1.9 Assignment 1: Case Study

Student Name: David Smart
Date: 11/30/2025

For this assignment I will assume the case study's referral hospital setting is a U.S. hospital system (rather than the actual location). All other facts, findings, threats, and conclusions are the same. The objective of this paper is to identify and discuss the existing controls (from the study) to determine if they would be expected to be effective under the U.S. healthcare expectations and recommend improvement changes to reach U.S. applicable laws, standards, and baselines.

1. **What US laws, policies, standards, and baselines did you apply to this case study? Justify your answer and be thorough in your response.**
   - When I "moved" the case study to the United States, I utilized U.S. privacy and security requirements for ePHI and leveraged well-known U.S. cybersecurity baselines that can be mapped to the hospital EHR.
   - **HIPAA (Privacy Rule & Security Rule)**
     - I first chose to apply HIPAA as it is the main US law that deals with how covered entities and their business associates need to handle ePHI. As for the EHR threats in this case study, it includes access by unauthorized users, lack of encryption, lack of backup, and weak access permissions. In the U.S., these directly correlate to the required safeguards (administrative, physical, and technical) as required by HIPAA and would be handled as compliance and risk management issues.
   - **HITECH Act + HIPAA Breach Notification Rule (45 CFR 164.400–414)**
     - I also selected the HITECH Act and HIPAA Breach Notification Rule since they enhance enforcement as well as mandating notifications following breaches of unsecured PHI. In a U.S. setting, these gaps (missing encryption, weak account management, poor audit trails) increase the likelihood that an incident will be a reportable breach. This fact renders prevention and detection controls (access control, logging, and incident response) even more critical.
   - **NIST SP 800-53 Rev. 5 (Controls Catalog) and NIST SP 800-53A (Assessment)**
     - I selected NIST SP 800-53 as my control baseline since it offers a catalog of security and privacy controls that is broadly accepted and used as a best practice even beyond federal systems. The issues from the case study clearly show NIST control families like Access Control (AC), Identification and Authentication (IA), Audit and Accountability (AU), Configuration Management (CM), Contingency Planning (CP), Incident Response (IR), and Personnel Security (PS). I could use NIST SP 800-53A to assess whether controls are effective as it's focused on assessing "what is implemented and how effective it is."
   - **NIST Cybersecurity Framework (NIST CSF 2.0)**
     - I also used the NIST Cybersecurity Framework because it is a "lightweight, risk-based approach" to managing cybersecurity through the five functions of Identify, Protect, Detect, Respond, and Recover. Overall, the case study's results suggest that the hospital is best in some "Protect" areas (physical security) but lacking in "Detect," "Respond," and "Recover" (auditing, incident response, and reliable backup/recovery).
   - **HHS 405(d) Health Industry Cybersecurity Practices (HICP)**
     - Last, I implemented HHS 405(d) / HICP since it is healthcare-focused guidance designed to increase cybersecurity consistency within the Healthcare and Public Health sector. HICP has practical controls that are tailored to the threats listed in the case study (i.e., social engineering/phishing, ransomware-style data loss threats, and insider abuse).

2. **Do you agree with the suggestions that are 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.**

- Yes, I agree with the recommended additional controls from Section 6.4 as they apply to the exact same "real" gaps that the study identified: weak authentication, poor auditing, and limited resilience. The study highlights how unauthorized access (93.5%) and social engineering (87.2%) were identified by hospitals as the top threats, and how lack of encryption (79.7%) and lack of backups (64.2%) were high. Thus, the recommended mitigations of proper disposal of media, ownership of privileged accounts, frequent audits, strong identification/authentication, secure configuration, and automated offsite backups are precisely the types of safeguards that would mitigate those threats. In my opinion, the best feature of Section 6.4 is that it incorporates administrative, technical, and physical controls evenly rather than relying on one of the three.

The three additional controls that I would recommend, in a U.S. hospital environment, include:

- The HIPAA Security Rule Requirements for Formal HIPAA Security Rule risk analysis and ongoing risk management.
- Job-based role-based access control (RBAC), automated provisioning/deprovisioning for terminated employees.
- Enforced multi-factor authentication on all remote access and privileged/admin access.
- Centralized security logging + alerting (SIEM), and regular audit of EHR access logs for abuse.
- A tested incident response plan (tabletop exercises) and disaster recovery testing.
- Encryption of ePHI at rest and in transit, and robust key management.
- Vendor/Business Associate oversight (including contracts, security requirements and assurance).

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.**

- In my opinion, the current controls are not effective at the moment because according to the research results, although the implementation of physical safeguards is relatively high (94%), perceived effectiveness of physical security is even more prominent (97%), while many technical and administrative safeguards were not implemented or are not uniformly followed. For example, the article mentions some basic safeguards, such as the presence of a security professional, management of access rights, deletion of users no longer using the system, backup power, and the protection of software from attackers were not established. This is a big gap in terms of a U.S.-based scenario, as HIPAA requires "reasonable and appropriate" safeguards to be in place across administrative, physical, and technical categories.

To be more effective, the most important changes I would make are:

A. Improved identity and access management (RBAC + MFA + least privilege)
B. Full user lifecycle control (immediate deprovisioning for terminated employees)
C. Better backup and recovery (automated offsite backups + regular restore testing + power redundancy)
D. Continuous auditing and monitoring (centralized logging, regular access reviews, and incident response preparedness).

If the controls are implemented consistently, the organization will be moved from "a little security exists" to a much more defensible, repeatable security posture more consistent with U.S. healthcare expectations.

References:

U.S. Department of Health and Human Services. (2024). *Summary of the HIPAA Security Rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Federal Register :: Request Access. (n.d.). Unblock.federalregister.gov. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C

U.S. Department of Health and Human Services. (2013, July 26). *Breach Notification Rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HHS 405(d). (n.d.). 405d.hhs.gov. https://405d.hhs.gov/cornerstone/hicp

NIST. (2020, September). *Security and Privacy Controls for Information Systems and Organizations*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *2.0*(29). https://doi.org/10.6028/nist.cswp.29

Get more familiar with the HITRUST Framework (HITRUST CSF®). (n.d.). Hitrustalliance.net. https://hitrustalliance.net/hitrust-framework