Leo Newton

12/28/23

#4

Organizational Security Policy Outline

1. Security Policy Goals

- Define the scope and purpose of the policy.

- Ensure alignment with healthcare regulations (e.g., HIPAA in the U.S.).

- Prioritize patient data confidentiality, integrity, and availability.

2. BYOD (Bring Your Own Device)

- Establish guidelines for acceptable personal devices.

- Implement security controls (encryption, remote wipe capabilities).

- Define a process for reporting lost or stolen devices.

3. AUP (Acceptable Use Policy)

- Outline permissible use of organizational resources.

- Educate staff on the risks of phishing, social engineering, and unsafe browsing.

- Specify disciplinary actions for policy violations.

4. NDA (Non-Disclosure Agreement)

- Require all staff and third parties to sign NDAs to protect patient information.

- Clearly define what constitutes confidential information.

- Outline legal consequences for unauthorized disclosure.

5. Password Policy

- Enforce strong password creation rules (complexity, length).

- Implement regular password change schedules.

- Introduce multi-factor authentication wherever possible.

6. Privileged User Agreement

- Identify roles with privileged access to sensitive data.

- Monitor and audit privileged account activities.

- Provide training on the responsible use of privileged access.

7. Anti-Malware Policy

- Deploy and regularly update anti-malware solutions.

- Conduct regular system scans and incident response drills.

- Train staff to recognize and report potential malware incidents.

General Steps to Develop the Security Policy:

- Assess Current Security Posture: Understand where the organization currently stands in terms of security measures and risk.

- Identify Specific Health Care Regulatory Requirements: Ensure compliance with laws and regulations specific to patient data.

- Involve Stakeholders: Engage with healthcare professionals, IT staff, and legal advisors.

- Implement Training and Awareness Programs: Educate all members of the organization on their roles in maintaining security.

- Regularly Review and Update Policies: Adapt the policy to emerging threats and changing regulations.