Chapter 98
Maturing an Information Technology Privacy Program: Assessment, Improvement, and Change Leadership

Mike Gregory
Community Healthcare System, USA

Cynthia Roberts
School of Business and Economics, Indiana University Northwest, USA

ABSTRACT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was initially enacted as an administrative simplification to standardize electronic transmission of common administrative and financial transactions. The program also calls for implementation specifications regarding privacy and security standards to protect the confidentiality and integrity of individually identifiable health information or protected health information. The Affordable Care Act further expanded many of the protective provisions set forth by HIPAA. Since its implementation, healthcare organizations around the nation have invested billions of dollars and have cycled through numerous program attempts aimed at meeting these standards. This chapter reviews the process taken by one organization to review the privacy policy in place utilizing a maturity model, identify deficiencies, and lead change in order to heighten the maturity of the system. The authors conclude with reflection related to effectiveness of the process as well as implications for practice.

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), hereafter ("HIPAA"), was initially enacted as an administrative simplification to standardize the electronic transmission of common administrative and financial transactions. The program, administered by the Department of Health and Human Services ("DHHS") and enforced by the Office for Civil Rights

DOI: 10.4018/978-1-7998-8954-0.ch098

("OCR"), also calls for implementation specifications regarding privacy and security standards to protect the confidentiality and integrity of individually identifiable health information or protected health information, hereafter ("PHI") (Office for Civil Rights, 2015). Although health information technology is not specifically covered in any one section of the Affordable Care Act of 2010 (Public Law 111-148), hereafter ("ACA"), it is a necessary condition to enact many of its initiatives such as streamlining services, improving access and quality of healthcare, and facilitating the analysis of large amounts of data for benchmarking best practices (Fontenot, 2013). As the use of electronic data expands, the need for assurance of privacy becomes paramount. The ACA itself references HIPAA and mentions privacy throughout the entire document.

Since its implementation, healthcare organizations around the nation have invested billions of dollars and have cycled through numerous program attempts aimed at meeting these standards. As intended, the law forced the industry at large to work together towards the same goal, that is, to increase the portability of PHI securely across the wide-open cyberspace platform. This was a tall order for an industry that had focused on making data widely available on the open market without any attempt to secure its system, programs, or data interconnected by the Internet. To date, information technology has made great progress in securing private networks by making smarter appliances to process data securely, encoding plain text with stronger cipher algorithms to prevent unauthorized exposure, and adopting best industry practices in the management of data and data systems.

Nevertheless, the assurance that information is viewed, obtained, or otherwise managed legitimately and responsibly, regardless of how secure the data is stored and transmitted, remains to be a considerable challenge. For this reason, HIPAA included the requirement to implement privacy programs for the purpose of monitoring for the proper use and disclosure of PHI. To help organizations strengthen their privacy policies, procedures, and practices, organizations such as the American Institute of Certified Public Accountants have created maturity models that have been adopted into the healthcare environment to satisfy the privacy requirements from HIPAA (AICPA, 2011). With this background in mind, this chapter presents a case example of the evaluation of a privacy program within a healthcare system in the Midwestern United States, identifies its deficiencies, and discusses the role of leadership in reinvigorating the program, heighten its maturity and meet the present demands of the organization.

The effort involved an exhaustive comparison against a known maturity model (AICPA, 2011). While the current privacy program complied with the implementation specifications outlined in HIPAA, its policies, practices, and procedures for monitoring the use of Electronic Protected Health Information ("ePHI") had remained at a standstill since the law went into effect. It is worth noting that the gaps identified in the privacy program related solely to the monitoring and enforcement of its privacy policies and procedures related to the *use* of ePHI. We conclude with reflection related to the effectiveness of the process as well as implications for practice.

BACKGROUND: PRIVACY PROTECTION AND THE HUMAN FACTOR

As a HIPAA mandate, covered entities are required to perform an annual risk assessment of all administrative, physical, and technical safeguards to identify gaps in privacy and select appropriate remediation plans for each of the environments. Most companies spend millions of dollars a year in acquiring and/or implementing technology strategies not only to comply with HIPAA regulations but to meet or exceed best industry practices. The stakes are heightened whenever a regulatory body imposes fines for the