Develop the Organization Security Policy

Ryan Coon

CYB-650

Dr. Howard Goodman

July 23, 2025

**Introduction**

Augusta Medical Hospital prioritizes patient data protection and system security. As a healthcare provider, we must adhere to HIPAA, HITECH, and other relevant regulations to safeguard sensitive information. This policy details the physical, administrative, and technical safeguards protecting our data, systems, and infrastructure. Compliance is mandatory for all employees, contractors, and vendors to ensure patient data confidentiality, integrity, and availability, supporting secure and efficient hospital operations.

**Acceptable Use Policy**

**Purpose**:

This policy outlines acceptable use of Augusta Medical Hospital's (AMH) information systems, including computers, networks, software, and data. It's designed to protect patient data, maintain system integrity, and ensure efficient operations, complying with all applicable laws and regulations, including HIPAA (Health Insurance Portability and Accountability Act of 1996) and HITECH (Health Information Technology for Economic and Clinical Health Act).

**Scope**:

This policy applies to all AMH employees, contractors, volunteers, and any third-party users accessing AMH information systems.

**Acceptable Use**:

Confidentiality - All users must maintain the confidentiality of patient health information (PHI) and other sensitive data. Access to information is limited to what is necessary for job duties.

Integrity - Users must not alter, delete, or damage AMH's information systems or data. Software must only be installed through authorized channels.

Availability - Users must not perform actions that could compromise the availability of AMH's information systems, such as launching denial-of-service attacks.

Compliance - All users must adhere to all applicable laws, regulations (including HIPAA, HITECH, and state-specific regulations), and AMH policies. This includes proper handling of PHI and adherence to data security best practices.

Personal Use - Limited personal use of AMH information systems is permitted, provided it does not interfere with work responsibilities or violate other policies. Inappropriate or excessive personal use is prohibited. Examples of prohibited uses include accessing illegal or inappropriate websites, downloading copyrighted materials, or engaging in online gambling or other prohibited activities.

Software - Only authorized software may be installed on AMH systems. Unauthorized software installation can lead to security vulnerabilities and system instability.

**Unacceptable Use**:

Accessing, downloading, or distributing illegal or inappropriate content.

Installing unauthorized software.

Using AMH systems for personal gain or commercial purposes.

Sharing passwords or login credentials.

Circumventing security measures.

Engaging in any activity that could compromise the security or integrity of [AMH](https://www.google.com/search?q=AMH)'s information systems.

Using AMH systems to harass or bully others.

Accessing PHI or other sensitive data without authorization.

Violating any applicable laws, regulations, or AMH policies.

**Employee Onboarding and Offboarding Procedures**

**Onboarding Procedures**

**Pre-Employment:**

Background Checks and Reference Verification **-** Comprehensive background checks and reference verifications are conducted to ensure candidate suitability and compliance with hospital regulations.

**First Day:**

Welcome Package **-** New employees receive a welcome package containing essential information, including the employee handbook, IT policies, and other relevant documents.

Department Introduction **-** Introduction to the department, team members, and immediate supervisor.

IT Setup **-** Access to email, network drives, and relevant software is provided and configured.

**Offboarding Procedures**

**Notification:**

Formal Resignation **-** Employees provide formal notification of their resignation, adhering to the hospital's notice period policy.

**Exit Interview:**

Feedback Session **-** An exit interview is conducted to gather feedback, address any outstanding issues, and ensure a smooth transition.

**Account Deactivation:**

System Access **-** Access to all hospital systems, including email, network drives, and software, is deactivated.

Property Return **-** Return of company property, including laptops, badges, and other equipment.

**Final Pay and Benefits:**

Compensation - Final paycheck and benefits information are processed and provided to the employee in accordance with all applicable laws and regulations.

**Social Media Policy Inside and Outside the Organization**

This policy applies to all employees, contractors, volunteers, and anyone representing Augusta Medical Hospital on social media platforms. It aims to protect patient privacy, maintain the hospital's reputation, and ensure compliance with relevant laws and regulations.

**Internal Use of Social Media:**

* Communication **-** Social media tools may be used for internal communication, such as project updates or team discussions, provided they are used on approved hospital platforms and adhere to confidentiality policies.
* Training **-** Social media may be used for training purposes, such as sharing educational materials or conducting online discussions, provided the content is appropriate and complies with all relevant regulations.
* Prohibited Activities - Using internal social media platforms for personal use, sharing confidential patient information, or engaging in inappropriate or harassing behavior is strictly prohibited.

**External Use of Social Media:**

Representing the Hospital **-** When using social media outside of work, employees should be mindful of their online presence and avoid making statements that could be construed as representing the hospital's official position. If speaking publicly about AMH, always ensure your statements are factual and align with the hospital's values.

Professional Conduct **-** Maintain professional conduct online. Avoid posting inappropriate content, engaging in arguments or disputes, or making negative comments about the hospital or colleagues.

Confidential Information **-** Never share confidential information about the hospital, patients, or colleagues on social media.

Disclaimer **-** If you choose to post about AMH on your personal social media, a disclaimer stating that the views expressed are your own and do not necessarily reflect those of the hospital is recommended.

**Insider Threats**

Insider threats refer to the potential risks posed by individuals within an organization who have authorized access to its systems and data. These threats can originate from various sources, including employees, contractors, or business partners. Insider threats at Augusta Medical Hospital encompass several risky actions. These include:

* Accessing data or systems beyond the scope of one's assigned job responsibilities.
* Downloading or transferring data without proper authorization.
* Manipulating system logs or disabling security measures.
* Sharing login credentials with individuals who are not authorized to have them.

To mitigate these risks, Augusta Medical Hospital employs a multi-faceted approach. This includes the implementation of stringent access controls, continuous monitoring of employee activity, and comprehensive, ongoing security training programs. Any behavior that raises suspicion will be thoroughly investigated.

**Mobile Device Policy**

To safeguard patient data and maintain robust security, Augusta Medical Hospital mandates a comprehensive Mobile Device Policy for all employees using smartphones, tablets, or laptops for work purposes. This policy dictates:

Authorized Devices **-** Access to hospital systems is strictly limited to approved devices, regardless of whether they are hospital-issued or employee-owned. All devices must have essential security features enabled, including data encryption and up-to-date antivirus software.

Enhanced Security - All mobile devices require strong password protection and the implementation of multi-factor authentication (MFA) for added security. In the event of loss or theft, immediate reporting is critical to facilitate remote data wiping.

Mobile Device Management (MDM) - The hospital utilizes MDM software to enforce consistent security settings across all devices, monitor usage, and guarantee ongoing compliance with security policies. This includes maintaining the latest security patches and updates.

Prohibited Activities **-** Storing or processing patient data on unauthorized apps or cloud services is strictly forbidden. Downloading unapproved apps or accessing unapproved websites while connected to hospital systems is also prohibited.

**Key Provisions of Common Standards**

Augusta Medical Hospital prioritizes data protection and regulatory compliance by adhering to the following security standards:

1. NIST Cybersecurity Framework (CSF) - We employ the NIST CSF to proactively manage cybersecurity risks. This framework provides a structured approach for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents.
2. HIPAA (Health Insurance Portability and Accountability Act) - We rigorously comply with HIPAA regulations to safeguard Protected Health Information (PHI). This includes implementing required safeguards to protect patient data within our healthcare environment.
3. ISO/IEC 27001 - We utilize the ISO/IEC 27001 framework to effectively manage sensitive information. This helps ensure the confidentiality, integrity, and availability of our data.
4. PCI DSS (Payment Card Industry Data Security Standard) - If Augusta Medical Hospital processes credit card payments, we strictly adhere to the PCI DSS to secure financial transactions. Augusta Medical Hospital is committed to data security and compliance, and we achieve this through the following:
5. NIST Cybersecurity Framework (CSF) - This framework is our roadmap for cybersecurity. It helps us identify, protect against, detect, respond to, and recover from any potential incidents.
6. HIPAA (Health Insurance Portability and Accountability Act) - We strictly follow HIPAA to protect patient health information (PHI). This means we have safeguards in place to keep patient data secure.
7. ISO/IEC 27001 - We use this framework to manage our sensitive information, ensuring data is confidential, accurate, and always available.

**Conclusion**

Protecting the information systems at Augusta Medical Hospital is paramount to safeguarding patients, employees, and all stakeholders. This policy outlines a comprehensive security framework encompassing physical, administrative, and technical controls designed to mitigate risks, protect sensitive data, and ensure ongoing compliance with all relevant regulations. Security is a collaborative effort; therefore, unwavering adherence to these policies is expected from every employee, contractor, and third-party vendor to maintain the hospital's security posture and overall success.

References:

Fitzgerald, A. (2024, June 5). A Guide to Onboarding and Offboarding Employees for Risk Prevention. Secureframe. https://secureframe.com/blog/onboarding-and-offboarding

Fortinet. (2023). What Is an Insider Threat? Definition, Types, and Prevention. Fortinet. https://www.fortinet.com/resources/cyberglossary/insider-threats

Hannah, S. T., Sumanth, J. J., Lester, P., & Cavarretta, F. (2014). Debunking the false dichotomy of leadership idealism and pragmatism: Critical evaluation and support of newer genre leadership theories. Journal of Organizational Behavior, 35(5), 598–621. https://doi.org/10.1002/job.1931

Health Information Privacy. (2015, August 26). Health Information Privacy. HHS.gov. https://www.hhs.gov/hipaa/

ITGovernance. (2016). Cybersecurity Standards and Frameworks | IT Governance USA. Itgovernanceusa.com. https://www.itgovernanceusa.com/cybersecurity-standards

NIST. (2021). Security and Privacy Controls for Federal Information Systems and Organizations. NIST, 4. https://doi.org/10.6028/nist.sp.800-53r4

PCI Security Standards Council. (2024). PCI Security Standards Overview. PCI Security Standards Council. https://www.pcisecuritystandards.org/standards/

TechTarget. (n.d.). What is employee onboarding and offboarding? - Definition from WhatIs.com. SearchHRSoftware. https://www.techtarget.com/searchhrsoftware/definition/employee-onboarding-and-offboarding