We have policies, procedures, and standards that document the controls we have in place for endpoint protection. We also include user awareness procedures on reporting possible malicious code as part of our mandatory annual Ethics and Compliance training.

Humana equips all associate and network computers (personal laptops and desktops) with software that prohibits authorized users from making connections to the public internet without first connecting to Humana's secure network. We leverage **Digital Guardian Endpoint Data Loss Prevention (DLP) software**, which prevents sensitive data from getting out of our systems at the endpoint. The DLP software can capture and record all system, user, and data events on or off the network, facilitate file transfer and/or file upload blocking, etc. We additionally have **software that monitors emails for classified information and will prevent it from leaving our network unless it is transmitted securely**. Humana also encrypts the data on all laptop hard drives along with all the traditional protections like anti-virus, software firewalls, etc. These additional endpoint levels of technical real time enforcement controls on all Humana personal computers also provide protections against unauthorized access and data leakage risks that Wi-Fi use may introduce or in the event where a laptop may be lost or stolen.

Humana uses security products that offer protection for the endpoint and are required to be on all desktops and laptops to include solutions for:

- Virus protection
- Encryption to meet Safe Harbor
- Data loss prevention (provided by Symantec)
- Excessive privileges and password controls

We also use several network-based tools that offer protection for the endpoint, including:

- Web proxy/filtering
- Vulnerability management
- IDS and IPS (provided by Cisco)
- Web application firewall (provided by Akamai)
- Virtual private networks (VPN) with strong authentication
- VirusScan Enterprise (VSE) + Anti-Spyware (provided by McAfee)
- Spam filtering (provided by Barracuda)

At Humana, we monitor and log all security events at the system, application, and data levels. We review logs on a risk-appropriate basis and update data files for anti-virus protection daily. Our Cyber Security Operations Center (CSOC) is alerted whenever a malicious code is detected by any of the above systems. Malicious code protection mechanisms are centrally managed and locked from user disablement.

8. PORTABLE MEDIA SECURITY

Humana has policies and standards in place that describe how assets, including portable media, are protected and securely wiped before reuse or securely destroyed at the end of their usefulness. We identify, own, and actively manage assets associated with information processing internally. This holds individuals within the organization accountable for the protection of information assets. We identify all assets with a financial or security impact and maintain an inventory of those assets. An asset inventory includes all information necessary in order to recover from an interruption to business.

In order to advance Humana's overall business reporting, business intelligence, and analytical capabilities, **we govern and treat information as a corporate asset**. Types of information assets include, but are not limited to, the following:

- Information: Databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, event logs, and archived information
- Software assets: Application software, system software, development tools, and utilities, irrespective of deployment location
- Physical assets: Computer equipment, communications equipment, removable media, and other equipment that access, view/display, store, process, or transmit electronic information
- Virtual assets: Virtual devices, servers, containers, templates, and machine images
- Services: Computing and communications services, general utilities, e.g., heating, lighting, power, and air conditioning

We label, encrypt, and handle media according to its classification. The table below shows an overview of our information classifications:

Table I.C.28-2 Humana Information Classifications

Public	Information that is not business sensitive and is available for public release. This classification includes advertising materials, public/press announcements, SEC filings, etc. Humana internal assets consist of information that is generally available to Humana associates but not for public disclosure.
Humana Internal	Assets include organization charts, internal announcements, project information, etc.
Humana Restricted	Consists of proprietary information such as sensitive company information intended for use by named individuals or department and intellectual property. Includes copyrightable works, patented inventions, trademarks, trade secrets, etc.
Confidential	Consists of confidential protected information that includes Enrollee, patient, provider, third party and private person information protected by State or federal regulations. Humana confidential information includes Individually Identifiable Health Information (IIHI), electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), and Personally Identifiable Financial Information (PIFI). This asset category includes Enrollee information, prospective Enrollee information, as well as health information, financial information, Social Security numbers, DOB, and Payment Card Industry (PCI) data.

Humana uses a regulatory-compliant and EIP-approved encryption algorithm with minimum bit strengths (256 bit minimum) to protect confidential information including but not limited to ePHI, PCI data, and Personal Information (PI), and/or Humana restricted information. Humana uses **encryption for the protection of confidential or Humana restricted information transported by mobile or removable media, devices, or across communication lines**.

We dispose of ePHI or electronic data storage media in such a manner as to confirm the data have been completely removed and the device has been irreparably destroyed or damaged (e.g., burning, crushing, melting, shredding, cutting, etc.).

Humana follows its “Records Retention Policy” and schedule that states the period to retain its information. The Humana Legal department regularly issues legal holds that suspend the time set forth in the Records Retention Policy and schedule. This requires Humana to retain some electronic and paper documents, information (PHI and ePHI) for an extended period on the Information Systems from which they are produced, or stored securely for paper documents.

Humana uses overwriting of media storage devices (an industry-recognized and effective sanitization practice) for removing Humana internal, Humana restricted, or confidential data. We also use meaningless data characters or character strings to overwrite all memory storage areas on the media, which we typically do more than once and then combine with data erasure or deletion steps to complete the sanitization process. We use the degauss procedure, the process of decreasing or eliminating a remnant magnetic field, to confirm the sanitization of the media device.

9. MOBILE DEVICE SECURITY

While associates use handheld mobile devices within the company to enhance business efficiency, Humana controls and restricts the use of portable devices. We have set secure data transmission policies and procedures where authentication and authorization are required and based on Humana standards. **All Humana non-public data are encrypted within mobile applications**.

Humana requires that associates use only trusted IT systems and devices or Humana secured remote access services when sending, uploading, receiving, or downloading Humana internal, Humana restricted, and confidential information. Humana associates must use secured remote access services with laptop devices: Citrix (Launchpad), Array (myPC), or an approved platform for mobile devices such as BlackBerry Work.

Humana installs, updates, and modifies as needed security-related software, business applications, agents, or tools on Humana-provided and trusted devices as a condition of participation. Untrusted devices do not have Humana’s standard security safeguards. The user is responsible to ensure that the device has all necessary system updates and must regularly check for updates to stay current. We require users to take all necessary precautions to prevent theft and vandalism of Humana-provided or Humana-managed devices.

Humana requires that lost, stolen, suspected cloned devices, or personal devices with the BlackBerry Work containerized application be reported to our internal IT department, Customer Systems Support (CSS). To maintain the privacy and security of Humana information and systems, **Humana can remotely disable Humana-provided devices or remove data** within the BlackBerry Work and Microsoft Intune containerized applications.

Humana automatically requires that users select a secure method for sending externally-bound email messages containing Humana internal, Humana restricted, or confidential content, which may be included in the subject line, body and/or file attachments of the email, to authorized individuals or entities out of Humana's protected computing environment. **Secure Mail in Microsoft Outlook** is the preferred method. Data allowed to leave the Humana internal network are controlled, tracked, and contained using security control methods. If data are approved to be transferred to an external system, appropriate contractual, administrative, and technical controls must be in place to protect the data and indemnify Humana.

Authorized users of Humana computer systems, networks, and data repositories are permitted to connect remotely to systems for conducting company-related business only through secure, authenticated, and centrally-managed access methods. **All remote user access requires Level 2 (“Strong”) authentication or Level 3 (“Multi Factor”) authentication as defined by the NIST Special Publication 800-63-2**. Humana monitors and logs all remote access and control connections, identifying the person conducting the activity. We monitor and review unauthorized remote access or failed access attempts 24 hours a day, seven days a week based on security events presented via Humana’s Intrusion Detection/Prevention System (IDPS).

10. WIRELESS SECURITY

Humana works earnestly to maintain and update DiD controls to ensure that we achieve and preserve an optimal security posture. Wireless technologies are open to traditional wired network attacks and unique threats due to the nature of the medium leveraged to transmit information.

At Humana, we encrypt all wireless transmissions in accordance with Humana policies, standards, and industry best practices. Secure authentication between the wireless clients and the access points (AP) is controlled by **WPA2 Enterprise (Wi-Fi Protected Access)**. Humana limits the wireless infrastructure attack surface by implementing **Wireless Intrusion Prevention System (WIPS)**, which we tune and update on a quarterly basis.

Humana has implemented Rogue Mitigation to prevent Rogue APs from operating within Humana's Radio Frequency (RF) "umbrella." Humana actively monitors Humana facilities for Rogue APs. Any Rogue AP is reported to the Humana EIP-Forensic Security Investigations Group and is investigated as a security incident.

Humana defends against "Evil Twin" or "Watering Hole" attacks by actively preventing wireless clients and access points from associating. Humana continuously monitors user access controls to the wireless infrastructure. For additional security, we modify the default username for administration of wireless access to reflect a non-descriptive account name that cannot be differentiated from others as the powerful admin account.

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."**

CONDUCTING VULNERABILITY ASESSMENTS

Humana's EIP program conducts vulnerability assessments for applicable threats and assigns an initial risk rating. The risk rating takes into consideration many factors, such as the attack vectors used, whether exploits are available, the criticality of vulnerable systems to Humana, and the current state of mitigating controls. We communicate vulnerability and risk treatment information to SMEs and IT owners responsible for remediation. Our network appliances, servers, and workstations are managed (patched) by technologies used by various IT teams within Humana. The patch solutions use auto-discover assets, install patches, and track deployment progress. Our EIP program tracks remediation progress by reviewing reports provided by the IT teams and validates remediation through vulnerability scanning tools.

We conduct our vulnerability assessments using a non-intrusive gray-box approach to discover if access can be discovered, programming flaws, data leakage, and information that could allow an intruder to attack the web applications. We scan web applications and web services without credentials to identify vulnerabilities related to the Open Web Application Security Project (OWASP) top 10 vulnerabilities and SysAdmin Audit Network Security (SANS) top 25 programming errors. These vulnerabilities include:

1. Injection
2. Broken authentication and session management
3. Cross-site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access
8. Cross-site request forgery (CSRF)
9. Using known vulnerable components
10. Invalidated redirects and forwards

ROBUST SYSTEM + CAPABILITIES +

Humana uses the Qualys vulnerability scanning tool to scan all systems including Windows servers, Windows workstations, Unix/Linux assets, AIX assets, and network devices. We perform both internal and external scans weekly. Qualys is used to perform scheduled authenticated and unauthenticated scans of assets discovered and identified on all Humana internal and external networks. We send reports of vulnerabilities to stakeholders for review and remediation based on Operational Level Agreements (OLA).

VULNERABILITY MANAGEMENT

Humana requires that IT assets be proactively monitored for technical vulnerabilities. We remediate identified vulnerabilities in a timely fashion to reduce the likelihood of a threat agent successfully exploiting vulnerability. Humana maintains technical vulnerability-related policies and standards (available upon request) that include but are not limited to:

- Information asset management
- Application security administrative
- Information systems acquisitions, development, and maintenance
- Technical vulnerability management
- Information security incident management and response

Humana has implemented a **Technical Vulnerability Management (TVM)** program to maintain a consistently configured environment that is secure against known vulnerabilities in operating systems, databases, applications, and network devices and to reduce the risks resulting from exploitation of technical vulnerabilities.

Humana's TVM plan includes the following processes:

- Discovering and identifying assets on all Humana internal and external networks
- Categorizing assets by technology and/or type of asset
- Conducting vulnerability scans on a regular schedule using both authenticated and unauthenticated scans to identify vulnerabilities
- Reporting vulnerability information to TVM stakeholders
- TVM stakeholders evaluating and remediating the vulnerabilities, using the OLA to assist with prioritizing the remediation
- Validating the remediation of vulnerabilities by regularly-scheduled vulnerability scans

Humana's TVM team monitors security sources for threat intelligence to identify newly-discovered security vulnerabilities and their corresponding patch and non-patch remediation and emerging threats that correspond to the software with the asset inventory. On an ongoing basis, Humana develops and updates standards for all main system components that include but are not limited to workstations, databases, applications, servers, and computer network devices. Configuration standards are hardened to address, to the extent practical, all known security vulnerabilities and are consistent with industry-accepted system hardening standards including but not limited to:

- The Center for Internet Security (CIS)
- The International Organization for Standardization (ISO)
- NIST
- SANS

We risk rank any newly discovered technical vulnerabilities, with consideration given to the **Common Vulnerability Scoring System (CVSS)** score assigned to the vulnerability, classification of the subcontractor-supplied patch, number of affected IT assets and their assigned criticality and/or classification ranking, and the existence of security controls (preventive, detective, and corrective).