Introduction to the

HIMSS Privacy & Security Toolkit

for Small Provider Organizations

By
Lisa A. Gallagher, BSEE, CISM, CPHIMS
Kenneth G. Hartman, CISSP, CPHIMS
Robert Tennant, MA, MGMA

Introduction

All healthcare providers, regardless of size, have an obligation to their patients to protect the personal information provided or created as a result of medical care. Many legal jurisdictions have created legislation to codify the provider's obligations and to provide the patient with recourse in the event that the protected health information is mishandled. In the United States, this body of legislation is primarily HIPAA and HITECH. These laws, as well as the privacy laws of other modern countries, are all based on the well-defined best practices of the field of Information Security.

Results from the HIMSS 2010 Annual Security Survey, supported by the Medical Group Management Association (MGMA) indicated that small provider organizations are less likely to have dedicated personnel, such as a Chief Security Officer or Chief Information Security Officer. While small providers are less likely to have dedicated security or privacy staff, HIPAA does require each entity to specifically identify the individual who is ultimately responsible for the development and implementation of the security & privacy policies and procedures for the organization. The lack of IT/security staff at medical practices leaves the security function to staff who may not have the expertise and background to negotiate the complex issues surrounding the privacy and security of data. Additionally, both HIPAA and Stage 1 Criteria for the CMS Meaningful Use incentive program require healthcare organizations to conduct a security risk assessment, yet HIMSS survey results indicate that fully 33% of small provider respondents have never conducted such an assessment.

These observations point clearly to the need for external resources that are clear, concise, and tailored to the needs of small provider organizations.

As a result of the HIMSS security survey and the needs of its members, HIMSS and MGMA decided to create a special version of the Security & Privacy Toolkit focused on the needs of small provider organizations, such as solo practitioners, physician groups, or independent ambulatory practices or clinics. The Toolkit is a set of tools, white papers, analysis, best practices and other reference materials. We envision the Toolkit to be an ever-evolving reference, based on new developments in industry as well as input from our users. We hope you will find the Toolkit useful and ask you to kindly give us feedback using the following link: <LINK HERE>.

Important Responsibilities of Every Provider

Regardless of the size of your organization, corporate officers are expected to run the business according to accepted business practices and in compliance with applicable laws in an ethical manner. This is referred to as the "reasonable and prudent person" rule (Wikipedia). Every organization desires to avoid costly litigation and of course, no corporate officer would want to be found liable of negligence. When a court of law attempts to determine if certain actions or inactions constitute negligence, the concepts of *due care* and *due diligence* come into play (Conrad, Misenar and Feldman 419).

Shon Harris, one of the leading experts in information security has defined due care and due diligence as follows:

> "Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees." And, [due diligence are the] "continual activities that make sure the protection mechanisms are continually maintained and operational." (Harris 85)

The concepts of due care and due diligence are woven tightly into the HIPAA and HITECH laws. The laws spell out the minimum necessary standards of protection *(due care)* and set forth the expectation that the organization continually evaluate the adequacy and effectiveness of their information protection controls *(due diligence).* Furthermore, the expectation is that provider organizations implement these controls with the same diligent and attentive approach that other *reasonable and prudent persons* would, in similarly situated businesses, with similar resources. The HITECH act calls this "reasonable diligence:"

> "The term 'reasonable diligence' means the 'business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.'" (United States Deptartment of Health and Human Services 42749)

The HIMSS Privacy & Security Toolkit for Small Provider Organizations offers resources that can help decision makers at the smaller provider entities understand how to comply and demonstrate due care and due diligence. Networking with other small provider organizations associated with HIMSS can help you understand what your peers are doing to proactively comply and protect the trust of their patients and other stakeholders.

The Risks of Non-Compliance

An organization that fails to comply with HIPAA can face fines ranging from $100 to $50,000 per violation up to an annual maximum of $1.5 million, depending on the organization's lack of reasonable diligence and the nature of harm resulting from the violation (American Medical Association). In addition, criminal penalties are possible for individuals or entities that knowingly obtain or disclose protected health information in violation of HIPAA with penalties ranging from fines and one to ten years of imprisonment based on the misuse intent. (United States Department of Justice)

The breach notification requirements of the HITECH Act explicitly state the legislative intention to create an incentive on all covered entities to secure and protect PHI or suffer financially from the loss of customer goodwill.

> "By imposing a duty on all covered entities to notify affected individuals of breaches of protected health information, the statute and the interim final regulation place a similar burden on all covered entities to notify affected individuals and run the same risk of losing business as a result of notification. Moreover,

requiring breach notification creates an incentive on all covered entities to invest in data security improvements in efforts to minimize the possibility of reportable data breaches." (United States Deptartment of Health and Human Services 42758)

Like all organizations, small provider organizations rely on the trust of the patients that they serve in their communities. Imagine how uncomfortable it must be to explain to a long-time patient that you chose not to adopt the proper procedures to safeguard his or her personal health information.

The Benefits of Proper Information Security

Traditionally, expenditures for improved security controls have focused on the risks of not taking appropriate security precautions. Elaborate financial metrics have been developed to support the justification process (Fitzgerald). These include:

- Total Cost of Ownership (TCO),
- Return on Security Investment (ROSI),
- Economic Value Added (EVA), and
- Annualized Loss Expectancy (ALE)

In the past, information security has been viewed as an afterthought or just a compliance requirement. However, as businesses have increased their reliance on timely and accurate information, many are starting to see information assurance as a key enabler of their business, producing positive outcomes (Dhillon). Many of the required activities in a security management program, such as documenting policies and procedures, are the same steps that are essential to a quality improvement initiative.

Ezingeard, McFadzean, and Birchall in a journal article titled, *A Model of Information Assurance Benefits*, elaborate on several positive consequences of a good information assurance program. Some of these are:

- Resilient Business Processes
- Improved Customer Service
- Better Information Usage
- Improved Responsiveness
- Easier Compliance
- Better Operational Control
- Better Understanding of Business Opportunities
- Lower Costs

Layout of the HIMSS Privacy and Security Toolkit for Small Provider Organizations

In this document, we have discussed the affirmative duty of reasonable diligence that healthcare providers have toward their stakeholders to protect and secure patient health information. In addition, we have discussed the risks and business benefits of doing so. This introduction discusses the "why;" the remainder of the toolkit will provide you with valuable resources that show "what" you need to comply with, and "how" to ensure that you are meeting every compliance requirement and creating competitive advantage as a result.

The HIMSS Privacy and Security Toolkit for Small Provider Organizations is organized as follows:

Introduction/Background/Compelling Argument for Action

CMS Meaningful Use - Stage 1, Privacy and Security

ARRA/HITECH - New Privacy and Security Requirements

HIPAA

Other Privacy and Security Resources

- Risk Analysis
- Fundamentals of Security Auditing
- Specific Materials For Small Entities

Research/Data

- HIMSS Annual Security Survey

Information for the Executive/Key Decision Maker

References

American Medical Association. HIPAA Violations and Enforcement. n.d. 26 December 2010 <http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.shtml>.

Conrad, Eric, Seth Misenar and Joshua Feldman. CISSP Study Guide. Burlington, MA: Syngress, 2010.

Dhillon, G. "The Challenge of Managing Information Security - Guest Editorial." International Journal of Information Management (2004): 3-4.

Ezingeard, Jean-Noel, Elspeth McFadzean and David Birchall. "A Model of Information Assurance Benifits." Information Systems Management (Spring 2005): 20-29.

Fitzgerald, Michael. Security and Business: Financial Basics. n.d. 26 December 2010 <http://www.csoonline.com/article/394963/security-and-business-financial-basics>.

Harris, Shon. CISSP All-in-One Exam Guide. Emeryville, CA: McGraw-Hill/Osborne, 2003.

United States Department of Justice. SCOPE OF CRIMINAL ENFORCEMENT UNDER 42 U.S.C. § 1320d-6. 1 June 2005. 26 December 2010 <http://www.justice.gov/olc/hipaa_final.htm>.

United States Deptartment of Health and Human Services. "Breach Notification for Unsecured Protected Health Information; Interim Final Rule." Federal Register 24 August 2009: 42740-42770.

Wikipedia. 26 December 2010. 26 December 2010 <http://en.wikipedia.org/wiki/Information_security>.