The Aftermath of HIPAA Violations and the Costs on U.S. Healthcare Organizations

Divakaran Liginlal
Dietrich College of Humanities & Social Sciences, Carnegie Mellon University, USA

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) established national standards for healthcare organizations in the U.S.A to protect individuals' medical records (U.S. Department of Health & Human Services, 2013a). The Health Information Technology for Economic and Clinical Health (HITECH) Act, on the other hand, seeks to accelerate the universal adoption of electronic health records, widens the scope of privacy and security protections available under HIPAA and mandates stricter enforcement. Enforcement of HIPAA is the responsibility of the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR). Mercuri (2004) describes the HIPAA legislation as a "HIPAA-potamus" that imposes huge burdens on U.S. healthcare organizations in added overhead costs for compliance. Recent enforcement actions by the OCR (U.S. Department of Health & Human Services, 2013b) highlight other significant costs arising after a breach, such as those for implementing remedial measures and penalties. In this article, we analyze costs to healthcare organizations in the U.S.A. in the aftermath of such breaches, and based on Rasmussen's SRK model of human behavior (Rasmussen, 1983), examine the causes of the breaches, and propose cost mitigation strategies.

The HIPAA Privacy Rule defines "individually identifiable health information" as information, including demographic data that relates to an individual's past, present or future physical or mental health or condition, the provision of healthcare to an individual and the associated payment information, and other information that specifically identifies the individual. A covered entity, under HIPAA, is defined as a healthcare provider, a health plan, a clearinghouse, and any healthcare provider who transmits health information in electronic form in connection with transactions. Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral is referred to as protected health information (PHI).

In routine organizational work, the Privacy Rule is implemented as policies and recommended practices. Table 1 summarizes these five important policy formulation guidelines. Their key objective is to ensure that individuals control their PHI. For instance, a covered entity must get an individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or healthcare operations. A covered entity must make reasonable efforts to request, use, and disclose only the minimum amount of PHI needed to accomplish an intended purpose. Further, patients have the right to examine and obtain a copy of their health records and to request corrections.

The HHS defines a HIPAA privacy breach as "any acquisition, access, use, or disclosure of PHI in a manner that is not permitted by the HIPAA Privacy Rule, provided that it poses a significant risk of financial, reputational, or other harm to the individual." The HITECH Act further established new security breach notification requirements that encompass covered entities and their business partners, such as physicians' lawyers and accountants.

According to Rasmussen (1983), three types of processes can cause human error in typical operational situations. Skill-based processes involve the application of a set of stored patterns of preprogrammed sequences without conscious monitoring or much thinking. Common errors in this category occur because of inattention or misplaced attention. A forgetful administrative assistant leaving medical records containing PHI in a publicly accessible location is an example of such an error. Rule-based processes apply to familiar situations and are governed by the application of a set of explicit rules or heuristics. Errors occur as a result of picking an inappropriate rule caused by misunderstood view of state or because of deficient rules. A pharmacy chain

DOI: 10.4018/978-1-4666-5888-2.ch543

Table 1. Important policy formulation guidelines of the privacy rule

Policy Guideline	Key Objective of the Policy
Communication Policy	Establish standards for the electronic transmission of health-related information and implement controls to protect the security and privacy of PHI.
De-identification Policy	De-identify PHI before sharing the information by removing identifying information such as names, addresses, and Social Security numbers.
Medical Records Policy	Establish guidelines for handling medical records, such as requiring employees to retrieve and use only the information they need for legitimate purposes, and specify roles and responsibilities of employees who need access to PHI.
Administration Policy	Appoint a privacy officer who establishes and implements privacy policies and enforces a contract with business associates related to sharing PHI.
Safeguards Policy	Implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

disclosing PHI to municipal authorities without realizing that such disclosures can be made only with a written request, unless state laws mandate otherwise, is an example. Knowledge-based processes that apply to new situations require a thought process directed by interpreted knowledge and involve reasoning and planning to arrive at a solution. Errors occur because of incomplete or inaccurate understanding of the system, confirmation bias, overconfidence, and cognitive strain. An overzealous private practitioner refusing to provide treatment records to a patient because the patient has not settled her account belongs to this category of error. The SRK model has also been classified by Reason (1990) into slips and mistakes. Slips (and lapses) are failures in the process of executing a task and represent errors associated with skill-based processes. Mistakes, on the other hand, are failures in planning or problem solving and represent errors associated with rule- and knowledge-based processes.

Prior research has shown that most privacy breaches in organizations arise from human errors (Schultz, 2005; Wood and Banks, 1993). For instance, a study reported in (Liginlal et al., 2009) analysed five years of publicly reported privacy breaches within the U.S. using Reason's error typology and concluded that human error-related incidents consistently overshadowed malicious incidents in both their number and frequency of occurrence. The study determined that despite awareness of human error as an important cause of privacy breaches, organizations paid relatively less attention to error management than to malicious attacks. Liginlal, Sim, Khansa, and Fearn (Liginlal et al., 2011) subsequently undertook a more in-depth analysis of human errors specifically in healthcare organizations. The results of interviewing privacy officers of major U.S. healthcare organizations revealed that these organizations have difficulty preventing and managing human error when these errors are systemic, belong to the category of mistakes, and are committed by clinical staff.

Most prior studies have examined only the costs incurred by healthcare organizations in the U.S.A. prior to implementing HIPAA safeguards (Khansa et al., 2012; Kilbridge, 2003; Moynihan & McLure, 2000; Williams et al., 2008). For instance, an event study method was employed in (Khansa et al., 2012) to confirm that HIPAA legislation has negatively impacted the stock market value of healthcare firms. Also, it has been shown that HIPAA places a considerable resource burden on research, thus hampering healthcare organizations' ability to carry out research in a timely and cost-effective manner (Gorby et al., 2004; O'Herrin et al., 2004; Raghavan, 2005). The key objective of this article is to study the financial aftermath of privacy breaches on healthcare organizations in the U.S.A. In this article, we first consider a simple model of the information flow in a typical healthcare organization. We then classify and analyse documented examples of HIPAA enforcement actions by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services at three stages of information flow – information collection, information processing, and information dissemination. We then consider the specific value of Rasmussen's model of human behaviour in identifying the causes of human errors that lead to HIPAA breaches. We conclude the article with an overview of cost mitigation strategies and important recommendations for healthcare managers.