Fall 2024 Cycle A - F01E - Principles of Information Security

American Health Solution Cybersecurity Plan

Group 4:

Giorgio Jarrett

Michael Valenzuela

Company Overview and the Need for Information Security

American Health Solutions (AHS) is a premier healthcare provider, offering a broad spectrum of medical services to patients across multiple facilities. AHS has embraced technology advancements such as electronic health records (EHRs), telemedicine, and cloud-based data solutions to improve patient care, enhance operational efficiency, and streamline services. This digital transformation has optimized processes and expanded patient reach through virtual consultations and real-time data sharing across different healthcare units.

However, with this increased reliance on technology comes significant cybersecurity challenges. The healthcare sector is highly vulnerable to cyberattacks, with ransomware and data breaches posing severe risks to the confidentiality, integrity, and availability of critical patient information. As noted in the **Health Industry Cybersecurity – Strategic Plan (2024–2029),** healthcare organizations are frequent targets for cybercriminals due to the value of personally identifiable information (PII) and protected health information (PHI). The plan emphasizes the necessity of robust data protection strategies, including encryption, access controls, and multi-factor authentication (MFA), to mitigate risks and ensure regulatory compliance with laws such as HIPAA and GDPR.

The widespread shift toward telemedicine and remote work further increases the attack surface, as healthcare data is now shared and accessed beyond traditional, secured hospital environments. This has elevated the need for comprehensive cybersecurity frameworks that address both local and remote operations. The strategic importance of protecting patient trust and the organization's reputation is another key driver for cybersecurity in healthcare. As indicated in the Strategic Plan, building resilience and ensuring continuous service delivery in the face of these growing threats is vital for organizations like AHS. Without strong cybersecurity measures, the organization risks not only financial penalties but also the potential loss of patient confidence, which could harm its long-term success.

Strategic Plan for Information Security

AHS will adopt a phased and strategic approach to strengthening its information security framework, aligning its initiatives with the Health Industry Cybersecurity – Strategic Plan (2024–2029). The plan focuses on **data protection**, **cyber resilience**, and **regulatory compliance**, ensuring that AHS can maintain the highest levels of security while continuing to provide uninterrupted patient care.

Phase 1: Risk Assessment and Policy Development (Q1 2024)

AHS will start by conducting a comprehensive **risk assessment** to identify potential vulnerabilities across its systems, particularly in its electronic health records (EHR) and telemedicine platforms. This assessment will help prioritize areas for improvement. Simultaneously, AHS will update its **Enterprise Information Security Policy (EISP)**, defining the overarching security measures, and develop an **Issue-Specific Security Policy (ISSP)** and **System-Specific Security Policy (SSP)** that focus on specific threats, like ransomware and phishing, and systems such as remote access.

Phase 2: Implementation of Security Controls (Q2–Q3 2024)

The second phase will involve rolling out **technical controls** such as **multi-factor authentication (MFA)**, **encryption protocols**, and **role-based access control (RBAC)** for sensitive systems. AHS will also deploy **AI-driven threat detection systems** to monitor for suspicious activities in real time. These controls will enhance protection against unauthorized access, insider threats, and external attacks. Additionally, AHS will introduce an **Incident Response Plan (IRP)**, in page 3, to ensure swift and efficient handling of security incidents, in line with the Health Industry Cybersecurity Strategic Plan.

Phase 3: Employee Training and Awareness (Q3 2024)

A key component of AHS's strategy is **employee education**. AHS will implement ongoing **cybersecurity awareness training programs** for all staff, focusing on recognizing phishing attempts, securing remote work environments, and following best practices in data handling. Training will be mandatory, with periodic assessments to ensure compliance and understanding.

Phase 4: Monitoring and Continuous Improvement (Q4 2024 onwards)

After the initial implementation of security measures, AHS will adopt a cycle of **continuous monitoring and improvement**. This will include regular **system audits**, **vulnerability testing**, and **patch management** to ensure that systems remain secure and compliant with evolving regulations. AHS will also analyze the effectiveness of its **AI-driven monitoring** and **incident response** systems, making adjustments as necessary to stay ahead of new and emerging threats.

Enterprise Information Security Policy

Purpose:
This policy safeguards the confidentiality, integrity, and availability of sensitive health information at American Health Solutions (AHS), ensuring compliance with HIPAA, HITECH, NIST, GDPR, and FERPA.

Scope:
Applies to all AHS employees, contractors, and vendors with system access, ensuring compliance with security protocols and regulations.

Policy Overview:
Personnel must protect health information from unauthorized access, alteration, or destruction. Access is restricted to essential personnel. All users must complete mandatory security training.

1. **Governance & Risk Management:**
   An Information Security Committee will enforce policies, ensuring compliance and conducting regular risk assessments to maintain effective controls (HealthIT.gov, n.d.).
2. **Data Protection:**
   Data will be encrypted (TLS in transit, AES-256 at rest). Weekly backups will be tested quarterly. HIPAA retention rules require data to be stored for six years, with secure disposal afterward.
3. **Access Control:**
   Access will follow the least privilege principle with multi-factor authentication (MFA). Role-based access control will be reviewed quarterly. Passwords must meet complexity standards and be changed every 90 days (AHIMA, 2023).
4. **Incident Response:**
   AHS's incident response plan outlines the steps for detecting, reporting, and recovering from incidents, with annual tests. Data breaches require notification within 60 days (ASPR, 2023).
5. **Compliance & Third-Party Management:**
   Internal audits will monitor compliance with HIPAA, HITECH, GDPR, and FERPA. Third-party vendors will undergo regular risk assessments to ensure adherence to security policies.

Training & Awareness & Implementation:
Employees must complete annual training on phishing, data privacy, and cybersecurity, with continuous updates on evolving threats. AHS will regularly audit systems, develop controls, and ensure clear communication on security roles and responsibilities.

Issue-Specific Security Policy (ISSP) (with Incident Response)

The **Issue-Specific Security Policy (ISSP)** for American Health Solutions focuses on managing two of the most critical cybersecurity threats in the healthcare sector: **ransomware attacks** and **phishing attacks**. These threats are of particular concern as healthcare organizations, like AHS, handle sensitive patient data and require uninterrupted service delivery. The Health Industry Cybersecurity – Strategic Plan (2024–2029) emphasizes the importance of mitigating these risks through a structured and proactive approach, which includes robust security measures and an effective **Incident Response Plan (IRP)**.

To strengthen **ransomware defenses**, AHS will implement a multi-layered approach that includes **frequent data backups** stored in secure, offsite locations, as well as **regular backup tests** to ensure data can be restored quickly in the event of a ransomware attack. In addition, **endpoint detection and response (EDR)** systems will be deployed to continuously monitor network devices for suspicious activities, allowing for early identification and containment of ransomware threats before they can spread.

For **phishing attacks**, AHS will introduce comprehensive **cybersecurity awareness training** for employees, focusing on identifying and reporting phishing attempts. In conjunction with this, **email filtering and AI-based threat detection** systems will be utilized to flag and block malicious communications. These systems will use machine learning models to detect patterns in phishing attempts and prevent them from reaching the end-user.

A critical component of the ISSP is the **Incident Response Plan (IRP)**, which ensures that AHS is prepared to respond effectively to security incidents. The IRP will include the following key stages:

1. **Preparation**: Establishing response teams and defining roles and responsibilities for responding to incidents.
2. **Identification**: Detecting and analyzing the incident using AI-driven monitoring tools, enabling rapid identification of threats.
3. **Containment**: Implementing immediate containment measures to prevent the spread of an attack, such as isolating affected systems.
4. **Eradication**: Removing malware or compromised elements from the system while addressing any vulnerabilities that were exploited.
5. **Recovery**: Restoring affected systems from backups and ensuring data integrity is maintained.
6. **Lessons Learned**: Conducting a post-incident review to understand the root cause and improve future defenses.

Business Continuity Plan (BCP)

A Business Continuity Plan (BCP) ensures the continuation of critical services during and after disruptions. It emphasizes that AHS's use of technologies, such as electronic health records (EHRs) and telemedicine, can enhance both care delivery and operational efficiency. The plan highlights those essential functions, like patient check-ins and diagnostics—should be prioritized for swift recovery. Additionally, the BCP outlines strategies for maintaining operations during events such as natural disasters and cyberattacks, ensuring patient safety, data protection, and regulatory compliance, while also addressing challenges like power outages and ventilation failures.

Key objectives:

1. **Resource Acquisition:** Ensure access to essential resources, including patient records.
2. **Movement Support:** Assist with relocating to alternate sites as necessary.
3. **Coordination:** Collaborate with IT and logistics for technology needs and operational restoration.
4. **Operational Restoration:** Efficiently resume operations across all branches.

Risk Assessment

In the risk assessment process, potential risks that can disrupt operations must be identified, including cybersecurity threats like ransomware, natural disasters such as hurricanes and floods, equipment failures including power outages, and public health emergencies like pandemics.

Business Impact Analysis (BIA)

A BIA prioritizes recovery actions and identifies essential resources such as personnel, facilities, and equipment. Key steps include maintaining emergency contact lists, essential vendor information, backup plans for supplies, and inventories of specialized equipment.

Utility Outages

In the event of utility outages, emergency backup power solutions, such as uninterruptible power supplies (UPS)—must be implemented. Additionally, protocols for managing temperature-sensitive medications should be established to maintain their efficacy and ensure patient safety throughout the disruption.

Disaster Recovery and Relocation

AHS should establish a relocation plan identifying alternate operational sites, forming partnerships for mutual aid, and sharing resources during disasters.

Emergency Communication

This plan should identify key audiences, assign communication responsibilities, and utilize multiple channels (email, phone, text) for redundancy. Messages must focus on essential information, and updates should be scheduled regularly to ensure consistent communication with all stakeholders during a crisis.

Employee Preparedness

Ensure staff are familiar with emergency plans, promote personal preparedness strategies, and provide critical function employees with a preparedness kit.

Testing and Exercising the Plan

Conducting regular tabletop exercises or walkthroughs ensures the plan's effectiveness, familiarizes staff with procedures, and aligns the plan with operational needs.

Activation of BCP

Upon disruption, the Command Center (CC) oversees recovery efforts, restoring mission-critical services within 8-24 hours. During activation, the On-Duty Manager assesses essential equipment and supplies, transitioning to manual operations if needed.

System-Specific Security Policy (SSP)

The **System-Specific Security Policy (SSP)** for AHS is designed to secure its critical infrastructure, focusing primarily on the **electronic health record system**, **telemedicine platforms**, and **cloud-based data solutions**. As healthcare organizations increasingly adopt digital technologies, safeguarding these systems from cyber threats becomes a top priority. The Health Industry Cybersecurity – Strategic Plan (2024–2029) stresses the importance of implementing **multi-layered security approaches** to prevent unauthorized access and ensure data integrity.

AHS will implement **encryption protocols** for both data at rest and data in transit, ensuring sensitive patient information remains secure across all channels of communication. Additionally, **multi-factor authentication (MFA)** will be enforced for both local and remote users to reduce the risk of unauthorized access to critical systems. **Role-based access control (RBAC)** will be implemented to ensure that users only have access to the systems and data necessary for their job functions, minimizing the likelihood of insider threats or accidental data exposure.

In alignment with the Health Industry Cybersecurity Strategic Plan, AHS will conduct **regular system audits** and **vulnerability assessments** to identify and rectify potential weaknesses. This proactive approach ensures the infrastructure remains compliant with industry regulations and can swiftly adapt to new security threats. The policy will also include a **patch management program** to ensure that all systems and software are up to date and free of known vulnerabilities. In addition to these measures, cisco-based **AI-driven threat detection systems** will monitor for anomalies and suspicious behavior in real-time, enabling immediate response to potential cyber threats.

This SSP is designed to protect patient data while allowing healthcare professionals seamless access to the tools they need, especially in telemedicine contexts, where accessibility and security must coexist. By aligning with industry best practices and strategic initiatives outlined in the **Strategic Plan**, AHS can enhance its cybersecurity posture, protect against evolving threats, and ensure operational continuity.

Contingency Plan

The **American Health Solutions Contingency Plan** outlines procedures for recovering healthcare services and IT systems after disruptions, ensuring minimal impact on patient care. The plan complies with OMB Circular A-130, HIPAA, and follows FISMA and NIST SP 800-34 guidelines for IT contingency planning.

Objectives & Phases:

1. **Notification/Activation:** Detect disruption, assess, and activate the plan.
2. **Recovery:** Temporarily restore IT functions and recover damaged systems.
3. **Reconstitution:** Return all systems to full normal operations.
4. **Resource Management:** Ensure adequate resources and procedures for sustained operations.
5. **Roles & Responsibilities:** Clearly assign recovery tasks to personnel.
6. **Coordination:** Seamless cooperation with internal staff and external vendors.

Planning Principles:
Assume the main facility may become inaccessible, requiring a pre-arranged contract with an alternate site for continued operations. The alternate site will be pre-configured to process critical systems until full recovery.

Key Assumptions:

- The system will be down for at least 48 hours.
- Preventive measures, like generators and Uninterruptible Power Supplies (UPS), will maintain operations for 45-60 minutes.
- Offsite data backups and alternate site resources will support seamless recovery.

Leadership & Team Structure:
The Chief Information Officer (CIO) leads the execution of the plan, with the Deputy CIO as backup. Designated recovery teams will manage the process and daily operations.

Testing & Maintenance:
Annual tests, including tabletop and technical exercises, will validate readiness, ensuring the alternate site can support communication and data recovery.

Return to Normal Operations:
Teams will follow procedures to transition from the alternate site back to normal, ensuring system stability and the secure handling of sensitive information.

Disaster Recovery Plan (DRP)

American Health Solutions acknowledges the necessity of a robust Disaster Recovery Plan (DRP) to ensure uninterrupted healthcare services during unforeseen events. This plan details the procedures AHS will employ to effectively manage disasters, protect patient information, and maintain operational integrity.

Administrative Oversight

Senior leadership at AHS plays a key role in the development and management of the Disaster Recovery Plan (DRP), focusing on financial implications and insurance considerations to ensure the organization is well-prepared for potential disasters.

Activation of the Disaster Recovery Plan

When an incident is detected, AHS Information Technology Services (ITS) leadership will assess its scope and impact. If deemed a disaster, the Disaster Recovery Team (DRT) is activated, led by a designated Disaster Recovery Coordinator (DRC) who oversees the recovery efforts.

ITS Disaster Recovery Team

Upon activation, the DRC promptly informs team members about the incident's details, including its nature, the command center's location, and immediate support requirements.

Damage Assessment

A preliminary damage assessment will identify the incident's cause, potential for further harm, and affected areas, while also determining recovery requirements, including the status of critical systems.

Resource Needs

The DRP highlights the importance of human resources, technical infrastructure, and equipment, prioritizing effective communication with external partners and vendors to support recovery efforts.

Recovery Command Center

A centralized command center will coordinate recovery activities, equipped with essential resources like hardware, software, communication tools, and workspace supplies.

Recovery Resources Supply Checklist

The plan will feature a detailed checklist of necessary recovery resources, including hardware, software, communication tools, and office supplies to facilitate recovery efforts.

Recovery Priorities
AHS will categorize systems and applications by operational importance:

- **Critical (Priority 1)**: Immediate restoration required.
- **Essential (Priority 2)**: Short-term downtime acceptable.
- **Necessary (Priority 3)**: Some downtime acceptable.
- **Desirable (Priority 4)**: Low priority; significant downtime tolerable.

Recovery Processes
Post-assessment, the DRC will create a data recovery strategy, focusing on backup systems and detailing steps for salvaging hardware and restoring data at the recovery site.

Reconstitution Activities
AHS will restore operations at the original site or prepare a new permanent location as needed.

Data Backup Procedures
Regular backups are crucial for mission-critical systems like EHRs, with outlined procedures ensuring data availability during downtime.

Temporary Documentation Tools
AHS will use a Master Patient Index (MPI) thumb drive for accessing patient information and key patient care forms available on the shared drive during system downtimes.

Other important steps:

- **Annual Review and Testing**: Review DRP annually or after incidents to update contacts and lessons learned.
- **Threat Assessment**: Regular facility integrity and security assessments to mitigate risks.
- **Emergency Procedures**: Notification process for effective damage assessment and data protection.
- **Recovery Procedures**: Begin recovery at the primary site; activate alternate data center if needed.
- **Post-Recovery**: Validate system functionality and conduct improvement reviews.
- **Prescription Recovery**: Contact pharmacies for prescriptions issued during outages.

References

AHIMA. (2023). ***Policy statement on cybersecurity and information security*****. AHIMA.** **https://www.ahima.org/media/w0knrxej/cybersecurity_information-security-policy-statement-final.pdf**

ASPR. (2023). ***Healthcare sector cybersecurity framework implementation guide*****. ASPR.** **https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf**

HealthIT.gov. (n.d.). ***Information security policy template*****. U.S. Department of Health and Human Services.** **https://www.healthit.gov/resource/information-security-policy-template**

Health Sector Coordinating Council. (2024, February). ***Health industry cybersecurity – Strategic plan (2024–2029)*****.** **https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf**

Santa Cruz County Health Services Agency. (n.d.). ***Business continuity plan example*****.** **https://www.santacruzhealth.org/Portals/7/Pdfs/HPP/CO_Pharmacy_Template.docx**

Shulmistra, D. (2024, September 26). Protect patient care and privacy with healthcare business continuity planning. Invenio IT. **https://invenioit.com/continuity/healthcare-business-continuity-planning/**

Yale Office of Emergency Management. (2016, November). ***Guide to business continuity and recovery planning*****.** **https://emergency.yale.edu/planning/business-continuity-planning**