Topic 1 Discussion 2

Organizations must comply with different regulatory and legal policies based on the type of data the organization processes, transmits, and stores on their business application systems. Organizations must implement a security policy that supports and complies with the regulatory and legal policies for different data types and the information security systems they use. Discuss the different regulatory policies that an organization may be required to comply with, and the technical security controls requirement(s) based on the regulatory requirement(s). Examples should include all of the following, but are not limited to: HIPAA, HITECH, FDA 21 CFR , PCI-DSS, SOX, and COPPA.

Hello Class,

The Health Insurance Portability and Accountability Act (HIPAA) mandates that healthcare organizations implement stringent security measures to protect Protected Health Information (PHI). This includes administrative, physical, and technical safeguards, such as access controls, encryption, and regular risk assessments to ensure the confidentiality and integrity of health data(Office for Cicil Rights, 2024).

Similarly, the Health Information Technology for Economic and Clinical Health (HITECH) Act enhances HIPAA's requirements by promoting the adoption of electronic health records and establishing stricter penalties for data breaches(U.S. Department of Health and Human Services, 2017). Organizations must implement robust security policies that include breach notification procedures and risk analysis protocols to comply with HITECH.

In the realm of pharmaceuticals, the FDA 21 CFR Part 11 sets forth regulations for electronic records and electronic signatures, requiring organizations to ensure data integrity through validation, audit trails, and secure access controls(FDA, 2003). This is critical for maintaining compliance in clinical trials and product development.

For businesses that handle payment card information, the Payment Card Industry Data Security Standard (PCI-DSS) outlines a comprehensive set of security controls aimed at protecting cardholder data. Compliance requires organizations to implement measures such as encryption, firewalls, and regular security testing to safeguard against data breaches(Perry, 2019).

The Sarbanes-Oxley Act (SOX) imposes strict requirements on publicly traded companies to ensure the accuracy of financial reporting. Organizations must establish internal controls and procedures for financial reporting, which includes safeguarding sensitive financial data through access controls and regular audits(Staff, 2023).

Lastly, the Children's Online Privacy Protection Act (COPPA) requires organizations that collect personal information from children under 13 to implement specific privacy protections(FTC, 1998). This includes obtaining verifiable parental consent and ensuring the security of children's data through appropriate technical measures.

References:

FDA. (2003, September). *Part 11 Electronic Records Electronic Signatures Scope and Application*. U.S. Food and Drug Administration. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

FTC. (1998). *Children’s Online Privacy Protection Rule (“COPPA”)*. Federal Trade Commission; Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Office for Civil Rights. (2024, December 30). *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

Perry, Y. (2019, September 17). *Data Compliance for Regulations Around the World | NetApp*. Netapp.com. https://www.netapp.com/blog/data-compliance-regulations-hipaa-gdpr-and-pci-dss/

Staff, C. (2023, September 12). *Security and privacy laws, regulations, and compliance: The complete guide*. CSO Online. https://www.csoonline.com/article/570281/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html

U.S. Department of Health and Human Services. (2017). *HITECH act enforcement interim final rule*. US Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html