Six Information Security Policies for the Hospital

Leo Newton

11/24/24

These policies outline security measures for a hospital environment, addressing crucial areas like firewall management, personnel conduct, physical security, software development, mobile device usage, and network access. The policies are informed by industry best practices and regulatory requirements, such as those outlined by HIPAA (NIST, 2024). Effective security policy implementation requires a multi-layered approach, addressing both technical and human factors (Bayuk et al., 2012).

1. Firewall Port and Service Request Management Policy

**Objectives**: To establish a standardized process for requesting and approving changes to firewall configurations, ensuring network security and minimizing risks associated with unauthorized access.

**Scope**: This policy applies to all requests for opening ports or enabling services on hospital firewalls, including internal and external network segments.

Audience: IT staff, security personnel, department heads, and any individual requesting firewall changes.

**Policy Specifics**:

* + All firewall change requests must be submitted through a designated online form, providing justification, technical details (ports, protocols, destination IPs), and the requesting department's approval.
  + Requests will be reviewed by the IT Security team, who will assess the security implications and potential risks associated with the change.
  + Approval will be based on a risk assessment, adherence to hospital security standards, and business justification. Changes deemed high-risk may require additional approvals from senior management or the Information Security Officer.
  + Approved changes will be implemented by authorized IT staff, following established change management procedures. Implementation will be documented, including date, time, and personnel involved.
  + Periodic reviews of open ports and services will be conducted to identify and close any unnecessary or unauthorized access points.

**Enforcement**: Unauthorized changes to firewall configurations will result in disciplinary action, up to and including termination of employment.

**Responsibility**: The IT Security Manager is responsible for maintaining and updating this policy.

2. Personnel/Appropriate Usage Security Policy

**Objectives**: To define acceptable user behavior regarding the use of hospital IT resources, ensuring data confidentiality, integrity, and availability.

**Scope**: This policy applies to all employees, contractors, and other individuals accessing hospital IT systems, including computers, networks, and mobile devices.

**Audience**: All hospital personnel, including medical staff, administrative staff, and IT personnel.

**Policy Specifics**:

* + Users must protect their login credentials and never share them with others.
  + Accessing patient data is restricted to authorized personnel with a legitimate need-to-know.
  + Users must comply with HIPAA regulations regarding the handling and protection of patient health information (PHI).
  + Installing unauthorized software or hardware on hospital systems is prohibited.
  + Personal use of hospital IT resources must not interfere with work duties or compromise network security. Downloading or accessing inappropriate content (e.g., illegal or offensive material) is strictly prohibited.
  + Social media usage should adhere to professional standards and avoid disclosing confidential hospital information.

**Enforcement**: Violations of this policy will result in disciplinary action, up to and including termination of employment.

**Responsibility**: The Chief Information Officer (CIO) is responsible for maintaining and updating this policy.

3. Physical and Environmental Security Policy

**Objectives**: To protect hospital facilities, equipment, and data from unauthorized access, theft, damage, and environmental hazards.

**Scope**: This policy covers all physical locations and IT assets within the hospital's control.

**Audience**: All hospital personnel, security staff, and facilities management.

**Policy Specifics**:

* + Access to restricted areas (e.g., server rooms, data centers) is limited to authorized personnel with appropriate credentials.
  + Security cameras and intrusion detection systems will be deployed in strategic locations to monitor and deter unauthorized access.
  + Visitor access will be controlled, requiring proper identification and escort by authorized personnel.
  + Environmental controls (e.g., temperature, humidity) will be maintained within acceptable ranges to protect sensitive equipment and data.
  + Physical security measures (e.g., locks, alarms) will be regularly inspected and maintained to ensure their effectiveness.
  + Data center infrastructure (e.g., power supplies, fire suppression systems) will be designed and maintained to provide redundancy and prevent data loss.

**Enforcement**: Unauthorized access or tampering with security systems will result in disciplinary action and potential legal repercussions.

**Responsibility**: The Facilities Manager is responsible for maintaining and updating this policy.

4. Software Development and Maintenance Security Policy

**Objectives**: To ensure that all software developed or maintained for the hospital adheres to secure coding practices, minimizing vulnerabilities and protecting patient data.

**Scope**: This policy applies to all in-house software development projects and maintenance activities, including web applications, mobile apps, and desktop software.

**Audience**: Software developers, IT staff, and project managers involved in software development or maintenance.

**Policy Specifics**:

* + Secure coding practices must be followed throughout the software development lifecycle (SDLC), including input validation, secure data storage, and access control mechanisms.
  + Code reviews and security testing will be conducted for all new software and major updates before deployment to production environments.
  + Open-source components used in software development must be carefully vetted for known vulnerabilities.
  + Vulnerability management procedures will be implemented to address security flaws identified in existing software.
  + Software developers will receive regular training on secure coding practices and current security threats.

**Enforcement**: Failure to comply with this policy may result in project delays or rejection of software deployments.

**Responsibility**: The Software Development Manager is responsible for maintaining and updating this policy.

5. BYOD/Mobile Device Policy

**Objectives**: To secure hospital data accessed or stored on personally owned mobile devices, while respecting employee privacy.

**Scope**: This policy applies to all personally owned mobile devices (e.g., smartphones, tablets, laptops) that connect to the hospital network or access hospital data.

**Audience**: All employees who use personal mobile devices for work-related purposes.

**Policy Specifics**:

* + Mobile devices must be protected by strong passwords or biometric authentication.
  + Devices must have up-to-date operating systems and security software installed.
  + Access to hospital data will be controlled through secure VPN connections and mobile device management (MDM) software.
  + Data stored on mobile devices must be encrypted.
  + Lost or stolen devices must be reported immediately to the IT Help Desk.
  + The hospital reserves the right to remotely wipe data from lost or stolen devices.

**Enforcement**: Non-compliance with this policy may result in restrictions on mobile device access to hospital resources.

**Responsibility**: The IT Security Manager is responsible for maintaining and updating this policy.

6. Network Wired and Wireless Policy

**Objectives**: To secure the hospital's wired and wireless networks, preventing unauthorized access and protecting data transmitted over the network.

**Scope**: This policy covers all wired and wireless network infrastructure within the hospital's control.

**Audience**: All hospital personnel, IT staff, and security personnel.

**Policy Specifics**:

* + Strong encryption (e.g., WPA2/3) must be used for all wireless networks.
  + Network access will be controlled through a combination of firewalls, access control lists (ACLs), and network segmentation.
  + Regular vulnerability scanning and penetration testing will be conducted to identify and address network security weaknesses.
  + Intrusion detection and prevention systems will be deployed to monitor network traffic for malicious activity.
  + Network devices (e.g., routers, switches) will be configured securely and regularly updated with security patches.
  + Guest wireless networks will be isolated from the main hospital network and subject to strict access controls.

**Enforcement**: Unauthorized access or attempts to compromise network security will result in disciplinary action and potential legal repercussions.

**Responsibility**: The Network Administrator is responsible for maintaining and updating this policy.

References

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons, Incorporated.

National Institute of Standards and Technology (NIST). (2024). NIST Special Publication 800-66r2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-66r2>.