Anthem

Cybersecurity Assessment

4/20/2025

Jocelyn Peguero, Avery McLean, Tim Klein, Ethan De Jong

Table of Contents

Company Profile (Avery McLean & Jocelyn Peguero)

One of the biggest health insurance companies in the US, Anthem (Elevance Health Inc.) provides coverage and medical services to millions of people and businesses. Anthem depends on safe, effective, and scalable cybersecurity solutions to safeguard patient data and uphold regulatory compliance due to its extensive network of healthcare providers and digital health services. Electronic health records (EHR), claims processing systems, telemedicine platforms, and fraud detection tools are all part of the company's vast digital infrastructure and are essential to its operations and patient confidence.

Within the healthcare industry, Elevance has prioritized its company strategies: whole health, exceptional experiences and care, and providing digital solutions for all its consumers. The ability to provide several services and promote accessibility to healthcare serves its community. When engaging in the industry, organizations are expected to conduct business with regard to the impact on stakeholders, customers, etc. Elevance has the leverage to touch multiple states, improving healthcare services, quality, and availability. Elevance has created many different products and healthcare initiatives to provide quality care and promote the overall health of the community. Within the healthcare industry, Elevance has prioritized its company strategies: whole health, exceptional experiences and care, and providing digital solutions for all its consumers. The ability to provide several services and promote accessibility to healthcare serves its community. When engaging in the industry, organizations are expected to conduct business with regard to the impact on stakeholders, customers, etc.

Overview (Avery McLean & Jocelyn Peguero)

Anthem needs a thorough cybersecurity plan to protect its vast digital infrastructure, which includes electronic health records, telemedicine services, and claims processing systems. While maintaining compliance with laws like HIPAA, the business must handle serious dangers like ransomware, data breaches, and insider threats. Protecting patient data and preserving operational resilience requires a proactive strategy that includes risk assessments, ongoing monitoring, and strong mitigation techniques. Anthem confronts major cybersecurity difficulties because of the high sensitivity of healthcare data and the growing sophistication of cyber attackers. Its approach must be in line with the NIST Cybersecurity Framework in order to reduce risks, preserve regulatory compliance, and preserve stakeholder trust. To strengthen Anthem's defenses against cyberattacks, this study identifies important assets, addresses possible risks, and suggests tactical cybersecurity solutions. This report identifies key assets, outlines associated risks, and highlights cybersecurity solutions.

Asset Ranking (Avery McLean & Jocelyn Peguero)

1. **Electronic Health Records (EHR) System** – Most critical due to sensitive patient data and high frequency of ransomware attacks.

2. **Claims Processing System** – Contains private health and financial information; significant regulatory impact if breached. Accurate data and information may aid in legal implications and court proceedings.

3. **Data Analytics Platform** – Integrity issues could mislead operations, regulatory compliance, and financial outcomes. Overall patient satisfaction may be impacted by incorrect information, errors, and other digital difficulties.

4. **Credential & Compliance Systems** – False credentials and unauthorized access can result in legal and operational damage. The CIA may be heavily compromised leading to the instability of the company.

5. **Medical Device Integration Platforms** – Unauthorized device access risks patient safety and can introduce vulnerabilities that may be life threatening.

6. **Human Resources Payroll System** – Insider threats could lead to identity theft, fraud, and compliance failures. Proper training and authorizations can assist in prevention methods.

7. **Anthem Member Portal & Mobile App** – Breaches here directly affect customer trust and service delivery. Slow or delayed services can leave negative impressions on users and third-party influence.

8. **Data Centers & Cloud Infrastructure** – Core infrastructure; outages or breaches affect the entire organization. Physical security and maintenance is essential for daily operations.

Risk Management Matrix (Avery McLean)

Asset	Threat	Likelihood (1-3)	Impact (1-3)	Risk Level (Score)
Electronic Health Records (EHR) System	Ransomware Attack	3	3	9
Claims Processing System	Data Breach	3	3	9
Data Analytics Platform	Data Accuracy/Integrity Issues	2	3	3
Credential & Compliance Systems	False Credentials/Unauthorized Access	3	2	6
Medical Device Integration Platforms	Unauthorized Device Access	2	3	7
Human Resources Payroll System	Insider Threats & Data Manipulation	2	2	4
Anthem Member Portal & Mobile App	Data Errors or Breaches	2	3	5
Data Centers & Cloud Infrastructure	Service Outages & Breaches	2	3	8

Assessment Recommendations (Avery McLean)

Electronic Health Records (EHR) System

- Secure, offline backups.

- Network segmentation.
- Multi-factor authentication for privileged accounts.
- Phishing prevention training.
- Frequent response plan updates and testing.

Claims Processing System

- Regular vulnerability assessments and penetration testing.
- Integration of threat intelligence feeds.
- Role-based access controls (RBAC).
- SIEM system deployment.
- Insider threat awareness training.

Data Analytics Platform

- Blockchain for audit trails.
- Zero Trust Architecture with continuous security monitoring.
- Data sharding for sensitive information.
- Real-time monitoring with biometrics.
- Simulated attack testing and penetration tests.

Credential & Compliance Systems

- Security awareness training for all staff and third-party partners.
- Regular audits and access reviews.
- Routine testing of protocols.
- Dedicated incident response plans with continuous improvement analysis.

Medical Device Integration Platforms

- Routine inventory and risk assessments of devices.
- Strict network segmentation.
- Enforce MFA on all remote access.
- Deploy endpoint detection and response (EDR).
- Vendor onboarding policies with mandatory security evaluations.

Human Resources Payroll System

- Strict RBAC enforcement.
- Real-time monitoring and automated anomaly alerts.
- Routine audits for access control and privilege creep detection.
- Incident response plans targeting insider threat scenarios.
- Training for HR/finance staff on insider risks and social engineering.

Anthem Member Portal & Mobile App

- Routine audits and data validation.
- Automated discrepancy detection systems.
- Strong encryption to protect against unauthorized data changes.
- Clear, pre-established communication protocols for breaches/errors.
- Continuous improvement cycles for recovery and data quality management.

Data Centers & Cloud Infrastructure

- Frequent vulnerability and penetration assessments.
  Redundancy and robust backup systems.
- Real-time monitoring and threat detection tools.
- Comprehensive disaster recovery plan development and testing.

- Update recovery strategies based on evolving threats and tech.
- Clear and timely communication protocols for all stakeholders during incidents.

Rationale Overview

The selection of assets was based on how crucial they were to maintaining regulatory compliance, safeguarding private patient information, and assisting with business operations. The most important data is stored in the top priorities, EHR and Claims Processing, which are also frequently threatened and high risk elements in the healthcare industry. Other resources, such as medical devices, credential systems, and data analytics, were selected due to their function in preserving data security and integrity. In order to lower risk and safeguard Anthem's reputation, the guidelines emphasize prevention, detection, and quick response. They do this by combining stringent technical safeguards with ongoing monitoring and staff awareness.

Asset 1: Electronic Health Records (EHR) System (Avery McLean)

Risk: Ransomware Attack

Rationale:
Ransomware frequently targets the Electronic Health Records system, which contains extremely sensitive patient data. To prevent unwanted access and guarantee data integrity, protective technologies (PR.PT) and data security (PR.DS) are crucial. The probability and effect of encryption-based ransomware are decreased by restricting access and safeguarding data while it is in transit or at rest. Response planning (RS.RP) and mitigation (RS.MI) provide rapid isolation, containment, and recovery in the event of an attack. After every event, these categories guarantee Anthem's ability to react quickly and enhance defenses.

Asset:	Electronic Health Records (EHR) System
Risk:	Ransomware Attack
Function:	Protect (PR), Respond (RS)
Category:	PR.DS (Data Security), PR.PT (Protective Technology), RS.RP (Response Planning), RS.MI (Mitigation)
Sub-Category:	PR.DS-1 (Data-at-rest is protected), PR.DS-2 (Data-in-transit is protected), PR.PT-1 (Audit/log records are maintained and protected), PR.PT-3 (Access to systems is limited to authorized users), RS.RP-1 (Response plans are executed during or after an incident), RS.RP-2 (Response plans are updated to reflect lessons learned), RS.MI-1 (Incidents are contained to prevent further damage), RS.MI-2 (Newly identified vulnerabilities are documented and addressed)
Rationale Ransomware frequently targets EHR systems, which contain extremely sensitive patient data. To prevent unauthorized access and maintain data integrity, encryption and protective technology are essential. Secure access controls and continuous logging reduce exposure. Rapid response planning and mitigation strategies ensure Anthem can isolate attacks, recover quickly, and improve defenses.	
Policy:	All EHR data at rest must be encrypted using AES-256, and data in transit protected with TLS 1.3. Access will be limited to authorized personnel using RBAC and MFA. Audit and log records will be maintained in a secure SIEM platform. Incident response plans must be executed during incidents and updated following all security events.
Procedure:	The IT department will implement encryption and configure secure protocols on all EHR systems. Access permissions will be granted on a need-to-know basis with quarterly reviews. Logs will be reviewed weekly by the SOC team. Incident response plans will be tested biannually, and post-incident reviews will feed into plan improvements.
Review Period:	Semi-annually
Control:	Quarterly audits will verify encryption and access controls. Monthly SOC reports will confirm monitoring activity. Third-party audits will assess compliance with HIPAA and NIST standards, and corrective actions will be tracked to completion.

Asset 2: Claims Processing System (Avery McLean)

Risk: Data Breach

Rationale:
Since the Claims Processing System manages private health and financial information, security lapses could have disastrous consequences. Finding vulnerabilities, defining roles, and enforcing regulations are all made possible by carrying out ongoing risk assessments (ID.RA) and upholding transparent governance (ID.GV). In order to identify and look into suspicious activity before large-scale data exfiltration may take place, continuous monitoring (DE.CM) and the establishment of anomalous baselines using DE.AE are essential. Together, these features help stop breaches and identify threats quickly.

Asset:	Claims Processing System
Risk:	Data Breach
Function:	Identify (ID), Detect (DE)
Category:	ID.RA (Risk Assessment), ID.GV (Governance), DE.CM (Security Continuous Monitoring), DE.AE (Anomalies and Events)
Sub-Category:	ID.RA-1 (Asset vulnerabilities are identified and documented), ID.RA-2 (Threat intelligence is integrated into risk assessment), ID.GV-1 (Cybersecurity policies are established and communicated), ID.GV-2 (Security roles and responsibilities are assigned), DE.CM-1 (The network is monitored to detect potential cybersecurity events), DE.CM-3 (Personnel activity is monitored to detect potential insider threats), DE.AE-1 (A baseline of network operations and expected data flows is established and managed), DE.AE-3 (Detected events are analyzed to understand attack targets and methods)
Rationale The Claims Processing System manages confidential financial and health data. A breach could result in legal violations, regulatory fines, and reputational damage. Conducting regular risk assessments, enforcing strong governance, and detecting anomalies quickly are key to maintaining trust and protecting sensitive information.	
Policy:	Regular vulnerability assessments will be conducted, and threat intelligence will be integrated into risk assessments. Cybersecurity policies will be communicated annually, and security roles clearly defined. Continuous monitoring and anomaly detection will be deployed across all claim processing systems.
Procedure:	Monthly vulnerability scans will be completed by IT security teams.

	Policy updates and training will be provided quarterly. The SOC will monitor all user activity, while anomaly baselines will be updated every six months. Any detected suspicious activity will be investigated within 24 hours and documented.
Review Period:	Semi-annually
Control:	Quarterly reports will verify vulnerability remediation and policy adherence. SOC activity logs and investigations will be reviewed monthly. An annual third-party audit will confirm that monitoring and detection practices are effective.times at rest (stored on local or cloud media).

Asset 1: Data Analytics (Jocelyn Peguero)

Risk: Data Accuracy and Quality/Integrity

Rationale:

Organizations, especially those within the healthcare industry, rely on data analytics to make informed decisions and optimize day-to-day operations. As a critical component in the industry, data accuracy and quality can impact results and implicate sources. The integrity of collected data can be used in planning and execution of strategies (ID.BE). Unreliable data can affect Anthem's ability to properly assess risks and maintain regulatory compliance, directly impacting business operations. Data analytics is highly vulnerable to manipulation, breach, system downtime, and more (ID.RA). In the event of any exploited vulnerabilities, the reaction and recovery make a difference in the repair and maintenance of company reputation (RC.RP & RC.CO). It is essential to identify and address the risks and vulnerabilities in regards to data analytics. For Anthem, Elevance Health Inc., this means strengthening the security and compliance measures to protect sensitive data and deliver reliable insights and feedback. The organization may benefit in financial security, leverageable data in market trends, and creating efficient operations.

Asset:	Data Analytics
Risk:	Data Accuracy & Integrity
Function:	Identify (ID) & Recover (RC)
Category:	Business Environment (ID.BE), Risk Assessment (ID.RA), Communications (RC.CO), Recovery Planning (RC.RP)
Sub-Category:	Dependencies and critical functions for delivery of critical services are established (ID.BE-4). Resilience requirements to support the delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) (ID.BE-5) Potential business impacts and likelihoods are identified (ID.RA-4). Risk responses are identified and prioritized (ID.RA-6). Reputation is

	repaired after an incident (RC.CO-2). Recovery activities are communicated to internal and external stakeholders as well as executive and management teams (RC.CO-3). Recovery plan is executed during or after a cybersecurity incident (RC.RP-1).
Rationale: Ensuring data accuracy and integrity requires identifying dependencies, assessing resilience across all operational states, and evaluating business impacts. Risk response measures must be prioritized to mitigate potential threats. Effective communication and incident recovery planning are crucial to restoring operations and maintaining stakeholder trust. Unreliable data can affect Anthem's ability to properly assess risks and maintain regulatory compliance, directly impacting business operations.	
Policy:	IT teams will ensure data accuracy and integrity by identifying critical dependencies, assessing risks, and implementing resilience measures. Risk assessments will evaluate business impacts, prioritize responses, and establish resilience structured recovery plans that will be executed with timely stakeholder communication and reputation management.
Procedure:	Conduct dependency mapping for critical data sources and processes. Perform regular risk assessments to evaluate potential impacts and likelihoods. Establish resilience measures, including redundancy and failover mechanisms. Develop and test a recovery plan, including stakeholder communication strategies and reputation management initiatives.
Review Period:	Semi annual reviews and large scale annual audits.
Control:	Dependency validation, failover testing, recovery drills, and stakeholder communication audits. Implementation of zero trust architecture and (MFA) Multi-factor Authentication. Real time biometrics and simulations. Integrating blockchain technology to provide logs and statistics on changes to collected data. Using the Zero Trust Architecture (ZTA) approach, implementing multi-factor authentication and continuous security monitoring. Improved data sharding - breaking sensitive data into fragments, storing them securely in multiple locations rather than one. Real time response using biometrics and following patterns. Penetration testing and attack simulations to verify and view impacts and potential data manipulations.

Asset 2: Credential & Compliance Systems (Jocelyn Peguero)

Risk: False Credentials and Unauthorized Access

Rationale:

Confirming authorization and optimizing compliance can protect Anthem from unauthorized access, legal implications, and more. There are many vulnerabilities within this asset, from mobile compromise to

physical threat and insider harm. It is important that all users and third-parties only have access to authorized information, of which they are authenticated and the integrity of the information/data is protected (PR.AC). Training and awareness is crucial to ensuring all employees and members are informed and understand the significance of maintaining CIA (confidentiality, integrity, availability). In the event of an attack, it is important that Anthem is able to detect breaches and loopholes before the loss and attack on sensitive functions. A strong monitoring system and protocol is necessary, requiring organized data logs, consistent protocol checks, updates, and analyses.

Asset:	Credential & Compliance Systems
Risk:	False Credentials & Unauthorized Access
Function:	Detect (DE) & Protect (PR)
Category:	Security Continuous Monitoring (DE.CM), Detection Processes (DE.DP), Awareness and Training (PR.AT), & Identity Management, Authentication, and Access Control (PR.AC).
Sub-Category:	Personnel activity is monitored to detect potential cybersecurity events (DE.CM-3). Monitoring for unauthorized personnel, connections, devices, and software is performed (DE.CM-7) Detection processes are tested (DE.DP-3). Detection processes are continuously improved (DE.DP-5). All users are informed and trained (PR.AT-1). Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities (PR.AT-3).Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes (PR.AC-1). Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)(PR.AC-7)
Rationale: To prevent fake credentials and unauthorized access, detection processes must be monitored, tested, and improved on a constant basis. Proper identity management and user authentication reduce security threats, while training ensures that people and third parties understand their roles in security. To reduce these dangers, it is essential to guarantee thorough credential verification, ongoing monitoring, and prompt identification.	
Policy:	Anthem will strictly enforce credential issuing, authentication, and access management regulations. Continuous monitoring, testing, and upgrading of detection processes are required. Training is required for all users.
Procedure:	Incorporate real-time activity monitoring, unauthorized usage detection, and periodic credential audits. Provide frequent security awareness training.

Review Period:	Semi Annually
Control:	To find security flaws, guarantee compliance, and improve detection procedures for stopping unwanted access and credential misuse, access audits, monitoring reports, detection testing, authentication logs, and training completion records will all be examined on a regular basis. Security awareness training programs for all staff and members in order to educate on protocols, access, and common vulnerability points. Regular audits and reviews in terms of qualifications, access logs, contractors, etc. Testing of services and protocols. Creating incident response plans and analyzing changes to improve systems over time.

Asset 1: Medical Devices (Tim Klein)

Risk: Unauthorized Medical Device Access

Rationale:

Device integration platforms play a crucial role in Anthem's infrastructure by connecting various devices, systems, and third-party services. However, without a well-maintained inventory and a clear prioritization process, vulnerable or unpatched devices could serve as potential entry points for cyberattacks. Maintaining an accurate device inventory (ID.AM-1) and conducting thorough criticality assessments (ID.AM-5) are vital to ensuring that security efforts are focused on the most critical areas. Additionally, given the remote nature of many integrations, robust management of remote access (PR.AC-3) and safeguarding network integrity (PR.AC-5) are essential to prevent unauthorized access or lateral movement within the system. Implementing strong access control measures is key to mitigating risks such as data breaches or malicious attacks that could originate from integrated devices.

Asset:	Medical Devices
Risk:	Unauthorized access, firmware vulnerabilities, and lack of patching
Function:	Identify (ID) – Understand and manage cybersecurity risks Protect (PR) – Implement safeguards to ensure service delivery
Category:	Asset Management (ID.AM) Access Control (PR.AC) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA)

Sub-Category:	ID.AM-1 - Physical devices and systems within the organization are inventoried ID.AM-5 - Resources are prioritized based on classification, criticality, and business value PR.AC-3 - Remote access is managed PR.AC-5 - Network integrity is protected (e.g., network segmentation) PR.IP-3 - Configuration change control processes are in place PR.MA-1 - Maintenance and repair of organizational assets are performed and logged
Rationale: Medical devices are high-risk due to outdated software and frequent lack of patching. Without strong controls, these devices can be accessed by unauthorized users or exploited by malware. Inventorying devices (ID.AM-1) and prioritizing by risk (ID.AM-5) ensures attention to the most critical systems. Segmenting device networks (PR.AC-5), managing remote access (PR.AC-3), and maintaining change controls (PR.IP-3) reduce risk. Regular maintenance and patching (PR.MA-1) help mitigate known vulnerabilities.	
Policy:	All network-connected medical devices must be inventoried and prioritized by risk level. Devices must be isolated on segmented networks. Remote access must be restricted to authorized personnel using multi-factor authentication. All configuration changes must follow Anthem's change control procedures. Maintenance and patching must be scheduled, documented, and performed using approved tools.
Procedure:	Maintain a current inventory of all medical devices. Assign each device a criticality level based on business and clinical importance. Segment all medical devices into isolated VLANs with firewalls. Allow remote access only through Anthem's VPN with MFA and logging. Schedule firmware/patch updates quarterly or upon vendor release. Log all maintenance activities and require formal approval for configuration changes.
Review Period:	Annual
Control:	Quarterly reports confirm inventory accuracy, patch status, and change logs. Remote access logs are reviewed monthly. SIEM tools monitor medical device network segments. Internal audits sample devices yearly to ensure compliance and validate procedures.

Asset 2: Human Resources Payroll System (Tim Klein)

Risk: Insider Threats and Data Manipulation

Rationale:
The Human Resources Payroll System houses highly sensitive personal and financial employee data, making it a significant target for insider threats. Unauthorized modifications to this system could lead to fraud, identity theft, or regulatory non-compliance. To mitigate these risks, it is essential to monitor personnel activity (DE.CM-3) to detect and flag suspicious behavior early. Identifying unauthorized devices or connections (DE.CM-7) is crucial for uncovering potential external or insider threats. Rapid investigation (RS.AN-1) and thorough impact analysis (RS.AN-2) are vital to minimizing damage, preserving operational integrity, and safeguarding employee privacy as well as Anthem's reputation.

Asset:	Human Resources Payroll System
Risk:	Insider threats and external breaches (phishing, ransomware)
Function:	Protect (PR) – Safeguard critical data and services Detect (DE) – Identify cybersecurity events Respond (RS) – Contain and mitigate the impact of events
Category:	Access Control (PR.AC) Awareness and Training (PR.AT) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM) Analysis (RS.AN)
Sub-Category:	PR.AC-1: Identities and credentials are issued, managed, and audited for users and devices PR.AT-1: All users are informed and trained PR.PT-4: Communications and control networks are protected DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed RS.AN-1: Notifications from detection systems are investigated RS.AN-2: The impact of the incident is understood
Rationale: The payroll system contains sensitive financial and personal information, making it a target for insider threats and external attacks like phishing or ransomware. Access control (PR.AC-1) and user training (PR.AT-1) reduce the risk of user-related breaches. Monitoring system activity (DE.CM-3) and detecting unauthorized access (DE.CM-7) provide early warning signs. Investigation and analysis of incidents (RS.AN-1, RS.AN-2) support timely response and limit damage.	

Policy:	Access to the HR payroll system must be limited to authorized personnel using role-based permissions and multi-factor authentication. All system use must be logged and monitored for anomalies. Security awareness training is mandatory for all staff. The system must be protected by email and web filtering. Any incidents must be investigated, and their impact assessed by the security team.
Procedure:	User access must be granted based on job role and reviewed quarterly. MFA is required for all administrative and remote users. All system actions are logged and monitored through a SIEM. HR staff receive cybersecurity training annually and during onboarding. Simulated phishing tests are conducted regularly. Alerts are triaged by the SOC, and confirmed incidents are analyzed for impact.
Review Period:	Annual
Control:	Access audits and permissions reviews conducted quarterly SIEM logs monitored by the SOC to detect anomalies Phishing simulation results tracked to gauge user awareness Email/web filtering reports reviewed monthly Annual incident response drills validate response readiness and identify gaps

Asset 1: Anthem Member Portal & Mobile App (Ethan De Jong)

Risk: Anthem Member Portal & Mobile App

Rationale:

Data accuracy is vital for the Anthem Member Portal and Mobile App, as they handle sensitive member data, including health and financial information. Any errors or inaccuracies could lead to major problems, such as incorrect claims, service disruptions, or loss of trust. Identifying key business functions and ensuring they remain operational under all circumstances (ID.BE) is essential to maintaining data quality. By assessing potential risks to this data (ID.RA) and preparing for recovery in case of issues (RC), Anthem can maintain the integrity of its member services. Continuous monitoring of data quality and implementing quick recovery measures ensure that any disruptions or inaccuracies are swiftly addressed, minimizing their impact.

Asset:	Anthem member portal and mobile app
Risk:	Unauthorized access, firmware vulnerabilities, and lack of patching
Function:	Protect (PR) – Safeguard critical data and services Detect (DE) – Identify cybersecurity events

	Respond (RS) – Contain and mitigate the impact of events
Category:	Business Environment (ID.BE) Risk Assessment (ID.RA) Communications (RC.CO) Improvements (RC.IM)
Sub-Category:	ID.BE-4: Dependencies and critical functions for delivery of critical services are established. ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and normal operations). ID.RA-4: Potential business impacts and likelihoods are identified. ID.RA-6: Risk responses are identified and prioritized. RC.CO-3: Recovery activities are communicated to internal and external stakeholders, as well as executive and management teams RC.CO-2: Reputation is repaired after an incident. RC.IM-1: Recovery plans incorporate lessons learned. RC.IM-1: Recovery plans incorporate lessons learned.
Rationale: The Anthem Member Portal and Mobile App require precise data management because they handle sensitive information about personal health and financial details of millions of users. Data errors may lead to significant problems which include billing mistakes and insurance claim faults, denial of essential medical services and private data breaches that can harm Anthem's reputation and reduce user trust. Anthem needs to build a strategic cybersecurity framework that covers the identification of critical business environments (ID.BE), performs thorough risk assessments (ID.RA), and develops strong recovery strategies (RC) to maintain data integrity and system reliability. Through the Identify function organizations can pinpoint essential systems and data assets for operations while Risk Assessment components analyze potential threats and vulnerabilities that might affect data accuracy. Recovery planning operates alongside other processes to ensure services return to normal quickly after cyber incidents or errors with minimal disruption. The combination of ongoing system monitoring with proactive issue detection and quick response capabilities proves essential for sustaining digital health platform security and reliability.	
Policy:	To keep the Anthem Member Portal and Mobile App running smoothly, all data needs regular checks to ensure accuracy. If any issues pop up, they should be flagged and fixed right away to avoid problems for users and business operations.
Procedure:	Regularly check and verify data to keep it accurate. Use automated tools to catch and fix errors instantly. Protect data with strong security measures like encryption. Have a clear plan to inform members and stakeholders if issues arise. Continuously improve by learning from past incidents and updating recovery strategies.
Review Period:	Semi-Annual

Control:	Use continuous monitoring to keep data accurate and secure. Detects issues instantly with automated systems. Have quick-response plans to handle risks right away. Regularly update recovery plans based on new threats and past experiences.

Asset 2: Data Centers & Cloud Infrastructure (Ethan De Jong)

Risk: Data Centers & Cloud Infrastructure

Rationale:

Anthem's data centers and cloud infrastructure are the backbone of the business, ensuring that sensitive member data is protected and that key services continue without a hitch. If these systems were to face issues like data loss, outages, or security breaches, it could have major consequences. By identifying potential risks and putting in place recovery plans ahead of time, Anthem can bounce back quickly and minimize damage. Plus, by learning from past incidents and continuously adapting to new tech and threats, Anthem can stay ahead of the game.

Asset:	Data center in Cloud infrastructure
Risk:	Data Loss, System Outages, and Security Breaches in Data Centers & Cloud Infrastructure
Function:	Identify (ID) – Identify cybersecurity events Recover (RC) – Contain and mitigate the impact of events
Category:	Business Environment (ID.BE) Risk Assessment (ID.RA) Communications (RC.CO) Improvements (RC.IM)
Sub-Category:	ID.BE-4: Critical services that rely on data centers and cloud infrastructure are documented. ID.BE-5: Resilience requirements for critical services are established for operating during disruptions (e.g., cyberattacks or system outages). ID.RA-4: Potential business impacts of data losses, system outages, or security breaches are assessed. ID.RA-6: Risk responses like disaster recovery plans and systems redundancy are prioritized and documented. RC.CO-3: Recovery activities are communicated clearly to internal teams and external stakeholders. RC.CO-2: Efforts to restore trust and data availability after an incident are prioritized. RC.IM-1: Recovery plans incorporate lessons learned from past incidents. RC.IM-2: Recovery strategies are updated to keep up with new technologies and challenges (e.g., cloud migration, rising cyber threats).

Rationale: Anthem's data centers and cloud infrastructure are crucial for protecting sensitive member data and ensuring smooth services. Disruptions like data loss or outages can be damaging, but with risk assessments and recovery plans in place, Anthem can recover quickly. By learning from past incidents and embracing new technologies, Anthem keeps its systems resilient against emerging threats. To prevent issues, Anthem identifies key functions, assesses risks, and ensures recovery plans are ready. Continuous monitoring and fast fixes help keep services secure and reliable.	
Policy:	All data in Anthem's data centers and cloud infrastructure should undergo regular vulnerability checks and be included in disaster recovery plans. Redundant backup systems ensure data integrity during disruptions. Clear and timely communication is key to maintaining trust during and after incidents. Recovery plans should be updated regularly to address new risks, technologies, and lessons from past experiences.
Procedure:	Run vulnerability assessments and penetration tests every quarter on all data center and cloud systems. Set up redundant systems and check them monthly to make sure they're working. Use continuous monitoring tools to spot anomalies and react to threats right away. Test disaster recovery plans at least twice a year to minimize downtime during disruptions. Update recovery strategies annually to keep up with new technologies and threats. Regularly test the communication plan during incidents, ensuring real-time updates for stakeholders.
Review Period:	Semi-Annual
Control:	We'll regularly test for vulnerabilities and weaknesses to stay ahead of potential issues. Data backups and redundancy systems will be checked monthly to ensure they're working as they should. Monitoring tools and disaster recovery plans will be tested and reviewed on an ongoing basis. We'll evaluate communication protocols during recovery drills to ensure they're effective. Recovery strategies will be updated and tested annually to adapt to new tech challenges and learn from past experiences.

Conclusion (Tim Klein & Jocelyn Peguero)

This cybersecurity assessment of Anthem (Elevance Health Inc.) focused on identifying and protecting the organization's most critical assets across clinical, operational, and technological domains. Using the NIST Cybersecurity Framework as our foundation, the team selected subcategories that directly address Anthem's most pressing vulnerabilities: the safeguarding of patient data, defense against insider threats, and the stability of digital infrastructure that supports health services. We selected categories that emphasized **risk-based identification (ID.AM, ID.RA)**, **access control and authentication (PR.AC)**, **security monitoring (DE.CM)**, and **incident response and recovery (RS.AN, RC.IM)**. The subcategories among them were not only relevant to the types of systems under review such as electronic health records, claims processing, and HR/payroll systems but were also selected for their ability to strengthen Anthem's posture against both external cyberattacks and internal operational risks.

Our policy recommendations focused on enforcing **least privilege access**, establishing clear **response protocols**, and supporting **continuous improvement through regular reviews and training**. By clearly mapping these policies to procedures and measurable controls, we ensured a defensible and repeatable security practice. For example, segmentation and logging on medical devices reduces lateral threat movement, while SOC-led monitoring of payroll systems minimizes the potential for internal fraud or manipulation. The integration of these controls provides Anthem with a layered defense model, one that not only detects and prevents threats but also builds resilience into daily operations. Regular audits, updated recovery plans, and stakeholder communication protocols make Anthem better equipped to handle evolving cyber threats while staying compliant with healthcare regulations like HIPAA. Looking forward to the future, the company must continue prioritizing threat-informed improvements and investing in secure infrastructure. With scalable cybersecurity controls in place, Anthem can confidently support its mission of delivering secure, accessible healthcare across its digital ecosystem.

It is crucial for Anthem to strengthen their security in order to assure their position within the healthcare industry. Investing in the proper training, safeguards, and equipment, they have the opportunity to rise to the top of the industry and secure their title as the number one leading healthcare company in the nation. Without doing so, they invite instability and increase the threat to their ultimate success. In an industry where digital infrastructure is becoming increasingly important for both clinical results and operational efficiency, a solid security foundation is critical—not just for resilience, but also for competitive advantage. Strengthening cybersecurity is about more than defense; it's about fostering development, innovation, and sustained leadership in a rapidly changing healthcare sector.