Kaden Salazar

Week 4 Reading Assignment 3

Information Assurance and Security CIS 563

Dr. Charles Butler

September 21, 2025

Laws and regulations such as HIPAA, FISMA, HITECH, and the EU Data Protection Directive significantly shape organizational security by establishing requirements for handling sensitive information and protecting systems.

The Federal Information Security Modernization Act of 2014 (FISMA) mandates federal agencies and their contractors to develop comprehensive, risk-based information security programs (EC-Council, 2020). Key provisions include periodic risk assessments, development of policies and procedures, security awareness training, annual testing and evaluation of controls, incident response procedures, and continuity-of-operations planning (FISMA, 2014). FISMA emphasizes quantitative risk ratings and reporting compliance, with modernized practices codified under FISMA 2014 to enhance continuous monitoring and reduce inefficient reporting.

HIPAA governs the protection of personal health information (PHI) in the U.S. healthcare system. Its provisions require standardized electronic transactions, unique identifiers, and security measures. The Privacy Rule under HIPAA gives patients rights over their PHI and mandates federal protections for this information (HIPAA, 1996).

HITECH expands HIPAA's scope by imposing stricter security and privacy requirements on business associates handling PHI. It introduces breach notification obligations, higher penalties for willful neglect, stronger patient rights to access and restrict records, and limits on selling PHI or using it for marketing (HITECH, 2009).

EU Data Protection Directive, modernly know as EU Data Protection Regulation (GDPR), sets privacy and data protection rules for individuals in the European Union (EU) and European Economic Area (EEA). Organizations processing personally identifiable information (PII) must implement data protection by design and default, apply pseudonymization or anonymization, and comply with cross-border data transfer requirements (General Data Protection Regulation, 2019). GDPR enhances individual control over personal data and enforces compliance globally for entities handling EU citizens' data (EC-Council, 2020).

Together, these laws and regulations require organizations to implement structured security programs, protect sensitive information, train personnel, monitor systems continuously, and respond effectively to incidents, ensuring both legal compliance and the safeguarding of data.

References

EC-Council. (2020-11-01). Certified Chief Information Security Officer (CCISO) Version 3 eBook Ed. 3, 3rd Edition. [[VitalSource Bookshelf version]]. Retrieved from vbk://9781635673999

Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3024 (2014). https://www.govinfo.gov/app/details/PLAW-113publ283.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), (2016).

Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 115 (2009).

Health Insurance Portability and Accountability Act (FISMA) of 1936. Pub. L. No. 104-191, § 264, 110 Stat. (1936).