Topic 2 Discussion 2

Payment card industry (PCI) compliance refers to the standards businesses must follow to ensure the protection of cardholder credit card data. The purpose of the Health Insurance Portability and Accountability Act (HIPAA) is to protect health care information. What are the most common PCI and HIPAA violations? What are the differences between HIPAA and PCI compliance?

Hello Class,

Understanding the most common violations of Payment Card Industry (PCI) compliance and the Health Insurance Portability and Accountability Act (HIPAA) is crucial for organizations handling sensitive data. Among the most frequent PCI violations are the failure to encrypt cardholder data during transmission, not maintaining a secure network, and inadequate access control measures. These lapses can lead to significant data breaches, exposing cardholder information to unauthorized access. On the other hand, common HIPAA violations include snooping on healthcare records, improper disposal of protected health information (PHI), and lack of employee training on privacy policies(Alder, 2025). For instance, incidents such as losing unencrypted devices containing PHI or failing to conduct a thorough risk assessment are prevalent issues that can lead to severe penalties for healthcare organizations(Fortinet, 2023).

The differences between HIPAA and PCI compliance are notable. HIPAA is a federal law designed to protect the privacy and security of health information for U.S. residents, focusing specifically on PHI. In contrast, PCI compliance is a set of security standards created by the payment card industry to protect cardholder data globally, primarily aimed at reducing fraud related to credit card transactions. While HIPAA is enforced by government agencies, PCI compliance is managed by private industry standards, making it a more flexible framework that can be adapted by businesses worldwide(McKeon, 2022). Additionally, HIPAA applies strictly to healthcare entities and their business associates, whereas PCI compliance is relevant to any organization that processes credit card transactions, regardless of industry(Vanta, n.d.). Understanding these distinctions is essential for organizations to ensure they meet the necessary regulatory requirements and protect sensitive information effectively.

References:

Alder, S. (2025, January 2). *The Most Common HIPAA Violations You Should Be Aware Of*. HIPAA Journal. https://www.hipaajournal.com/common-hipaa-violations/

Fortinet. (2023). *8 Common HIPAA Violations | Fortinet*. Fortinet. https://www.fortinet.com/resources/articles/common-hipaa-violations

McKeon, J. (2022). *PCI Compliance Versus HIPAA Compliance In Healthcare*. Healthtech Security; TechTarget. https://www.techtarget.com/healthtechsecurity/feature/PCI-Compliance-Versus-HIPAA-Compliance-In-Healthcare

Vanta. (n.d.). *PCI DSS and HIPAA compliance: Do you need both?* Www.vanta.com. https://www.vanta.com/resources/the-roles-of-pci-dss-and-hipaa-compliance