1.9 Assignment 1: Case Study

Paola N. Baez Hernandez

CYB 469-0
Term C202509
Section 01

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

  Applying this case study to a U.S. hospital setting, I must say that the key law is definitely the HIPAA Security Rule, which lays the groundwork for safeguarding electronic protected health information. Under HIPAA, organizations must perform risk assessments and put in place administrative, physical, and technical safeguards, including access controls, audit logs, workforce training, and encryption.

  The HITECH Act and the HIPAA Omnibus Rule strengthen HIPAA by increasing the penalties for any noncompliance and expanding the breach notification requirements. On top of that, some states have made their own data breach notification laws an example as Florida's Information Protection Act, which adds specific timelines and requirements for notifying patients and regulators.

  Several NIST standards that could be applied are:
  - NIST SP 800-66 that aims to help educate the readers on the security standards included in the HIPAA Security Rule and assist regulated entities in their implementation of the Security Rule.
  - NIST SP 800-53 provides a catalog of security controls that hospitals can select and implement. This helps to manage and secure their information systems.
  - NIST SP 800-30 gives a framework for conducting risk assessments.
  - NIST Cybersecurity Framework (CSF 2.0) helps organize activities into Identify, Protect, Detect, Respond, and Recover. This can also help to identify areas where their cybersecurity processes need improvement.

- NIST SP 800-63 offers guidance for digital identity management and multi-factor authentication (MFA). Provides technical guidelines for managing digital identity within federal agencies.

In addition, the HHS 405(d) Health Industry Cybersecurity Practices (HICP) is directly more relevant because it highlights the importance and most common dangerous cyber threats in the healthcare industry, such as phishing and ransomware. The CIS Critical Security Controls v8 provides an open, prescriptive, and practical actions for securing systems and data. Finally, ISO/IEC 27001/27002 and ISO 27799 are internationally recognized frameworks that support an information security management system and focus specifically on health data.

These laws and standards come as one, together to form the baseline that hospitals in the U.S. must use to protect their electronic health records as a requirement while staying compliant.

- **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. (50 word minimum)**

Yes, I agree with the proposed security controls listed in Section 6.4, such as proper media disposal, privileged account ownership, regular system audits, better identification and also authentication, with a strong configuration management, and automated off-site backups. These are all very essential and align well with HIPAA and industry best practices.

However, in the U.S. context, I believe additional measures that are needed:

- Stronger identity and access management (IAM): Automate account creation and termination, enforce least privilege, and require multi-factor authentication (MFA) for all staff and vendors. This helps maintain security and compliance within an organization's digital systems.
- Privileged Access Management (PAM): Monitor and record all administrator sessions to mitigate insider risk. PAM helps organizations reduce the risk of breaches, ensure compliance, and maintain accountability for privileged actions.

- Centralized monitoring and logging: Utilize SIEM tools and user behavior analytics to promptly identify unusual activity (e.g., mass access to patient files). This helps streamline operations by eliminating data silos and tool sprawl, leading to improved visibility, faster issue resolution, and better decision-making.
- Ransomware resilience: Apply the 3-2-1 backup rule, test recovery processes, and deploy endpoint detection and response (EDR).
- Vendor and third-party risk management: Ensuring all business associates comply with HIPAA through contracts and regular reviews.
- Continuous training and awareness: Provide the staff with constant security awareness programs and phishing simulations to reduce any social engineering risk.
- Zero-trust segmentation: Separate networks for EHR systems, labs, imaging, admin, and guest access to reduce lateral movement in case of an attack.
- Configuration and MChange management: Apply CIS benchmarks to servers and databases and monitor the integrity of critical systems.

These additions address the extreme real weaknesses identified in the study, like password sharing, poor account lifecycle management, and limited backup processes. while aligning the hospital's security posture with U.S. regulations and standards.

- **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)**

The current controls described in the case study are only somewhat partially effective. Physical safeguards, such as locked facilities, are strong. However, administrative and technical controls remain, for the most part, weak. For example, staff still share passwords, MFA is not consistently applied as it is supposed to, backups are unreliable, which is a big concern, user accounts are not always deleted when employees leave (that's extremely bad), and there is limited helpdesk or user support. From a U.S. perspective, this situation would not be considered sufficient.

To increase effectiveness, the hospital needs to:

- Conduct and update a HIPAA-required risk analysis constantly.
- Enforce unique user accounts and multi-factor authentication for all users.
- Automate account creation and removal to prevent unauthorized access.
- Implement centralized logging and ensure logs are reviewed on a regular basis.
- Strengthen vulnerability management and patching processes with clear timelines.
- Develop and test a contingency and disaster recovery plan with defined recovery time and recovery point objectives (RTO/RPO).

On the technical side, the hospital should move toward a zero-trust architecture, deploy any endpoint detection and response (EDR), and adopt the privileged access management (PAM). Operationally, the hospital should run quarterly access reviews, and hold regular security training, and test incident response and disaster recovery plans. This should be on a consistent period.

By making these changes, the hospital would move from having only “basic compliance” to achieving a more reliable, measurable, and proactive security posture that protects patient data and builds trust.

An easy, Quick 90-day Roadmap that will help structure the plan.

- Days 0–30: Conduct risk analysis, inventory data flows, enable MFA for admins/remote access, validate immutable backups, and draft breach response playbooks.
- Days 31–60: Deploy SIEM/centralized logging, enforce MFA organization-wide, implement PAM, remove stale accounts, and start network segmentation.
- Days 61–90: Roll out EDR and vulnerability management, conduct a disaster recovery test, apply CIS hardening, run phishing simulations, and hold quarterly access reviews.