

Merton's theory of Unintended Consequences and Its Applicability to HIPAA

Posted on October 18, 2024

View this essay online:

<https://academic-master.com/mertons-theory-of-unintended-consequences-and-its-applicability-to-hipaa/>

Unintended consequences are the potential outcomes of a purposeful action that is not intended. Such action and its consequences can inadvertently lead to additional problems for individuals and society. Merton's theory, in this regard, highlights the importance of considering the significant interdependencies that lead to privacy breaches within the healthcare system. The potential consequences of a HIPAA privacy breach are significant and can have serious implications for the parties involved whether individuals or organizations in privacy breaches. This paper discusses Merton's theory of Unintended Consequences, its applicability to HIPAA, the potential consequences of HIPAA privacy breaches, and provisions of HIPAA related to privacy breaches.

Merton's Theory of Unintended Consequences

Robert K. Merton, a renowned American sociologist, was the first individual who analyzed the concept of "unintended consequences" in its complete manner, in 1936. Merton's theory of Unintended Consequences states that policies or actions that are designed to bring about a positive change in both the organization and society can have both intended and unintended negative consequences that may impact various aspects of systems or society. Merton, therefore, suggests in the theory that the failure to anticipate unintended consequences can stem from limited understanding or knowledge of the errors in analysis, interdependent parts of the issues at hand, or a reliance on past behaviours that may no longer be applicable (Garfield, 2004). Overall, Merton in the theory of unintended consequences stresses the significance of taking into consideration the potential outcomes of unintended actions and decision-making in order to ensure that risks are mitigated and desired outcomes are achieved effectively.

Applicability of Merton's Theory to HIPAA

In the context of HIPAA and the leadership inaction's consequences when a privacy breach occurs, the Unintended Consequences theory applies by highlighting the potential negative outcomes of the purposeful actions that can arise from not addressing breaches in privacy effectively and promptly. When a privacy breach occurs and the leadership of any healthcare organization fails to take action, it leads to further breaches in the system, legal consequences, damaged trust in the healthcare system, compromised patient data, and reputational damage. Furthermore, privacy breaches can result in

financial and legal consequences for the healthcare organization such as lawsuits, fines, or exclusion of the organization from healthcare programs.

HIPAA specifically anticipates the protection of patient privacy and the consequences of the privacy breach for which it provides regulations and guidelines for the privacy and safety of individual health information (Bloomrosen et al., 2011). However, it is up to the leadership of healthcare organizations to implement and regulate guidelines to overcome the consequences of privacy breaches within an organization. The inaction of leadership not only can have financial repercussions and regulatory penalties for the organization but can also leave detrimental impacts on patient care and outcomes. Merton's theory emphasizes that the consequences of delay or inaction in addressing policy breaches can result in leadership causing serious harm to the individuals and organizations affected by the breach.

Potential Consequences of HIPAA Privacy Breach

Violation of HIPAA privacy can have potentially negative consequences both legally and ethically for both individuals as well as the organization. HIPAA privacy breaches can lead to legal penalties, damaged business reputation, and termination of employment contracts. Moreover, it can also lead to substantial prison sentences as well as fines for criminal actions and interdisciplinary actions by the employer when an individual or organization steals patient information for wrongful disclosures or financial gain with the intent to cause serious harm. Violating the regulations set forth by the HIPAA can have far-reaching criminal, reputational, and financial consequences for both individuals and organizations (Chen & Benusa, 2017).

Provisions of HIPAA

"The Health Insurance Portability and Accountability Act" (HIPAA) has provisions regarding privacy breaches and their potential consequences that aim to protect the privacy of patients' health information. One of the significant provisions of HIPAA is that healthcare organizations are required to implement safeguards and procedural guidelines in order to prevent potential privacy breaches of protected health information of individuals. These procedural guidelines include administrative, physical, and technical measures throughout the organization to control access to health information and protect information from unauthorized disclosure. In healthcare organizations, governing bodies and regulatory agencies set and enforce certain standards for the safety and quality of the care provided to patients. These standards exercised by the oversight authorities serve as guidelines for healthcare organizational settings to follow in order to make certain that they are providing the best possible care as well as establishing the overall direction and strategy of the organization (Nahra, 2008). In addition, provisions of HIPAA mandate that healthcare providers within or outside the care facilities must conduct risk assessments. This would help organizations identify any vulnerabilities and complexities in the privacy of patient's health information. Moreover, it would be a helpful measure to

address vulnerabilities that can cause potential harm to the privacy of individuals or organizations.

References

Bloomrosen, M., Starren, J., Lorenzi, N. M., Ash, J. S., Patel, V. L., & Shortliffe, E. H. (2011). Anticipating and addressing the unintended consequences of health IT and policy: A report from the AMIA 2009 Health Policy Meeting. *Journal of the American Medical Informatics Association*, 18(1), 82–90.

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, 10(2), 135–146.

Garfield, E. (2004). The unintended and unanticipated consequences of Robert K. Merton. *Social Studies of Science*, 34(6), 845–853.

Nahra, K. J. (2008). HIPAA security enforcement is here. *IEEE Security & Privacy*, 6(6), 70–72.