Thomas-Shane Trippe

1.9 Assignment 1: Case Study

7/7/2025

1.9 Assignment 1: Case Study

1. What US laws, policies, standards, and baselines did you apply to this case study? Justify your answer and be thorough in your response.

To assess the effectiveness of EHR security in the U.S., I have chosen the following laws and frameworks to be applied:

- **HIPAA (Health Insurance Portability and Accountability Act) Security Rule:** This is the cornerstone U.S. regulation for safeguarding electronic protected health information, also known as ePHI. It mandates administrative, physical, and technical safeguards, aligning directly with the case s’udy's focus. HIPAA requires access controls, encryption, audit logs, and security training.
- **HITECH Act (Health Information Technology for Economic and Clinical Health Act):** Reinforces HIPPA by increasing penalties for breaches and requiring breach notifcation. It supports the meaningful use of EHRs and mandates robust security practices.
- **NIST SP 800 (800-30, 800-53, 800-66, etc.):** These provide guidelines for risk assessments, security and privacy controls, and implementation frameworks. NIST standards are widely accepted in U.S. healthcare environments and complement HIPAA requirements.
- **CISA (Cybersecurity and Infrastructure Security Agency) Health Sector Guidance:** CISA offers critical threat intelligence and mitigation strategies. Its advisories are used to strengthen healthcare system resilience.
- **FISMA (Federal Information Security Management Act):** Focused on federal systems, its risk management practices and security assessment processes serve as a model for healthcare institutions that process sensitive data.

These frameworks justify a layered approach to security, technical, administrative, and physical, and provide specific benchmarks for accountability, auditability, and resilience in the protection of electronic health records.

2. Do you agree with the suggestions offered in Section 6.4 Proposed additional security controls? Be sure to add any others that you think are needed. Justify your answer and be thorough in your response. (50 word minimum)

Yes, I agree with the proposed additional security controls in Section 6.4. The recommendations such as media disposal, privileged account control, frequent audits, strong identification methods, environmental safeguards, and offsite backups which are both necessary and consistent with HIPAA and NIST guidelines.

Additional recommendations I would add are as follows:

- **Role-Based Access Control:** Access rights should be based on job responsibilites to prevent data exposure.
- **Data Loss Prevention (DLP) systems:** These help detect and prevent the unauthorized sharing of ePHI via email or removable media.
- **Zero Trust Architecture:** This security model assumes no implicit trust inside or outside the network, requiring continuous verification of user identities and device posture.
- **Endpoint Detection Response:** Implement EDR tools for real-time detection of malicious activity on workstations and servers.

These auditions are critical because they address insider threats (which the case study highlights as a major issue), enhance automation, and close gaps left by standard perimeter defenses.

3. Based on the results of this case study, are the existing security controls effective? If not, what changes must be implemented to increase the effectiveness of the security controls? Justify your answer and be thorough in your response. (50 word minimum)

Based on the existing security controls, they are partially effective, but insufficient overall. While physical security measures were implemented and rated favorably, technical and administrative safeguards were lacking in seceral key areas:

- **Only 54.5% used multi-factor authentication,** which is a requirement under HIPAA for robust user verification.
- **Access permissions were not properly managed,** with former users still having credentials, resulting in serious vulnerabilites.
- **Backups were poorly handled,** threatening availability in the event of a data loss incident.
- **Antivirus and patching were inconsistent,** exposing systems to malware and exploitation.

To improve, the following must be implemented:

- **Comprehensive access control management,** with real-time provisioning/deprovisioning.
- **Mandatory security training programs,** tailored to each role.
- **A Security Operations Center or outsourced equivalent** for 24/7 monitoring.
- **Documented, enforced security policies** that align with HIPAA and NIST 800-66 controls.

Without these improvements, the system remains vulnerable to both accidental breaches and deliverate attacks. Security controls must be integrated and continuously evaluated, not just implemented once.