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.

- A law I would implement for the Electronic Health Records (EHR) in the US is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA will define administrative, physical, and technical controls and regulate how personal health information is used and released. A Policy I would implement would be the Health and Human Services information and Security Framework to implement governance and oversight to the EHR to ensure HIPPA enforcement. A standard I would implement would be the NIST 800-53 to ensure controls are in place for privacy and security and compliance with HIPAA.

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity

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. (50 words minimum)

- While yes, I agree with the suggestions offered, such as, proper media disposal privileged account ownership, frequent system audits, identification and authentication, proper system configuration maintenance, automated offsite backup, physical security, environmental security, Uninterruptible power supply (UPS), system maintenance, and personnel security. There are more controls that the EHR systems can benefit from. The HER systems can also use backup, recovery, and ransomware protection. Healthcare is a main source of ransomware attacks having back up and recovery in place will ensure recovery without paying the ransom.

https://www.rubrik.com/insights/protecting-healthcare-hospitals-fro-ransomware-2025-guide

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 words minimum)

- Yes, the existing security controls are effective. Administrative, technical, and physical controls provide a defense-in-depth approach but can still be considered inefficient. Regarding administrative controls, while yes there are policies in place, human error will still be a weak spot for administrative controls. Regarding the technical controls, Passwords are the biggest point of security and can be used by attackers if they steal credentials. To fix the weak spot in the administrative controls, I would implement compliance checks to ensure that controls are enforced. To fix the weak spot in the technical controls, I would implement MFA and strengthen the role-based access controls to ensure employees are only able to access information needed for their job.