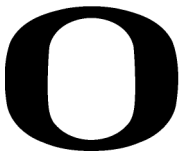
Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management and the Graduate School of the University of Oregon in partial fulfillment of the requirement for the degree of Master of Science

Information Security Policies and Governance to Safeguard Protected Health Information

CAPSTONE REPORT

Christi Noyes
Business Analyst
University of Arizona

University of Oregon
Applied Information Management
Program

July 2011

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Information Security Policies and Governance to Safeguard Protected Health Information

Christi Noyes

University of Arizona

Abstract

Healthcare organizations must comply with the Health Insurance Portability and Accountability Act of 1996 and develop information security policies that ensure the confidentiality, integrity, and accessibility of sensitive information; however guidelines are vague. This bibliography identifies policies and describes information security governance strategies designed to ensure compliance. Organizations must create a leadership committee to (a) assess current policies, (b) oversee policy enforcement, (c) note the effects of internal and external influences, and (d) maintain currency.

Keywords: ePHI security, healthcare information security, HIPAA, HIPAA security rule, information security, information security breach.

Table of Contents

List of Tables and Figures

Tables

Figures

Introduction to the Annotated Bibliography

Problem

According to Wu (2007), "health records are among the most sensitive pieces of information about us. The results of an unauthorized disclosure of health records could be devastating" (p. 1). As the public became aware of the potential negative consequences should this type of information be unsecure, a demand for control of disclosure became evident (Yee, 2006). As a result, the U.S. Congress addressed this concern as part of a larger initiative called the Health Insurance Portability and Accountability Act of 1996, or HIPAA (Wu, 2007). Sensitive and confidential records are now defined as Protected Health Information (PHI), and this HIPAA legislation outlines certain information security governance requirements needed to ensure that ePHI is protected (Hill, 2009).

Information security – or, INFOSEC – has become an important aspect of everyday life for the information manager (Leo, 2005). One of the major reasons for this is the pervasiveness of fraud, perpetrated by hackers, identity thieves, and even trusted employees. Information security typically employs three elements with which to formulate policy: confidentiality, integrity, and availability (CIA) (Scholl & National Institute of Standards and Technology, 2008). These same elements are used regarding health information and play a vital role in upholding the tenants of HIPAA (Scholl & N.I.S.T., 2008). The possibility of sensitive or confidential information being used in inappropriate or even unlawful ways is ever-present and measures must be taken to prevent instances as much as possible (Wu, 2007). As the backbone of a trusted information resource, information security is responsible for ensuring the security of ePHI and upholding the regulations of the established laws. To that end, Raggad (2010) says:

> The use of the security standards will improve the Medicare and Medicaid programs, and other federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. (p. 672)

Awareness of HIPAA regulations is essential (Harman, 2005). Although the Security Rule became effective on April 20, 2005, it is still not considered a success (Hoffman & Podgurski, 2007). Information is prevalent about issues such as regulation applicability, cost, and scope of required policy and procedure reforms; delaying the necessary actions to comply increases the risk of enduring penalties (Huston, 2001).

Purpose

The purpose of this scholarly annotated bibliography is to provide information that may help service organizations in the healthcare industry better design information security policies related to electronic protected health information (ePHI), within the context of the 1996 Health Insurance Portability and Accountability Act (Beaver & Herold, 2004). Focus is on policies that concern the confidentiality, integrity, and accessibility of ePHI (Raggad, 2010; Tipton & Krause, 2000c). The goal is to identify and organize literature that examines security policies needed across today's health care enterprise (Beaver & Herold, 2004) designed to address four related areas: (a) policies that define the role of information security governance within a health care organization, (b) policies that provide data security specific to the confidentiality, integrity, and availability of protected health information (Huston, 2001), (c) policies that avoid the consequences of security breaches involving ePHI (Sullivan, 2004), and (d) problems that healthcare organizations are facing when implementing changes to conform with the new regulations (Choi, Capitan, Krause, & Streeper, 2006). The context of the study is limited to

healthcare service organizations and framed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (Axelrod, Bayuk & Schutzer, 2009; Scholl & N.I.S.T., 2008).

Research Questions

Main question. What are the major information security policies needed in a healthcare service company in relation to the protection of patients' electronic protected health information (ePHI)?

Sub-questions.

- What is the role of information security governance within an organization (and particularly within a healthcare organization)?
- What organizational policies are needed to address the requirements of ensuring ePHI is secure as stipulated by the HIPAA Security Rule concerning (a) confidentiality, (b) integrity, and (c) accessibility of this data (Wylder, 2004)?
- What organizational policies are needed to avoid (or limit) the consequences of security breaches involving ePHI (Geffert, 2004)?
- What problems are healthcare organizations facing when implementing regulations stipulated by the HIPAA Security Rule (Choi, Capitan, Krause, & Streeper, 2006)?

Significance

The HIPAA law pertaining to the security of electronic protected health information (ePHI) is portioned into two sections: the Privacy Rule, and the Security Rule. The need for this new legislation governing the availability, integrity, and confidentiality of ePHI became apparent after several cases of unauthorized access gained public attention (Tipton & Krause, 2000a). In addition, lawmakers noted that employees who left one company and were hired by another were

not allowed to continue health coverage without a time gap (Raggad, 2010). Hence, the 1996 HIPAA legislation includes the "portability" of the employees' health insurance, in addition to the protected health information privacy and security rules (Tipton & Krause, 2000a).

Included in the Security Rule are specific parameters under which healthcare service organizations like health insurance plans and providers (officially named "covered entities") must design their information security policies to meet the requirements of the law (Tipton & Krause, 2003). Many of these service entities were surprised by these new requirements for data protection relating to ePHI and the timelines involved to achieve these new standards (Scholl & NIST, 2008). With the passage of the law, they found themselves scrambling to develop and institute new policies and protocols for meeting the requirements in the time allowed (Scholl & NIST, 2008). Even after the deadlines for implementation, many companies were struggling with how HIPAA affected them and the business policies/procedures that would need to be created and/or revised to ensure compliance (Mercuri, 2004). Regarding this, Choi, Capitan, Krause, and Streeper (2006) say "organizations may have a difficult time interpreting exactly what HIPAA security standards mean to their company and what exactly constitutes compliance" (p. 62). However, as noted by Brusil and Harley (2002), information security can provide an invaluable resource to these same health organizations if their patients are confident that their ePHI is not being unusually compromised.

Audience

The audience for this study is personnel directly responsible for creating and implementing security policies and procedures relating to patients' protected data. Additionally, members of healthcare service organizations at large would also benefit. These positions are listed and briefly described below:

- Information Security Manager – The Information Security manager serves as the process owner for all on-going activities that serve to provide appropriate access to and protect the confidentiality and integrity of patient, provider, employee, and business information in compliance with organizational policies and standards (Informatics Review, 2008). The major way in which this management role would benefit from this study is gaining greater knowledge on how to more securely protect sensitive data on proprietary networks. In addition, if these managers worked for a healthcare service organization governed by the rules outlined by HIPAA, they could gain additional insight into abiding by these regulations (Raggad, 2010).
- Information Technology Manager – "Computer and information systems managers plan, coordinate and direct research, and design the computer-related activities of firms" (McKay, 2010, para. 1). As with Information Security Managers, this position would benefit by gaining more knowledge about security management, but also would be able to participate in decision made in the formation technology hierarchy for their organization (Raggad, 2007).
- Healthcare service providers – While a broad range of descriptions could be used to describe members of this group, their common function is to provide a service or product to patients whom they serve. These members could be individuals such as doctors, and hospital management, or organizations such as companies that provide durable medical equipment. Additionally, they could provide the service of healthcare insurance. All of these entities would benefit from this study in that they would be more informed – and therefore better prepared – on how to secure their patients' ePHI

and conform to laws by which it is protected. This assists with avoiding the published consequences of violating these laws, including HIPAA (Wylder, 2004).

Delimitations

Topic scope. Wu (2007) writes that health information is one of the most sensitive pieces of information in existence and needs to be protected from potential security threats (p. 1). Even now, despite legislation requiring the use of standards pertaining to the security of health information, this protection remains a problem that can and must be solved through the implementation of information security governance policies (Choi, Capitan, Krause, & Streeper, 2006). Many of the reasons why this type of information remains unsecure and the law ignored is due to a simple ignorance or lack of authority on the part of the information security managers enlisted and entrusted to create and implement these new policies (Raggad, 2010). This study is limited in scope to informing the information technology and information security team managers, as well as health service organization leadership, about the policies needed to ensure the confidentiality, integrity, and accessibility of sensitive health information, or ePHI.

Focus. Literature for this study is selected that directly addresses the area of the Health Insurance Portability and Accountability Act of 1996 and its application to information technology policies dictated by the Act's Security Rule. According to Huston (2001), health service organizations, or "covered entities" as defined by Sullivan (2004), are encountering various issues when implementing and abiding by the stated regulations. To help resolve these factors, four goals are discussed. The first goal is to provide information security managers with references that address the role of information security governance in healthcare organizations. The second goal is to provide references that explore organizational policies that provide data security specific to ePHI in relation to three elements of information security – confidentiality,

integrity, and accessibility. The third goal is to provide references that discuss organizational policies that avoid (or limit) the consequences of security breaches (or incidents) involving ePHI. The fourth, and final, goal is to provide references that discover the problems healthcare organizations are facing with implementation of the regulations found in the Security Rule within HIPAA.

While this study does not focus on the forensic investigation aspect of security breaches, it does focus on the information security policies needed to ensure unauthorized incidents involving ePHI are avoided to the highest extent possible.

Time frame. The references provided in this study were published between 1996 and 2010. While this is a large time period to cover, the prevalence of materials within the first several years after the passage of the Health Insurance Portability and Accountability Act in 1996 necessitates the inclusion of the earliest date. In addition, whenever possible, newer material is included to cover the topics of implementation issues faced by healthcare organizations, and the current situation regarding completion deadlines set forth in ensuing legislation.

Types of sources. Literature is selected from books, journals, government publications, and professional association Web sites. Government publications provide foundational information and guidance including actual verbiage and interpretation of the Health Insurance Portability and Accountability Act itself, including the Security Rule. Professional literature provides further interpretation and implementation details. Additional resources located through traditional search methods are listed and used in a study-writing capacity.

Selection criteria. To ensure applicability to the selected topic, research materials selected in the area of information security governance are limited to authors who are members

of or affiliated with professional organizations (e.g. Health Informatics Association) and U.S. government agencies (e.g. Centers for Medicare and Medicaid Services and the National Institute of Standards and Technology). Other materials include selected published books, selected professional magazines and journals (e.g. Journal of Medical Systems, Information Systems Security, and Health Informatics Journal) and selected healthcare corporations (e.g. Mayo Clinic).

Literature is also selected based on the criteria above for applicability to other areas of interest including the parameters and description of legislation, policies and procedures already implemented, and current status of regulation compliance, among others. In some cases, individual authors are evaluated based on their association in the field of information security and/or information governance as defined within the context of this study.

Reading and Organization Plan Preview

Once a potential set of references is collected, items are first categorized and then read for specific content. The reading plan assigns each selected reference in a category (or categories) as they correspond to the research questions. Then, abstracts and/or summaries are read to determine suitability and applicability to this study. References that meet the preliminary criteria are selected for use in this study and read in their entirety. At this point, literature is evaluated for credibility using the principles outlined by Bell and Smith (2009).

After the initial categorization by content area, the literature is again reviewed to determine how to best organize the presentation of information in the Annotated Bibliography. References are arranged by research question, corresponding to the same content areas used to categorize literature during the initial reading. The goal is to present the set of annotated references in a way that allows the audience to follow through a prescribed sequence: general

information and background; specific information regarding HIPAA and its security requirements; and finally closing thoughts, recommendations, and potential pitfalls associated with implementation issues. Encouraging the audience to follow this path should provide them the knowledge to formulate their own solutions to ePHI security policy development in light of the HIPAA Security Rule.

Definitions

Specialized terminology used within this scholarly annotated bibliography is mined from the research literature as well as other reference sources. These terms include vocabulary relating to information technology, health care, as well as other business phrases that are pivotal in the structure of this study. This section provides definitions to these terms to ensure their meaning and the context of their usage is clear to the audience.

Covered entity. Sullivan (2004) defines a covered entity as "a health plan, health care clearinghouse, or health care provider that transmits health information in electronic form in connection with health care transactions" (p. 3).

ePHI. Wu (2007) states that ePHI is "Protected Health Information that is transmitted or maintained in electronic media" (p. 16).

Healthcare service organizations. (see *Covered Entity*).

HIPPA. According to Choi, Capitan, Krause, and Streeper (2006), HIPAA is an acronym that stands for the Health Insurance Portability and Accountability Act, which "specifies the privacy, security, and electronic transaction standards with regard to patient information for all health care providers" (p. 58).

HIPAA Privacy Rule. Choi, Capitan, Krause, and Streeper (2006) describe the Privacy Rule as protecting "individuals' ePHI by dictating how and when a person's ePHI may be disclosed and for what reasons" (p. 58).

HIPAA Security Rule. Wu (2007) explains that the Security Rule is a part of the original HIPAA legislation that is designed to protect the integrity, confidentiality, and availability of electronic Protected Health Information (ePHI). The Security Rule requires entities covered by

HIPAA (called 'Covered Entities' here) to implement reasonable and appropriate administrative, physical, and technical safeguards to protect ePHI (p. 3).

Information governance. According to Gartner Research (2011b), "information governance is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information" (Information/data governance section, para. 1). Also known as *data governance*.

Information security. Wylder (2004) defines information security as "a plan to mitigate risks associated with the processing of information" (p. 4). In addition, Wylder (2004) goes on to say that three elements are included in the basic theory (CIA):

- Confidentiality: "The prevention of unauthorized use or disclosure of information" (p. 4).
- Integrity: "Ensuring that information is accurate, complete, and has not been modified by unauthorized users or processes" (p. 4).
- Availability: "Ensuring that users have timely and reliable access to their information assets" (p. 4).

Information security governance. Knapp, Morris, Jr., Marshall and Byrd (2009) describe information security governance as "representing the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT" (p. 500).

Information security policy. According to Knapp, Morris, Jr., Marshall, and Byrd (2009), information security policy "addresses the integrity, availability, and confidentiality of electronic data held within and transmitted between information systems and is the precondition to implementing effective deterrents" (pp. 493-494).

Information technology. According to Gartner Research (2011a), this is defined as

"…the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use" (Information technology section, para. 1).

Input/Output (I/O). Hill (2009) defines Input/Output (I/O) as "the process of moving data between the main memory of a computer and some other device, such as a piece of storage media" (p. 293).

Protected Health Information (PHI). Sullivan (2004) defines Protected Health Information (PHI) as individually identifiable information that is recorded orally or in written form by a covered entity or received by a covered entity that relates to the past, present, or future physical or mental health of an individual, health care services, or payment for health care. This includes traditional medical records as well as health care providers' personal notes and billing information (p.5).

Security breach. According to Axelrod, Bayuk, and Schutzer (2009), a security breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of …personal information" (p. 132).

Research Parameters

The purpose of this section is to describe the parameters used in framing and conducting this study. Aspects of research depicted include a detailed explanation of search strategy including specific search terms, how collected literature is recorded and then evaluated in accordance with the goals of this study, and the methodology used in analyzing and organizing the references presented in the Annotated Bibliography section of the document.

Search Report

Searches for literature are conducted in peer-reviewed journals, published books and e-books, along with official government publications. Databases searched include: Medline/PubMed, Academic Search Premier, Article First, Business Source Complete, British Library Serials, ProQuest Congressional, Project Muse, Web of Science, and Worldcat.org.

Search terms. Search terms are derived from IT-industry terminology (Tipton & Krause, 2000a, 2000b, 2003). The following key words are used:

Key Search Terms

- Health Insurance Portability and Accountability Act
- HIPAA
- information security
- information technology

Role of Information Security Governance

- data security policy
- information security governance
- information security policy
- ePHI security

- protected health information data protection

Ensuring ePHI is Secure As Stipulated by the HIPAA Security Rule

- healthcare information security
- HIPAA Security Rule

Consequences of Security Breaches Involving ePHI

- consequences of information security breach
- information security breach
- information security incident

Search results. All searches are performed through the online library portals at the University of Oregon and the University of Arizona. Specific tools include each University's catalog, article, and journal name searches. Web sites such as Google Scholar are used. Additionally, because a mandated law has significant relevance in this topic, several government publications are included, not only to explain the law and outline its parameters, but also to explain how to implement regulations and consequences of non-compliance (Scholl & NIST, 2008).

Documentation approach. All citations, notes, and other information relating to sources, searches, and general thoughts regarding this topic are written in a Microsoft Word document that is segmented according to base question. Individual pages in this document are reserved for each of the research and sub-questions, where citations of pertinent sources, topic notes, or other thoughts can be written.

Within each page, all citations and/or notes are highlighted as especially pertinent or applicable and are organized together. Next, sources and/or notes are typed in italics if they may

provide pertinent or valuable contributions to their question. If anything is deemed as irrelevant or not applicable, then it is removed from the document altogether.

Evaluation criteria. Initially, information resources are first discovered through search methods already described including – but not limited to – the Delimitations section of this document. Then, further analysis is performed regarding authority, objectivity, quality, currency, and relevance of each reference as described by Bell and Smith (2009):

- Authority – Examine author's credentials and reputation, and publisher type, specialization, and values.
- Objectivity – Assess the stated goals of the publication as seen by the author, any demonstrated bias, any hidden agenda regarding affiliations, and the overall impression of validity of the content.
- Quality – Analyze the organization, grammar, use of graphics and other visual aids, and the inclusion of documented sources. Also examine overall methodology and theories.
- Coverage – Evaluate whether the work is substantiated by other found resources, and whether there is enough material to contribute to established goals.
- Currency – Determine the publication date and the need for current information. Research if there are other versions of the same work available.
- Relevancy – Evaluate how well the reference addresses research questions and helps to fulfill the requirements of the final goal.

Reading and Organization Plan

Due to the time that has elapsed since the Health Insurance Portability and Accountability Act was passed in 1996, there is a large amount of reference material related to healthcare information security that specifically addresses the Security Rule and its parameters. In addition, the topic of information security governance contributes another large pool of literature and this is also reviewed.

While reviewing each reference for potential inclusion, pertinent information is noted as it relates to the following content areas: (a) the role of information security governance within a healthcare organization, (b) organizational policies needed to address the requirements of ensuring ePHI is secure, (c) organizational policies needed to avoid the consequences of security breaches involving ePHI, and (d) the problems healthcare organizations are facing in implementing the regulations stipulated by the legislation. Within each of these content areas, sub-content areas are also explored, and are listed below.

The first content area presents ideas relating to how information security governance provides a framework for establishing effective standards within healthcare organizations and covered entities, specifically. Sub-content areas include:

- Assessing the confidentiality, integrity and accessibility of protected health information.
- Assessing current organizational policies and attitudes regarding information security governance.
- Understanding the requirements of the HIPAA Security Rule.

Content area two presents ideas relating to implementing the necessary security polices to comply with requirements designed to ensure the security of ePHI. Sub-content areas include:

- Updating physical security requirements.
- Implementing the required elements of the HIPAA Security Rule.
- Changing organizational administrative, technical, and documentation policies to be in compliance with the HIPAA Security Rule.

Content area three presents ideas relating to organizational policies needed to avoid the potential for security breaches of data covered by the HIPAA Security Rule. Sub-content areas include:

- Potential avoidable risks.
- Vulnerabilities in organizational and technical policies.
- Specific threats and neutralizations used to combat them.

Content area four presents ideas relating to some of the roadblocks covered entities are facing when faced with implementing the HIPAA Security Rule. Sub-content areas include:

- Increased cost of upgrading infrastructure,
- Training for information security staff,
- Ignorance as to the specific applicability of the legislation.

Literature is organized in the Annotated Bibliography according to the content areas initially assigned during reading. These correspond to the research questions as listed previously in this document, with each section labeled according to question. Within each section, resources are listed alphabetically by author. Each entry includes four elements: the formal APA-formatted bibliographic citation; an excerpt from the published abstract intended to provide an overview of its content; a summary of how the reference addresses a research question associated with this study and research topic; and the specific selection criteria used to evaluate the credibility and applicability to this study based on guidelines created by Bell and Smith (2009).

The goal of organizing the literature in this manner is to facilitate the reading and understanding by members of the audience. References listed early in the section are meant to provide background and introductory information to the problem and give information security managers a base of knowledge with which to read about and implement HIPAA security guidelines. Next, specific information about HIPAA including history, applicability, and implementation is presented in the next section of the literature, again corresponding with the research questions presented earlier in this study. Finally, concluding information is presented that is meant to illustrate how potential problems with non-compliance and other factors can be avoided. Presenting literature in this manner allows the audience to progress through the learning cycle and, ultimately, to formulate ideas and solutions regarding the implementation of the new security requirements based on individual situations.

Annotated Bibliography

An annotated bibliography is a collection of citations to books, articles, and other sources, which includes a brief descriptive and evaluative paragraph, the annotation. The main role of the annotation is to describe the relevance, accuracy, applicability, and quality of the sources cited in the collection in relation to a research topic (Engle, Blumenthal, & Cosgrave, 2011). In this study, each annotated entry contains four required elements. These are: (a) the bibliographic citation, in standard APA format, (b) an excerpt from the published abstract, (c) a summary of the key points the reference provides in relation to this study, and (d) an evaluation of the credibility of the reference, based on the evaluation criteria already described. Ideas presented in the summaries are paraphrased (or quoted, where noted) from the respective reference.

References are organized in the following categories, designed to answer the primary research question: *What are the major information security policies needed in a healthcare service company in relation to the protection of patients' electronic protected health information (ePHI)?*

Category #1: The role of information security governance within the environment of healthcare organizations.

Category #2: Organizational policies needed to ensure the requirements of securing ePHI as dictated by HIPAA's Security Rule.

Category #3: Organizational policies needed to avoid the consequences of security breaches involving ePHI.

Category #4: The problems faced by healthcare organizations when implementing legislated regulations.

The Role of Information Security Governance in a Healthcare Organization

Brotby, K. (2009). *Information security governance: A practical development and implementation approach.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Abstract. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset – information – can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that is critical to organizational success and survival.

Summary. This reference provides detailed descriptions of information security governance principles, beginning with a general overview, and includes a step-by-step approach for assessing, implementing, and maintaining information security systems based on action plans and sample policies. It provides guidance on assessing current organizational polices and attitudes regarding information security governance in general and in relation to the Health Insurance Portability and Accountability Act in specific. Elements from organizations such as the Information Systems Audit and Control Association and the Information Technology Governance Institute on how to design and assess information security systems are presented. A general discussion about regulatory concerns is included, in which some of the reasons for delaying compliance are listed and explored. Also included are steps needed for the creation and implementation of information security policies that not only assist with achieving compliance, but also provide a formidable infrastructure of general security policies that can be applied to every part of the organization. Brotby suggests that management consider the outcomes of the Information Technology Governance Institute to define their expectations when planning a security system, which include strategic alignment, risk management, business process

assurance/convergence, value delivery, resource management, and performance measurement (p. 33). Information regarding designing, implementing, and monitoring an information security system is described, including setting up metrics and responding to security incidents.

Credibility. This book is written by a principal author and editor of the Information Systems Audit and Control Association's Certified Information Security Manager exam review manual. The book is one of several publications by this author related to information security risk management and governance and is the culmination of the author's twenty-five years of experience in the field.

Chute, C. G., Beck, S. A., Fisk, T. B., & Mohr, D. N. (2010). The enterprise data trust at Mayo Clinic: A semantically integrated warehouse of biomedical data. *Journal of the American Medical informatics Association, 17(2),* 131-135. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3000789/pdf/jamia002691.pdf

Abstract. Data governance enables unprecedented organization of enterprise information about patient, genomic, and research data. While facile access for cohort definition or aggregate retrieval is supported, a high level of security, retrieval audit, and user authentication ensures privacy, confidentiality, and respect for the trust imparted by patients for the respectful use of information about their conditions.

Summary. The case study illustrates the need and importance for enterprise data governance, especially in the healthcare industry. This explanation is used to emphasize the assessment of current organizational policies and attitudes toward implementing new requirements as outlined by HIPAA. The authors say, "enterprise data governance establishes and enforces policies, principles, and standards to optimize enterprise data assets…" (p. 132). Enterprise data governance is so important that Mayo attributes the confidentiality, integrity, and accessibility of protected health information to the successful system-wide implementation of its principles. Vocabularies and reference data used in Mayo's IT systems are all created and maintained by enterprise data governance, and industry standard terms and information are used whenever possible to ensure compatibility and the ability to collaborate with other organizations' systems. Data is seen as an organizational asset and its optimization is overseen by a Data Governance Committee comprised of fifteen members from all three campus locations. Roughly ten of these individuals also comprise the data stewardship program which carries out operational activities and is solely responsible for activities that improve the quality of Mayo's

data asset. “The importance of [enterprise data governance] cannot be overstated as it is charged with fundamentally improving the standardization and quality of data captured by the source systems…” (p. 132).

Credibility. The primary author is a professor of Biomedical Informatics at the Mayo Clinic, and has written or co-written books for the healthcare and health informatics industries. He is Chair of the International Standards Organization’s Technical Committee on Health Informatics and conducts research for the Mayo Clinic in the area of Health Science Research. The article is published in a peer-reviewed journal.

Glaser, J., & Aske, J. (2010). Healthcare IT trends raise bar for information security. *Journal of the Healthcare Financial Management Association, 64*(7), 40-44. Retrieved from http://ezproxy.library.arizona.edu/login?url=http://proquest.umi.com/pqdweb?did=2080606411&sid=1&Fmt=6&clientId=43922&RQT=309&VName=PQD

Abstract. A provider's ability to ensure that its IT systems are there when they are needed can be threatened by hackers, viruses, and worms. And the confidentiality, integrity, and availability of patient, personal, and business data can be threatened. Knowing the risks that healthcare IT systems could face – and increasing the security of a hospital's and physician practice's information systems in response to these risks – is critical.

Summary. Though brief, this article presents specific information and examples relating to implementation of information security governance principles. Steps include forming a steering committee to oversee all aspects of assessing current organizational policies, and detailing "the tactical implementation of IT strategy and policies" (p. 42). The committee is responsible for describing those issues missed by HIPAA but required for compliance, such as how to secure a server. The authors suggest other key positions needed regardless of the size of the organization. Other parts of the overall information security plan are outlined and detailed suggestions for specific security measures, unrelated to HIPAA, are presented as fundamental security policies for any organization. These parts include establishing governance, an incident management plan, laptop and device encryption, internet content filtering, e-mail encryption, access management, and social media policy and guidelines. Establishing governance simply entails forming a governing body that will oversee the development and implementation of new security policies. An incident management plan consists of who will be contacted under what circumstances when a breach is detected or known. Data on mobile devices such as laptops or

thumb drives need to be encrypted as theft is an easy way for protected information to be compromised. Malware in the form of viruses, worms, or phishing can be avoided if there are appropriate Internet filtering in place. Many types of communication, including patient communication and supplier exchanges, happen through e-mail and these need to be secured. The use of strong passwords needs to be implemented to ensure only authorized access to sensitive information. Finally, the use of social media sites like Facebook and Twitter in the workplace need to be addressed in formalized organizational policy.

Credibility. Dr. Glaser is vice president and chief information officer of Partners Healthcare, Boston and is a member of the Healthcare Financial Management Association. He holds a PhD in Healthcare Information Management from the University of Minnesota. Mr. Aske received his JD from Boston University and currently serves as the chief information security officer for Partners Healthcare, Boston. In addition, he is a Certified Information Systems Security Professional and is a member of the Information Systems Security Association. The article is published in a peer-reviewed industry journal.

Hayden, L. (2009). Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies. *Information Security Journal*, *18*(6), 297-305. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=mth&AN=49232884&site=ehost-live&scope=site

Abstract. Information security professionals are faced with increasing compliance obligations associated with laws, regulations, and industry standards. To mitigate inefficiencies many organizations are seeking to streamline and rationalize frameworks in ways that combine overlapping control objectives into a smaller set of controls that still meet the requirements of all frameworks included. This article discusses strategies for such rationalizations, including benefits and limits.

Summary. Defining a control as "…a process or method by which organizations regulate their own activities to achieve specific objectives" (p. 298), the author explains that controls may refer to policies or technologies that are used to oversee organizational functions such as information security management. Controls exist in different frameworks, which are "logical structures that organize individual controls into integrated sets of activities (policies and procedures) and artifacts (documentation and technologies)" (p. 298). These frameworks can be designed in a variety of ways to address the needs of government regulations. Many different frameworks can be linked by similar characteristics, creating overlapping control requirements. This enables an organization to employ the use of a template, and may help to more efficiently and completely comply with regulations more quickly. Generally, frameworks that are designed to support information security are devised to maintain or establish best practices for securing data that the covered entity is required to safeguard. As organizations expand geographically, or

enter new markets, the need to manage compliance increases due to the increase in the number of control frameworks to which they can be subject. To resolve this, many organizations have begun to support various ways in which controls contained in one framework can be reproduced in another. This is now becoming an acceptable way of dealing with multiple compliance requirements, while maintaining effective use of current policies.

Credibility. The author is a professor at the University of Texas, where he earned his PhD in Information Science, teaching on the topics of security informatics, surveillance, and privacy. He has held several positions with Cisco Systems in their Information Security department. This article appears in a peer-reviewed journal and lists a bibliography.

Knapp, K., Morris, R., Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508. Retrieved from http://www.sciencedirect.com.libproxy.uoregon.edu/science?_ob=MImg&_imagekey=B6V8G-4WSHK03-2-5&_cdi=5870&_user=2148430&_pii=S0167404809000765&_origin=&_coverDate=10%2F31%2F2009&_sk=999719992&view=c&wchp=dGLzVzb-zSkWb&md5=d076cd08ac006744577a81a4b1842f8e&ie=/sdarticle.pdf

Abstract. Using a methodology involving qualitative techniques, the authors develop an information security policy process model based on responses from a sample of certified information security professionals. The proposed model illustrates a general yet comprehensive policy process and is grounded in focus groups and feedback from industry professionals.

Summary. The role and importance of information security is quickly becoming paramount in today's connected society, and the introduction of information technology governance is playing a critical part in designing security models. Policies are important building blocks for information security policy because they provide the basis for the overall security program and provide a structure on which to implement secure practices. The authors say "the objective of policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations" (p. 494). Based on these facts, the authors suggest a framework for a corporate information security model that addresses elements including (a) the necessity of policy enforcement, (b) the cyclical nature of policy management, (c) the role of governance, and (d) the effect of internal and external influences. Limitations of the model are also discussed, including the admission that due to legal

requirements, "…regulatory requirements will likely influence organizations in the healthcare and financial industries" more than other types of organizations (p. 501). As a result, some of the identified external influences addressed in the model may affect organizations in differing degrees. Legal and regulatory requirements are specifically listed as two of these external influences that will likely cause influences, especially in the healthcare and financial industries.

Credibility. All authors hold Assistant Professor, Associate Professor, or Professor teaching positions at Auburn University, The Citadel, or the University of Tampa, Florida and all have other publications in the field. Dr. Knapp's research topics focus on information security effectiveness and he is the editor of *Cyber Security and Global Information Assurance: Threat Analysis and Response* Solutions, a peer-reviewed book. This article appears in a peer-reviewed journal.

Leo, R., (Ed.). (2005). *The HIPAA program reference handbook.* Boca Raton, Florida: Auerbach Publications.

Abstract. The handbook explains all aspects of HIPAA including system design, implementation, compliance, liability, transactions, security, and privacy, focusing on pragmatic action instead of theoretic approaches. The handbook examines: HIPAA programs and processes; HIPAA standards and the compliance of products, policies, and technology; legal impacts and liabilities; transaction requirements; and security and privacy requirements.

Summary. This reference is a collection of works written by various authors in the healthcare industry. Topics include a general overview of HIPAA, specific information regarding the Security Rule, assessing the confidentiality, integrity, and accessibility of ePHI, incorporating the HIPAA Security Rule into an existing security program, and evaluating compliance after such a program has been created. An Information Security Operation Plan (ISOP) is introduced as "an important baseline that helps with budgeting and leadership awareness regarding security management" (p. 155). It is a useful tool in gauging the progression of the security plan, status of compliance, or requesting additional resources from executive management. Its main purpose, however, is to organize the security program components into a cohesive and effective plan that contains the right controls to ensure the confidentiality, integrity, and accessibility of ePHI. Also included are example policies regarding e-mail, stewardship, access, and code of ethics. Additionally, there is valuable information on viewing HIPAA and its regulations from a patient perspective; while this is applicable to HIPAA in its entirety, organizations will find this useful in designing security policies meant to protect those same patients. Finally, the role developers, vendors, and purchasers play in HIPAA compliance is addressed, with suggestions on how each role can assist in creating appropriate policy.

Credibility. The editor of this book is a Certified Information System Security Professional and has held information security positions at several technology companies over the past twenty-three years, including NASA Mission Control, IBM, and Rockwell International. In addition, he has written several publications on information security policy, risk analysis, and disaster recovery. He is currently the Chief Information Security Officer at the University of Texas in Galveston.

Scholl, M., & National Institute of Standards and Technology (U.S.). (2008). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Abstract. The HIPAA Security Rule specifically focuses on safeguarding electronic protected health information (ePHI). All HIPAA-covered entities, which include some federal agencies, must comply with the Security Rule, which specifically focuses on protecting the confidentiality, integrity, and availability of ePHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures.

Summary. This publication, created by an entity of the federal government, summarizes HIPAA's security standards and clarifies the structure and organization of the Security Rule. Separated into six sections, the Security Rule includes requirements and recommended specifications that covered entities must address when implementing HIPAA compliance. These sections are: (a) general rules, (b) administrative safeguards, (c) physical safeguards, (d) technical safeguards, (e) organizational requirements, and (f) policies, procedures, and documentation requirements. Key activities within each section of the Security Rule are discussed in detail, along with sample questions that organizations may want to ask themselves to ensure complete consideration. These activities are grouped by their corresponding HIPAA Standard within each of the sections mentioned above. In addition, definitions and contexts for terms used within the text of the Security Rule are provided and the security standards contained within the regulation are explained in an effort to increase understanding by covered entities. The publication guides readers to other documents created by the National Institute of Standards and

Technology relating to HIPAA and its Security Rule. While this publication can be used for implementation of Security Rule standards in any organization, its main audience is information technology personnel at federal agencies.

Credibility. This reference is a government-created publication; individual authors are employed by the National Institute on Standards and Technology. The authors collaborated with others in the Centers for Medicare and Medicaid Services, which is one of the fundamental players in the administration of HIPAA legislation and is specifically responsible for enforcing its regulations.

Organizational Policies that Provide Data Security Specific to ePHI in Relation to Confidentiality, Integrity, and Availability

Axelrod, C. W., Bayuk, J. L., & Schutzer, D., (Eds.). (2009). *Enterprise information security and privacy.* Norwood, Massachusetts: Artech House, Inc.

Abstract. This reference examines what how to protect sensitive data and systems and how to comply with the burgeoning roster of data protection laws and regulations. Topics include effectiveness and weaknesses of current approaches and practical methods and processes to improve the overall security environment.

Summary. This book provides a general overview of information security and related policies, and includes information on security trends such as HIPAA and its Security Rule, and other legislation designed to protect data from unauthorized access and use. Instructions on updating general physical security requirements and how to determine and mitigate risks are also included, along with advice on how to evaluate the effectiveness of current security methods and practices. Many types of information exist and all of them can have significant bearing on how security systems are designed. Some of these types of information are personal data, corporate financial data, transaction records, tax records, and e-mail. Despite these different types,

> the bottom line is that a company's duty to provide security may come from several different sources – each perhaps regulating a different aspect of corporate information – but the net result…is the imposition of a general obligation to provide security for all corporate data and information systems. (p. 118)

Regulations to secure data (whether from HIPAA or other legislation like the Sarbanes-Oxley Act of 2002 or the Gramm-Leach-Bliley Act) are a direct result of security failures and analyzing these instances proves invaluable to preventing them in the future. Unique security

requirements for specific industries like telecommunications, healthcare, and financial services are also discussed, and recommendations for addressing these are listed.

Credibility. All authors hold advanced degrees, have published other works, and have held executive management and/or consulting positions in large organizations such as U.S. Trust, AT&T Bell Laboratories, Citigroup, and the Financial Services Technology Consortium. Additionally, Dr. Axelrod has several industry certifications and holds a teaching position at Cornell University.

Beaver, K., & Herold, R. (2003). *The practical guide to HIPAA privacy & security compliance.* Boca Raton, Florida: Auerbach Publications.

Abstract. This how-to reference explains what HIPAA is about, what it requires, and what you can do to achieve and maintain compliance. It describes the HIPAA Privacy and Security Rules and compliance tasks, focusing not on technical jargon, but on what you need to do to meet requirements.

Summary. This resource provides extensive information on HIPAA's Security Rule. It includes definitions of key terms, a compliance checklist after implementation, and topics are applicable to organizations revising information security policies to be in compliance. Key to this study is a comprehensive description on writing policies designed to satisfy HIPAA Security Rule compliance. For general Security Rule compliance, every covered entity (CE) must adhere to several rules. These are: (a) ensure the confidentiality, integrity, and accessibility of all electronic PHI that the [covered entity] creates, receives, maintains, or transmits, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of PHI, (c) protect against any reasonably anticipated uses or disclosures of PHI, (d) ensures that its workforce complies with the Security Rule, (e) comply with the Security Rule standards with respect to all electronic PHI, and (e) review and modify security measures as needed to ensure reasonable and appropriate protection of electronic PHI (p. 162).

Additionally, a link is made between compliance and changing organizational administrative, technical, and documentation policies. This book also addresses the physical requirements when building a technology infrastructure and considerations for access controls, antivirus, data backup, firewalls, passwords, e-mail, and remote access. A description of related aspects includes training, education, and management of ongoing reviews on audits designed to

maintain compliance. The inclusion of case studies (involving covered entities) illustrates some of the problems and solutions that have been overcome on the road to implementing new security policies in light of HIPAA.

Credibility. Both authors have held several information security positions in their careers including consultant and information security manager. In addition, both have other publications in the field, and hold industry certifications such as Certified Information System Security Professional, Microsoft Certified Systems Engineer, Certified Information Systems Auditor, and affiliations with universities such as Georgia Tech and Norwich University.

Brown, C. (2005). HIPAA programs: Design and implementation. *Information Systems Security, 14*(1), 10-20. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=mth&AN=16195637&site=ehost-live&scope=site

Abstract. The degree of success an organization will realize while operating under the rules of Title II of the Health Insurance Portability and Accountability Act of 1996 depends on the ability of that organization to establish an information security program that ensures consistent execution of its requirements. This article describes a program approach to deal with the security and privacy standards required by HIPAA.

Summary. After defining *program* and illustrating the difference between a program and a project, the author discusses selecting an approach that organizations need when considering HIPAA compliance. The *traditional* approach entails focusing on HIPAA compliance as the justification for the new information security policies, and then modifying the policies as new requirements are discovered. Advantages to this approach include the inability of management and staff to disagree with its implementation, and it requires less of an initial commitment of time and money to get started. The *progressive* approach looks at "…what needs to occur throughout the organization to ensure the privacy and confidentiality of patient data and the general security of all other data…to the organization and its constituents" (p.11). The main advantage of this approach is that it presents opportunities for multiple needs to be met with creative solutions. Next, steps relating to the organization and implementation of this approach are described. The goal is to address changing organizational administrative, technical, and documentation policies in an effort to be in compliance of the Security Rule and provide a recommended body of policies for ongoing administration. For the "progressive" approach, the

author gives several examples and explanations for policies to be created, such as a program charter, risk management, staff behavior, data management, physical security, and account and access management, among others.

Credibility. The author is a Certified Information Security Systems Professional (CISSP) and a Certified Information Systems Auditor (CISA). He is the Information Security Program Administrator for Independent Health, a healthcare solutions company in Buffalo, New York. Additionally, Mr. Brown has founded two separate information security consulting firms. The article is published in a peer-reviewed journal.

Brusil, P. J., & Harley, D. (2002). Medical records security. In S. Bosworth & M. Kabay (Eds.). *Computer security handbook* (4th ed.)(pp. 49.1-49.32). New York, New York: John Wiley & Sons, Inc.

Abstract. This book chapter identifies and examines the issues pertaining to privacy and security within the healthcare industry. The role of information and technology in healthcare, and the needs and challenges of privacy and security, are considered.

Summary. While providing an extensive introduction to healthcare privacy and its necessity, this chapter also presents information about the less common drivers behind the need for information security in the healthcare industry. These include political, media, public, and legal pressures, and patient expectations. Regulations such as HIPAA fall under legal pressure and the impact it has will "change that will dramatically alter the use of technology and information in the health care industry" (p. 49.11). Administrative procedures safeguards are addressed, including contingency plans, access policies, chain of trust, and training, as outlined by the Security Rule. To protect the confidentiality, integrity, and accessibility of electronic protected health information, new technologies and standards are being proposed. These new standards are applicable to any covered entity (CE) that transmits or houses protected health information. The core security model in a healthcare context (confidentiality, integrity, and accessibility) is discussed, including the inclusion of a fourth element – accountability. The authors suggest that certain responsibilities must be assigned to specific individuals so that incidents are not the result of ignorance. The chapter includes an extensive description of HIPAA and outlines the major approaches to implementing information security policies based on its Security Rule.

Credibility. Dr. Brusil has worked with many government and healthcare organizations to improve specifications and implementation of security-related products and founded an information security consulting company. He is a member of the Board of the Journal of Network and Systems Management, and has been a pioneer in developing criteria for security and assurance systems. David Harley has co-authored books on enterprise anti-virus and security protocols, and is a senior manager for the National Health Services Information Authority in the United Kingdom. He has presented at several conferences throughout his career.

Hill, D. G. (2009). *Data protection: Governance, risk management, and compliance.* Boca Raton, Florida: CRC Press.

Abstract. This article explains the vital aspects of data protection, including the special technology requirements for compliance, governance, and data security. It allows readers to assess their overall strategy, identify security gaps, determine their unique requirements, and decide what technologies and tactics can best meet those requirements.

Summary. After defining data protection, the author discusses key foundations required for effective data protection, including business continuity and disaster recovery, as they affect data availability. There are four objectives when designing and implementing an information security system:

- *Data preservation* – data must be consistent and accurate all the time, and also must be complete within acceptable limits.
- *Data availability* – the ability of I/O requests to reach a storage device and take the appropriate action.
- *Data responsiveness* – the ability of I/Os to deliver data to authorized users according to measures of timeliness that are deemed appropriate for an application.
- *Data confidentiality* – data is available only to those authorized (p. 45).

Mandates included in HIPAA legislation fall under the data confidentiality objective, but more importantly, belong with the topic of compliance, which is under the umbrella of data protection. This perspective can be simplified into two forms: “what must be done and what must not be done. Compliance is really about controlling organization behavior” (p. 75). Implementing data protection can be very complex due to the numerous regulations being

introduced through HIPAA and other legislation, and coordination of people, technology, and policies is critical to achieve and maintain compliance.

Credibility. The author has been involved in the data management industry for more than 20 years, where he has served as executive-level management and directed the implementation of new business systems based on data security. Currently, he is the principal of Mesabi Group LLC, and holds an advanced degree from the Massachusetts Institute of Technology.

Hoffman, S., & Podgurski, A. (2006). In sickness, health, and cyberspace: Protecting the security of electronic private health information. *The Berkley Electronic Press*. Retrieved from http://law.bepress.com/expresso/eps/1522

Abstract. The electronic processing of health information provides considerable benefits to patients and health care providers at the same time that it creates serious risks to the confidentiality, integrity, and availability of the data. In order to address such threats to electronic private health information, the U.S. Department of Health and Human Services enacted the HIPAA Security Rule. This article presents a critique of the Security Rule from both legal and technical perspectives.

Summary. This reference analyzes the threats to protected health information (PHI) and the general inadequacy of regulations such as HIPAA meant to deal with them. It contains four sections: (a) the introduction, (b) a detailed description of the HIPAA Security Rule, (c) a critique of the Security Rule, and (d) recommendations for improving the effectiveness and applicability of the Security Rule for covered entities. The introduction contains background information as to the need for legislation concerning healthcare information security. This includes examples of how PHI may be fraudulently used for the benefit of others not authorized to view or store sensitive information. The description of the HIPAA Security Rule contains discussions regarding the administrative safeguards, technical safeguards, physical safeguards, and enforcement guidelines required for compliance. The critique of the Security Rule includes several deficiencies that negate its effectiveness. These are: (a) the limitations of the definition of covered entity in the Privacy Rule, which directly impacts the Security Rule, (b) the limitation of the individual to view their own medical records, outside of PHI, (c) insufficient guidance on implementing required regulations necessary for compliance, and (d) the ability for individuals

who have had their PHI disclosed inappropriately to collect damages from the covered entity in violation. Recommendations by the authors for covered entities include: (a) expanding the scope of the Privacy Rule, (b) enabling individuals to receive information concerning the origins and uses of their PHI, (c) bolstering standards and implementation specifications and providing covered entities with guidance, and (d) establishing a private cause of action for aggrieved individuals (p. 27).

Credibility. Ms. Hoffman is the Associate Dean of the Case Western Reserve University School of Law. She received her JD from Harvard Law School and also holds an LL.M. in Health Law from the University of Houston. She has published more than forty works, most in health law and civil rights law. Dr. Podgurski is a Professor in the Electrical Engineering and Computer Science Department at Case Western Reserve University. His research interests include artificial intelligence, health information systems, and software engineering.

Raggad, B. G. (2010). *Information security management: Concepts and practice*. Boca Raton, Florida: CRC Press.

Abstract. Meeting the need for an authoritative and practical classroom resource, this book provides a general overview of security auditing before examining the various elements of the information security life cycle. Topics include cyber security, security risk assessments, privacy rights, HIPAA, SOX, intrusion detection systems, security testing activities, cyber terrorism, and vulnerability assessments.

Summary. This reference provides an introduction to information security including why it is important, where and when it should be applied, and which governing body should oversee its structure and implementation. The concept of the information security life cycle is introduced (p. 68), including the following six steps: (a) security planning, (b) security analysis, (c) security design, (d) security implementation, (e) security review, and (f) continual security. According to Raggad, "security planning is the foundation on which the development of a security program rests" (p. 69). Security analysis involves determining the necessary security controls to adequately protect the targeted information asset (p. 75). Once the analysis is complete, the actual security needed is devised (p. 93), and then the plan is enacted in the security implementation phase (p. 99). Security review involves approval of the overall security plan (p. 100), and continual security consists of on-going program maintenance to ensure expected effectiveness and compliance (p. 101).

Raggad discusses several elements directly related to HIPAA including, (a) description, (b) purpose, and (c) vulnerabilities. There is also a section on the Security Rule which includes (a) definition, (b) a description of its Administrative Safeguards, and (c) physical and technical safeguards. Sub-sections regarding appointing key personnel, training for organizational staff,

and creating contingency plans give advice to organizations beginning the process of compliance.

Credibility. The author is a professor of IT security at Pace University in New York. He received his PhD in Information Systems from The Pennsylvania State University. Research interests include global computing, IT management, decision support systems, and information security. Dr. Raggad has written several books regarding information security, and serves as an international consultant in information security planning and auditing.

Tipton, H. F., & Krause, M., (Eds.). (2000a). *Information security management handbook* (4th ed.). Boca Raton, Florida: Auerbach Publications.

Abstract. The Information Security Management Handbook provides the professional tools for taking the offensive in the battle against information security threats. Top experts throughout the country share their secrets of success in all security-related areas - ensuring safe and secure information systems.

Summary. This reference provides detailed information regarding many different areas of information technology. While its general purpose is to prepare readers for the Certified Information Systems Security Professional exam, it contains specific recommendations and guidelines applicable to organizations striving for HIPAA compliance. The section on security management practices includes three areas that organizations need to utilize to be successful. They are: (a) a security program needs to be created, (b) security technologies need to be sufficient to support implementation, and (c) the concept of risk management must be addressed. The security program "must communicate to the users the significance of the organization's security policies, standards, and guidelines…in addition to the value proposition that is established by complying with policy" (p. 193). The technology infrastructure upon which the security program is built must be able to support and enforce compliance, and should be overseen by executive management. Risk management involves assessing the cost and level of protection in relation to the value of the resource being protected.

Related to health care and HIPAA, the following topics are addressed: (a) history of healthcare information systems and the inherent lack of controls, (b) challenges healthcare companies face concerning their information systems, (c) obstacles companies must overcome to implement consumer-centric systems in an environment of consumer distrust of both the

healthcare industry and the technology, (d) multitude of privacy laws, (e) e-commerce and the Internet, and (f) analysis of the HIPAA security standards. Despite the date of publication, the information is still relevant as many organizations are still in a state of non-compliance and need guidance to get there.

Credibility. Mr. Tipton is an information security consultant and is a past president of the International Information System Security Certification Consortium. He was also a director of computer security for Rockwell International Corporation and was a member of the National Institute for Standards and Technology. He holds an MA in Personnel Administration from George Washington University and is a Certified Information Systems Security Professional. Ms. Krause is the Chief Information Security Officer for Pacific Life Insurance Company. She holds an MBA and is a Certified Information Systems Security Professional.

Tipton, H. F., & Krause, M., (Eds.). (2000b). *Information security management handbook* (4th ed., Vol. 3). Boca Raton, Florida: Auerbach Publications.

Abstract. Providing an overview of the information security arena, each chapter presents a wealth of technical detail. The changes in the technology of information security and the increasing threats to security from open systems make a complete and up-to-date understanding of this material essential.

Summary. The editors address issues of access controls for ensuring the integrity and security of critical business information. These include: (a) user identification and authentication, (b) access control techniques and their administration, and (c) the innovation and evolution of methods of attack on implemented systems (p. 3). Regarding the implementation of security policies designed to achieve HIPAA compliance, the editors say, "Nowhere is the use of access controls more apparently important than in protecting the privacy, confidentiality, and security of patient healthcare information" (p. 3). One of the reasons for this is the potential exposure that Protected Health Information (PHI) can have under certain circumstances. Information security programs must be able to protect this data in these instances. Before HIPAA, these systems not only did not exist, but were thought unnecessary by information technology and healthcare industry professionals. Organizations in the United States lagged behind other countries, especially within the healthcare privacy sector. With the advent of technology like the Internet, and increased threats from outsiders, in addition to legislation including HIPAA, organizational executive management is now pressured to react. Information security policy has been shaped by HIPAA and other privacy laws, and by a heightened sense of public awareness in light of highly publicized security breaches.

Credibility. Mr. Tipton is an information security consultant and is a past president of the International Information System Security Certification Consortium. He was also a director of computer security for Rockwell International Corporation and was a member of the National Institute for Standards and Technology. He holds an MA in Personnel Administration from George Washington University and is a Certified Information Systems Security Professional. Ms. Krause is the Chief Information Security Officer for Pacific Life Insurance Company. She holds an MBA and is a Certified Information Systems Security Professional.

Tipton, H. F., & Krause, M., (Eds.). (2003). *Information security management handbook* (5th ed.). Boca Raton, Florida: Auerbach Publications.

Abstract. Providing an overview of the information security arena, each chapter presents technical detail of the discussed technology and techniques. The changes in the technology of information security and the increasing threats to security from open systems make understanding of this material essential.

Summary. Achieving HIPAA compliance is not an event, but an on-going process that must be monitored over time. Essentially, it must become part of an organization's day-to-day processes. To do this, organizations must deconstruct their business in ways that allows for all of HIPAA's requirements to be addressed, and a viable interpretation of those requirements must be created and enforced. After the organization of a security team, a readiness framework can help the business determine and address any issues encountered with achieving and maintaining compliance. There are four phases to this framework: (a) current design, (b) requirements interpretation, (c) gap assessment, and (d) execution. Examining the current design involves "the construction of a matrix that documents [the] organization's current design" (p. 1760). This includes business processes, the organizational environment, and the applicability of each HIPAA requirement. Requirements interpretation involves deciding how individual HIPAA requirements should be addressed. Gap assessment entails finding where current policies, practices, and documentation fall short of HIPAA requirements. The time an organization spends conducting this step varies, depending on the size and number of locations of torganization, the technology infrastructure (number of systems and applications), and the progress that has already been made regarding security policy implementation. Execution deals with project management and reporting the completion of the project to the organization as a whole.

Credibility. Mr. Tipton is an information security consultant and is a past president of the International Information System Security Certification Consortium. He was also a director of computer security for Rockwell International Corporation and was a member of the National Institute for Standards and Technology. He holds an MA in Personnel Administration from George Washington University and is a Certified Information Systems Security Professional. Ms. Krause is the Chief Information Security Officer for Pacific Life Insurance Company. She holds an MBA and is a Certified Information Systems Security Professional.

Wu, S., (Ed.). (2007). *A guide to HIPAA security and the law*. Chicago, Illinois: American Bar Association Publishing.

Abstract. This comprehensive guide will bridge the gap between the law and information security practices. The book clearly and concisely discusses the Security Rule's role in the broader context of HIPAA, and provides useful guidance for implementing HIPAA security.

Summary. This book includes a brief introduction and history of HIPAA and its Security Rule and provides the steps required to implement HIPAA and to ensure compliance. General rules, administrative safeguards, physical safeguards, technical safeguards, and policies, procedures, and documentation are all discussed. Under administrative safeguards, the Security Rule requires the establishment and implementation of policies and procedures in the following areas (p. 28): (a) security management process, (b) assigned security responsibility, (c) workforce security, (d) information access management, (e) security awareness and training, (f) security incident procedures, (g) contingency plans, and (h) evaluation. Within each of these areas, required tenets of the Security Rule are discussed and guidelines for implementation are suggested, along with ways of tailoring and scaling the requirements based on organizational size and function. The chapter on implementation examines why organizations may not yet be in compliance, even though deadlines have already passed (p. 97).

Though the Security Rule itself does not include any specific provisions for enforcement and penalties for non-compliance, Section 262 of HIPAA outlines civil and criminal repercussions. Enforced by the Centers for Medicare & Medicaid Services, civil violations can be penalized up to $100 per incident, with a limit of $25,000 per calendar year for “all violations of an identical requirement or prohibition” (p. 102).

Credibility. The editor is a partner in the Silicon Valley law office of Cooke, Kobrick, and Wu LLP and advises clients concerning legal matters relating to regulatory compliance, security breach liability, and incident response. He received his J.D. from Harvard Law School and has authored, co-authored, or co-edited four books regarding the law and information security.

Wylder, J. (2004). *Strategic information security.* Boca Raton, Florida: Auerbach Publications.

Abstract. Publicized events have led information security to gain greater importance as part of every business' risk management strategy. Most businesses have at least a rudimentary security program in place, and many programs are evolving and growing in maturity, especially in regard to legislation and other mandates. In doing so, information security programs need to move from tactical implementations of technology to strategic partners in business.

Summary. This reference provides a brief definition and introduction of information security, and then describes organizational issues affecting structure and on-going maintenance. These include (a) changing responsibilities for the information security manager or other key management positions, (b) changing skill levels of various positions within management and other roles, and (c) changing regulations (such as HIPAA and other legislation) affecting security policy. Types of risks are introduced and discussed, including (a) infrastructure risk, (b) vendor risk, (c) technology risk, and (d) information risk.

Part of the responsibility for mitigating risk falls on personal accountability, and that is one of the basic premises of HIPAA. The author notes that not only does HIPAA require that organizations be in compliance with its governing bodies, but there is also a requirement that the organization demand compliance from staff and other users of security policies designed to uphold HIPAA regulations. The purpose is defeated if an organization appears to be compliant but then allows (in varying ways) users to circumvent the security to accomplish tasks. It is the responsibility of management to develop and apply policies that ensure that the user population is sufficiently trained to operate within the confines of the established policies, but also to understand the logic behind the existence of such policies.

Credibility. The author has an MBA from Mercer University, a BA from Georgia Tech, and has been involved in the information security industry for twenty years. He was the Chief Information Security Officer for SunTrust Bank in Atlanta, Georgia. He is a Certified Information Systems Security Professional and a Certified in Homeland Security Professional.

Yee, G., (Ed.). (2006). *Privacy protection for e-services*. Hershey, Pennsylvania: Idea Group Publishing.

Abstract. This book reports on the latest advances in privacy protection issues and technologies for e-services, ranging from consumer empowerment to assess privacy risks, to security technologies needed for privacy protection, to systems for privacy policy enforcement, and even methods for assessing privacy technologies. The current situation regarding electronic privacy protection is presented, along with the challenges and opportunities that are being faced in implementing changes.

Summary. This book examines challenges and issues faced by organizations when trying to implement any type of security for e-services, including security needed to utilize e-services in the health care industry. An overall assessment of the impact of information technology in healthcare privacy includes discussions regarding the Internet and handheld wireless devices. Other issues addressed regarding health care include the role of physicians, the presence of health care privacy concerns, technological changes, employee issues, social engineering, and intrusions by hackers and others. A discussion on mechanisms useful for addressing health care privacy reveals that technological security tools are essential and must include the information security architecture of confidentiality, integrity, and accessibility principles, and examples are given for each. To ensure confidentiality, organizations may use firewalls, encryption, database security, and physical constraints. Application-specific encryption will also ensure integrity, and virus protection will help ensure accessibility. The principle of identification is also included, with user authentication ensuring validity. Future trends in health care security are discussed, along with examples of case studies where violations occurred due to a lack of security in place.

Credibility. The author is a senior research officer in the Information Security Group in Canada. Prior to that, he spent more than twenty years at Bell-Northern Research and Nortel Networks. He received his PhD in electrical engineering from Carleton University in Ottawa, Canada. He is a senior member of the Institute for Electrical and Electronics Engineers.

Organizational Policies that Avoid (or Limit) Consequences of Security Breaches Involving ePHI

Berghel, H. (2005). The two sides of ROI: Return on investment vs. risk of incarceration. *Communications of the ACM, 48*(4), 15-20. doi: 10.1145/1053291.1053305 Retrieved from http://delivery.acm.org/10.1145/1060000/1053305/p15-berghel.pdf?key1=1053305&key2=0254295031&coll=DL&dl=ACM&ip=150.135.241.143&CFID=22462419&CFTOKEN=40524661

Abstract. Legislative mandates potentially replace CIO's primary concerns of technology risk management with the possibility of serving jail time. Topics include the implications of the confidentiality, privacy, and security aspects of legislation as it relates to IT within modern organizations, considering each piece of legislation in the order in which it was implemented.

Summary. After a brief discussion of the goals of HIPAA, the structure of the Security Rule is described, including the fact that security specifications may be labeled as required or addressable within the text of the law itself. The author explains that "an addressable specification is one that requires attention and a documented decision to implement, not implement, or provide some alternative" (p. 17). Other fundamental characteristics of the Security Rule are explained, including its relative vagueness and the consequential confusion by covered entities in attempting to gain compliance. Specific examples of how the law would apply are given in an attempt to make the regulations and their nuances clear. Sanctions for violating the Security Rule are also listed, along with a discussion of who, organizationally speaking, would be required to respond to and be accountable for any violations that are assessed. To this end, Berghel says "Under HIPAA, due diligence now includes state-of-the-art expertise in

hacking, malware, and social engineering. These are not skills over which the typical chief information officer/chief security office has mastery" (p. 18). Berghel believes that the responsibility of risk management, as described by legislation including HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley, falls squarely on the chief information officer, and the challenge will be to find people to attempt the challenge.

Credibility. The author is currently the Director of University of Nevada at Las Vegas School of Computer Science and Director of the University's Center for Cybermedia Research. He also served as the founding Director of the Center for CyberSecurity Research and is a Fellow for the Institute for Electrical and Electronics Engineers. His research interests include digital security, law enforcement, cyberterrorism and information warfare.

Geffert, B. T. (2004). Incorporating HIPAA security requirements into an enterprise security program. *Information Security Journal: A Global Perspective, 13*(5), 21-28. Retrieved from http://dx.doi.org/10.1201/1086/44797.13.5.20041101/84906.4

Abstract. HIPAA Security regulations are forcing many organizations to secure electronic individually identifiable health information. Some side benefits of such an undertaking are improving information management processes, creating a foundation for compliance with other regulations, and maintaining their level of readiness within a security program that aligns with the HIPAA security risk-based approach. This provides effective, enterprise-wide risk management.

Summary. Due to the looming deadlines for implementing HIPAA security, organizations must devise a plan that meets the requirements of the finalized Security Plan. Though most organizations begin by examining the requirements as laid out by HIPAA, a better approach is to look at generally accepted practices and industry standards in designing solutions to reduce risk and then determine if HIPAA requires any additional measures be taken. Some level of flexibility is offered in implementing the regulations because they are not so specific and this allows organizations some leverage in mitigating security risks.

A security framework requires four steps: (a) business requirements definition, (b) business impact analysis, (c) solution implementation, and (d) compliance monitoring. Business requirements definition involves deciding how specific HIPAA requirements translate to a particular business, and there are standards readily available that can assist with this goal. Business impact analysis consists of "understanding the organization's operating environment and developing a[n]…analysis that addresses risks, costs, and the complexity of compliance activities in the…environment" (p. 24). After the completion of the analysis, suitable security

principles can be arranged into workable projects for implementation. Finally, the organizations' compliance should be monitored using pre-fabricated templates.

Credibility. The author holds an MBA from the University of Pittsburgh and is currently a Principal with Deloitte's Security Services Practice. In this capacity, he has gained over thirteen years of information security experience, including designing and implementing systems for the federal government and health care organizations. He is a Certified Information Systems Security Professional and a Certified Information Security Manager. This article appears in a peer-reviewed journal.

Hoffman, S., & Podgurski, A. (2007). In sickness, health, and cyberspace: Protecting the security of private health information. *Boston College Law Review*, *48*(2). Retrieved from http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2354&context=bclr

Abstract. Based on a close reading of the Security Rule and on empirical evidence, we argue that the Rule has thus far fallen far short of fulfilling its goal of safeguarding the security of electronic health information. This article briefly describes the provisions of the Security Rule and then offers a critique of it.

Summary. After reviewing the major details comprising the HIPAA Security Rule, the authors critique its regulations and offer suggestions to combat their deficiencies. Their recommendations are distilled into a *best practices standard*, including a provision in the Privacy Rule that states that covered entities need to secure their PHI using the current *best practices* method as a way to account for changing technology and changing security threats. They suggest the rule be changed to read: "Make reasonable efforts to identify and employ best practices relating to security measures, software development, validation, maintenance, and software system administration…" (p. 10). Other suggested recommendations include: (a) evidence of best practices will likely be found in the volume of literature available (especially on-line) from many reputable organizations like the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), (b) educational materials could be distributed by professional organizations or public-interest groups, (c) the Centers for Medicare and Medicaid Services (CMS) could provide official educational materials to covered entities, (d) CMS could create and monitor a forum on their Web site for visitors to post questions and

relate resolutions to situations that may be helpful to others, and (e) the inclusion of litigation could allow the courts to decide more specific and applicable best practices guidelines.

Credibility. Ms. Hoffman is the Associate Dean of the Case Western Reserve University School of Law. She received her JD from Harvard Law School and also holds an LL.M. in Health Law from the University of Houston. She has published more than forty works, most in health law and civil rights law. Dr. Podgurski is a Professor in the Electrical Engineering and Computer Science Department at Case Western Reserve University. His research interests include artificial intelligence, health information systems, and software engineering. This article appears in a peer-reviewed journal.

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. Communications of the ACM, 47(7), 25-28. Retrieved from http://delivery.acm.org.ezproxy1.library.arizona.edu/10.1145/1010000/1005840/p25-mercuri.pdf?key1=1005840&key2=1461423031&coll=DL&dl=ACM&ip=150.135.239.97&CFID=17050031&CFTOKEN=23246176

Abstract. Though intended to reduce costs and improve patient privacy, the Health Insurance Portability and Accountability Act of 1996 has proven to be a hippopotamus-sized piece of legislation that has simply confused and confounded health care organizations. Existing computer security guidelines and programs are being used to assist with the HIPAA security deployment process to enable organizations to avoid the stiff consequences of non-compliance.

Summary. Intended to reduce costs by limiting the number of insurance-related transactions, the Health Insurance Portability and Accountability Act of 1996 has actually had the opposite effect when the cost of compliance is considered. The bulk of this cost is associated with implementing the required security to ensure that patients' data is secure, while encouraging the electronic flow of information needed to ensure a high standard of care. Existing security programs and guidelines are helping to ease the difficulty of attaining compliance by transforming technologies used in other applications into useful tools that can assist with the requirements. Though compliance is not simply a matter of tweaking a system or technology to provide a magical solution, a stepped implementation, where noncompliance issues can be dealt with individually and completely, will allow the organization to incorporate new rules and structures into current business processes. This type of approach will also allow the time for management to develop an infrastructure that addresses administrative, physical, and technological safeguards. Finally, user and patient identity management policies may be useful in

ensuring that only authorized individuals are not only using the information systems, but also that only authorized individuals (ones who actually have health insurance) are contained within those systems.

Credibility. Dr. Mercuri has been involved in the information security industry for more than ten years after receiving her doctoral degree from the University of Pennsylvania. She has written numerous articles regarding computer forensics, electronic voting, and information security. She is a senior member of the Institute of Electrical and Electronics Engineers (IEEE). This article appears in a peer-reviewed journal.

Sullivan, J. M. (2004). *HIPAA: A practical guide to the privacy and security of health data.* Chicago, Illinois: American Bar Association Publishing.

Abstract. This book sets forth the practical aspects of the Health Insurance Portability and Accountability Act of 1996, including ways to obtain, maintain, and manage medical information under HIPAA. HIPAA directs how attorneys and other professionals obtain, control, and release medical records and other health-related documents. HIPAA provides strict guidelines for protection of the confidentiality of health information.

Summary. This reference provides a comprehensive review of HIPAA including (a) an introduction and overview, (b) authorized disclosures under HIPAA, (c) disclosures not needing authorization under HIPAA, (d) administrative requirements for covered entities, and (e) penalties and enforcement. Review of the introduction and overview includes information regarding general rules for disclosing HIPAA-protected data, and the obligations of covered entities. The differences between consent and authorization are discussed and the requirements for authorization validation are described. Disclosures not needing authorization regard 'the treatment, payment, or health care operations" (p. 27) of the health care provider. Administrative requirements for covered entities involve disclosing privacy practices to patients at the time care is received, and patient acknowledgment of such receipt with a signed form, among others. The penalties and enforcement section covers filing a complaint, compliance reviews, and the various civil and criminal penalties for non-compliance.

For the purpose of this study, focus is on the various penalties associated with a complaint of violation, after an investigation has been conducted and wrongdoing has been determined. Civil penalties assigned to the covered entity vary in severity. Criminal penalties can result from several kinds of violations, and are graduated to reflect severity of the abuse. They

are imposed by the Department of Justice, instead of the Office of Civil Rights, as are civil penalties.

Credibility. The author is a lawyer specializing in health law and is a partner at the law firm of Halloran & Sage, LLP in Hartford, Connecticut. She has over eighteen years of experience working in the health care field prior to becoming a lawyer, and is now a member of the American Bar Association in the Health Law Section. She received her JD from Quinnipiac University, where she was also an assistant professor.

Problems Faced by Healthcare Organizations with Implementation of Legislated Regulations

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in heath care industry: Implementation of HIPAA and the security rules. *Journal of Medical Systems, 30*(1), 57-64. Retrieved from http://www.springerlink.com/content/035317748wrk775t/fulltext.pdf

Abstract. This paper discusses the challenges associated with privacy in health care based on the Health Insurance Portability and Accountability Act (HIPAA) and the Security Rules, including the storing and transmission of sensitive patient data in the modern health care system and current security practices that health care providers institute to comply with HIPAA Security Rule regulations.

Summary. After giving detailed descriptions of HIPAA and its Privacy and Security Rules, the authors discuss the emerging importance of electronic transmission of healthcare data in the industry; they say "computer and [electronic data interchange] are integral components of all major health care organizations in today's age" (p. 59). Since this flow of information is critical in the industry, the presence of security to protect data being transmitted is required to ensure no unauthorized access is allowed. Within the Security Rule, there are five categories in which compliance is required: (a) administrative safeguards, (b) physical safeguards, (c) technical safeguards, (d) organizational requirements, and (e) policies, procedures, and documentation requirements. Due to the number and complexity of the requirements for compliance, many organizations are delaying the necessary steps to implement information security systems and policies. The most prevalent reasons for this are (a) the sheer effort needed to begin, manage, and complete a project of magnitude, and (b) the cost associated with its

planning and implementation. Other reasons for tardiness include (c) the overall vagueness of the requirements, (d) the efficiency of implementing safeguards on day-to-day processes, and (e) the patient belief that their protected health information is, in fact, protected.

Credibility. Dr. Choi is an Assistant Professor in the Department of Computer Information Systems and Management Science at James Madison University. He has been employed by Creative Technology Ltd and Compaq Computer Corporation as Principal Engineer. He received his PhD from the University of Missouri. The other authors he credits are his students at James Madison University. This article appears in a peer-reviewed journal.

Harman, L. B. (2005). HIPAA: A few years later. *Online Journal of Issues in Nursing, 10*(2), 95-110. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=17356284&site=ehost-live&scope=site

Abstract. This article addresses the impact of the Health Insurance Portability and Accountability Act (HIPAA) several years after implementation. The rationale for HIPAA and a clarification of key terms, including covered entities, personal health information, and designated record sets, is reviewed. The impact of HIPAA at work, including increased cost and the complexities of educating employees and patients is assessed.

Summary. Changes in the health care industry as a result of HIPAA include "the application of sophisticated technologies for controlling access to personal health information, including the identification and authentication of individuals…" (p. 98). In addition, HIPAA has increased overall patient privacy though the reduction of costs associated with simplification of general health insurance and information policies has not occurred. Sharing patient data among covered entities has also been improved. In addition, provisions for homeland security and natural disasters have been implemented along with guidelines dealing with media, relatives, and other entities in the instance of one of these events.

Despite the progress that has already been made, the health care industry as a whole must make HIPAA implementation and compliance a priority in the interest of patients and health care providers. The need for patients to know and understand about privacy is increasing and with that comes more demand for better protections. And though the process to achieve and maintain compliance is complex and on-going, the goals of HIPAA will be realized as the electronic

health record becomes commonplace in the industry. “Someday HIPAA will be an integral part of clinical practice and will not be such a struggle” (p. 105).

Credibility. Dr. Harman received her PhD from The Fielding Institute. She has been an educator and health information management professional for more than thirty-five years and has directed programs in the industry at George Washington University and The Ohio State University. She has conducted her own research on health information and has served on industry committees such as the American Health Information Management Association. This article appears in a peer-reviewed journal.

Huston, T. (2001). Security issues for implementation of e-medical records. *Communications of the ACM, 44*(9), 89-94. doi: 10.1145/383694.383712. Retrieved from http://delivery.acm.org/10.1145/390000/383712/p89-huston.pdf?key1=383712&key2=7813765031&coll=DL&dl=ACM&ip=150.135.129.173&CFID=21865939&CFTOKEN=31223648

Abstract. Since telemedicine encompasses an international venue, standardization of the electronic medical record is necessary and prototypical models are being developed. Confidentiality and security of a patient's health information has always been important and with the ease of access afforded electronically, security is likely more difficult to provide without advanced planning.

Summary. Though technological advances are making the electronic health record more robust and advanced, it seems that organizations are ignoring the fact that information security must be implemented to protect the data and the people it represents. Several key issues are involved: (a) potential threat related to a security breach, (b) management and end-user education, (c) costs of operational efficiencies and money spent, (d) the sheer number of personal computers and the naivety of their users, and (e) networks that are unsecured allow any number of types of intrusions. These issues are spotlighted when highly publicized security breaches occur, and health care information security managers must become more aware.

Executive management of a health care organization has the responsibility of creating an information security program, ensuring its implementation, and overseeing its continued maintenance. To that end, Huston says, "HIPAA may help because it essentially requires that such a program exists" (p. 91). How a newly developed security system will interact with any existing framework, the future needs of the business regarding security, and detailed information

regarding the system users all need to be addressed by the executive management security team. When implementing HIPAA to achieve compliance, management should prepare a business impact analysis, an operational impact analysis, and a security plan. A security staff, with the executive management team as a governing body, will assist in policy implementation to achieve HIPAA compliance.

Credibility. Dr. Huston is an Assistant Professor at the University of Victoria in British Columbia, Canada. He received his PhD from the University of Pittsburgh and his research interests include healthcare informatics, electronic commerce, artificial intelligence, telemedicine, and human information processing. He has authored and co-authored other publications regarding healthcare informatics and information security.

Lorence, D. P., & Churchill, R. (2005). Incremental adoption of information security in health-care organizations: Implications for document management. *IEEE Transactions on Information Technology in BioMedicine, 9*(2), 169-173. doi: 10.1109/TITB.2005.847137. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1435414

Abstract. Protective regulatory efforts have been proposed to address ineffective security of patient information, with severe noncompliance penalties. Using data from a nationwide survey of health information managers, this study examines how industry-wide knowledge management trends may influence the degree of security program adoption in healthcare organizations. Results suggest that significant non-adoption of mandated security measures continues to occur across the healthcare industry.

Summary. This reference examines the results from a nation-wide survey of 13,000 certified Registered Health Information Administrators or Registered Health Information Technicians. Detailed descriptions of research methods are discussed, and based on the 10,217 responses received, "a negative association was…found between greater adoption of computerized records and reported implementation of security" (p. 172). According to the authors, this indicates that organizations are "primarily predisposed to simply ignore regulatory requirements in the face of complex or costly security measures" (p. 172).

Reasons for organizational hesitation regarding compliance are explored, including (a) misconceptions that security measures are ways in which to avoid detection by government regulators, (b) paper-based records systems are universal in health care and organizations are reluctant to abolish them in favor of computerized, secured depositories, and (c) reluctance of implementing a new system where employees would need training. Another finding is the fact that many of the organizations implemented information systems specifically used to collect and

store patient data, but did not create the necessary corresponding security personnel needed for HIPAA implementation and compliance including security managers, coordinators, officers, committees, or teams.

Credibility. Dr. Lorence is an Assistant Professor at The Pennsylvania State University. He has appointments in Health Policy and Administration, and in Information Science and Technology. He has published 32 articles on the subject of information security, healthcare policy, and information technology in healthcare. Mr. Churchill is a Senior Research Fellow at The Virtual Management Institute in Gettysburg, Pennsylvania, and specializes in information science applications in healthcare delivery and medical practice.

Suleiman, J., & Huston, T. (2009). Data privacy and security: HIPAA and small business compliance. *International Journal of Information Security and Privacy, 3*(2), 42-53. Retrieved from http://find.galegroup.com.ezproxy2.library.arizona.edu/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T002&prodId=AONE&docId=A204309630&source=gale&srcprod=AONE&userGroupName=uarizona_main&version=1.0

Abstract. This case study provides a foundation for examining aspects of information security from the perspective of the small-business IT consultant. Information sharing, while concurrently adhering to the regulations of the Health Information Portability and Accountability Act of 1996, was a significant aspect of the project as were numerous other security and privacy legislative requirements.

Summary. This case study illustrates the many aspects of delayed HIPAA compliance for small businesses including limited financial and knowledge resources, differing state and federal regulations, and inadequate computer infrastructure. International security requirements are also discussed as well as solutions appropriate for the situation. These include: (a) encryption software to protect data being transmitted between locations, or (b) removal of all identifiable patient information, "thereby insulating the research project from any unknown conflicts with privacy and security legislation" (p. 47). Low-cost encryption solutions, attractive to small businesses, are examined, including: (a) client-based e-mail, (b) server-based, and (c) hosted. Client-based e-mail uses the concept of a public key that contains the "recipe" for how to send text so that the recipient can read it. Server-based entails require a secure server to handle file transfers. In a hosted situation, a Web-based solution is offered by another party.

Credibility. Dr. Suleiman is an Associate Professor of Information Systems at the University of Southern Maine. He received his PhD in Management Information Systems from the University of Georgia. He has worked for IBM and his research interests include computer security and information systems education. Dr. Huston is a health care information technology consultant in Canada and the United States. He received his PhD in Management Information Systems from the University of Pittsburgh and has a special interest in security and privacy in health care.

Conclusions

This study identifies and describes policies that service organizations in the healthcare industry will find useful when designing information security infrastructures within the context of the 1996 Health Insurance Portability and Accountability Act's Security Rule (Beaver & Herold, 2004). Policies that uphold the tenets of information security are examined, including (a) confidentiality, (b) integrity, and (c) accessibility (Raggad, 2010; Tipton & Krause, 2000c). Design principles intended to establish organizational governance are proposed, in addition to security policies that are needed to prevent breaches (Geffert, 2004). Significant roadblocks to implementation of these policies as experienced by healthcare organizations are examined, and suggestions for overcoming them are described (Berghel, 2005). The goal is to provide covered entities with the foundation to create policies that will allow them to achieve compliance with the Security Rule as efficiently as possible (Beaver & Herold, 2004) as described in four related areas: (a) policies that define the role of information security governance within a health care organization, (b) policies that provide data security specific to the confidentiality, integrity, and availability of protected health information (Huston, 2001), (c) policies that avoid the consequences of security breaches involving ePHI (Sullivan, 2004), and (d) problems that healthcare organizations are facing when implementing changes to conform with the new regulations (Choi, Capitan, Krause, & Streeper, 2006). The literature suggests that every organization needs to start the compliance process by ensuring that adequate leadership involvement is in place (Brotby, 2009). It is at this level that the responsibility falls when implementing policies, and maintaining compliance into the future once it is achieved (Glaser & Aske, 2010). There are several areas of the Security Rule that must be addressed for covered entities to be in compliance (Scholl & NIST, 2008) and several references included in this study

suggest policies for implementation. Berghel (2005) discusses the consequences that could result from either non-compliance or a security breach, and how management is ultimately accountable for these occurrences.

Role of Information Security Governance in a Healthcare Organization

According to Brotby (2009), once an organization determines that it is responsible for becoming HIPAA-compliant, a leadership committee must be created to effectively manage the planning, implementation, and maintenance of appropriate security policies. This team may simply be executive management, or it may include several additional key individuals such as management, end-users, and others.

Data needs to be seen as an asset, and one of the major responsibilities of the governance oversight attributed to this leadership committee is to ensure its viability (Chute et al., 2010). Another part of the governance process is to assess current information security policies already in place within the organization and to create frameworks that can be applied to these various areas (Hayden, 2009). Glaser and Aske (2010) suggest that it is the role of governance to ensure that areas of needed security within the organization and pertaining to protected health information are discussed, whether or not they are specifically noted in the Security Rule. In addition, the literature suggests that information security governance must address: (a) the necessity of policy enforcement, (b) the cyclical nature of policy management, (c) the role of governance, and (d) the effect of internal and external influences (Knapp et al., 2009). Finally, it is the role of governance to keep information security systems and policies current in relation to HIPPAA (Leo, 2005).

Organizational Policies that Provide Data Security Specific to ePHI in Relation to Confidentiality, Integrity, and Availability

Brown (2005) suggests that a *progressive approach* to creating and implementing information security policies is the most efficient way of upholding the confidentiality, integrity, and availability of health-related information. This involves determining what policy changes need to be made and implemented throughout the organization to ensure that the basic information technology principles are met. Bolted on to this approach are recommendations such as: (a) updating physical security requirements and hardware, as needed (Axelrod et al., 2009), (b) providing training and education for organizational staff at every hierarchal level (Axelrod et al., 2009), and (c) achieving the goal of recognizing and addressing changing organizational administrative, technical, and documentation policies (Brown, 2005). Using these policies, covered entities can achieve compliance despite the relative vagueness of the guidelines of the Security Rule (Hoffman & Podgurski, 2006).

Other factors must be considered when designing information security policies. These include political, media, public, and legal pressures, in addition to patient expectations (Brusil & Harley, 2002). These factors must be considered to ensure that an organization is protected from backlash that could result in reputation damage (Brown, 2005). Additionally, contingency plans, access policies, and a chain of trust are all recommended as they provide a backbone on which to build successful policies (Brusil & Harley, 2002). Hill (2009) recommends that the design and implementation of any information security systems intended to aid in HIPAA compliance should include the following four objectives: (a) data preservation, (b) data availability, (c) data responsiveness, and (d) data confidentiality; he also recommends the inclusion of a complete business continuity/disaster recovery plan.

Organizational Policies that Avoid (or Limit) Consequences of Security Breaches Involving ePHI

The Security Rule includes a list of general provisions that must be addressed when covered entities are seeking compliance. Under these provisions, categorical safeguards are listed, pertaining to administrative, physical, and technical aspects. Safeguards include industry standards that would apply, which are further detailed by a set of implementation specifications. Berghel (2005) provides a summary of these general provisions to give covered entities an idea of the overarching requirements, shown in Table 1.

Table 1.

Selected HIPAA Provisions.

Safeguard 1: Administrative
Standard 1: Security Management
Implementation Specification 1: Risk Analysis (required)
Implementation Specification 2: Risk Management (required)
Implementation specification 3: Sanctions (required)
Implementation Specification 4: Information System Activity Review (required)
Standard 2: Assigned Security Responsibility
Standard 3: Work Force Security
Implementation Specification 1: Work Force Authorization and Supervision (addressable)
….
Safeguard 2: Physical
Standard 1: Facility Access Controls
Implementation Specification 1: Contingency Operations (addressable)
Implementation Specification 2: Facility Security Plan (addressable)
Implementation Specification 3: Access Controls and Validation (addressable)
Implementation Specification 4: Maintenance Records (addressable)
Standard 2: Workstation Use
Standard 3: Workstation Security
Standard 4: Device and Media Controls
Implementation Specification 1: Disposal (required)
Implementation Specification 2: Media Reuse (required)
Implementation Specification 3: Accountability (addressable)
Implementation Specification 4: Data Backup and Storage (addressable)
Safeguard 3: Technical
Standard 1: Access Control
Implementation Specification 1: Unique User ID (required)
Implementation Specification 2: Emergency Access Procedures (required)
Implementation Specification 3: Automatic Logoff (addressable)
Implementation Specification 4: Encryption and Decryption (addressable)
Standard 2: Audit Controls
….
Requirement 1: Organizational
Requirement 2: Policies, Procedures, and Documentation

Based on these general provisions, the covered entity must address and execute policies that satisfy the implementation specifications that are marked as *required. Addressable* items must be evaluated and then a documented decision is made to implement, not implement, or find an alternative (Berghel, 2005). Compliant organizations can therefore be held accountable for the implementation of the *required* specifications, and there is a process by which anyone can file a formal complaint with the Office of Civil Rights if he/she feels that these general provisions were not upheld. Figure 1 is a graphical depiction of this process (U.S. Department of Health & Human Services, n.d.).

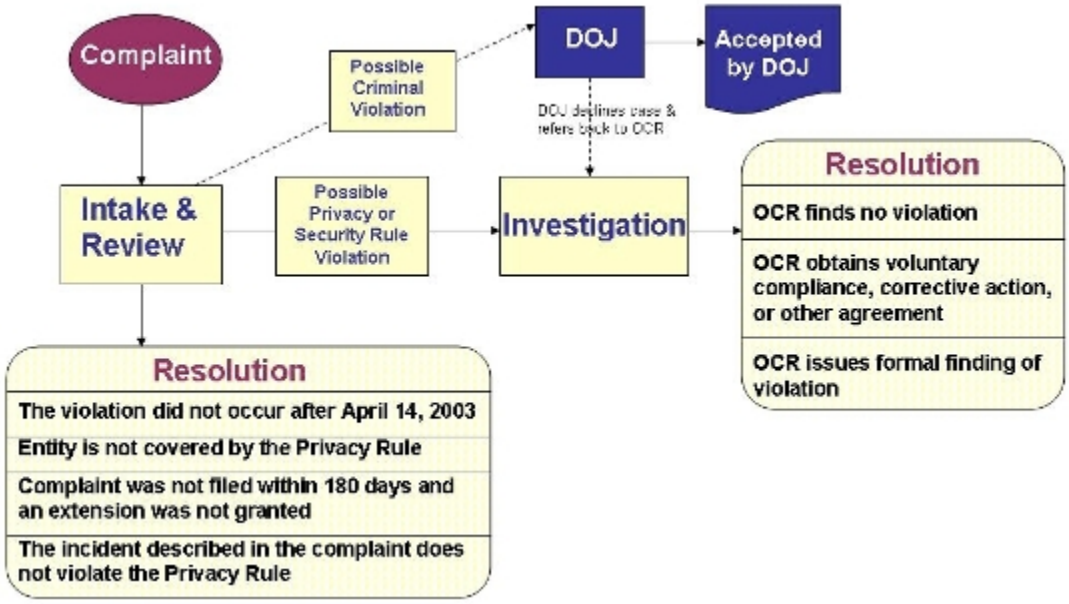


Figure 1. HIPPA Privacy and Security Complaint Process

To avoid this process, Geffert (2004) recommends that covered entities develop a security framework intended to address several parts of designing and implementing an information security plan. These include: (a) defining the requirements of the business, (b) analyzing the business impact of implementation, (c) putting a solution into place, and (d) monitoring compliance issues and keeping up with new industry requirements. Mercuri (2004) recommends a stepped implementation, whereby challenges that are encountered can be

mitigated and resolved before other new changes are made. This will keep the focus on compliance while allowing the flexibility for issues to be dealt with quickly.

Problems Faced by Healthcare Organizations with Implementation of Legislated Regulations

Organizations seeking compliance with HIPAA are required to address five categories of policy implementation. These are: (a) administrative safeguards, (b) physical safeguards, (c) technical safeguards, (d) organizational requirements, and (e) policies, procedures, and documentation requirements (Choi et al., 2006). Due to the complexity and number of issues that must be addressed, many covered entities have postponed the undertaking (Choi et al., 2006). Some of the reasons for this delay, beyond the number and complexity of tasks, include: (a) cost of needed resources, (b) prevalence of paper-based systems in health care and the reluctance to upgrade to a more efficient and controlled environment, (c) hesitation of implementing a new security system that will require extensive end-user training, and (d) lack of qualified staff to plan, design, and implement a system that would facilitate compliance (Lorence & Churchill, 2005). Choi et al., (2009) also indicate that just the sheer effort needed to successfully manage and complete a project of this scope and scale is a formidable deterrent.

Regardless of the reasoning for an organization's delay, implementation and successful compliance must be made a priority (Harman, 2005). The public's understanding about privacy is growing and with that comes a demand for increased security (Harman, 2005). Electronic health records will become a standard, says Harman (2005), and "someday HIPAA will be an integral part of clinical practice and will not be such a struggle" (p. 105).

References

Axelrod, C. W., Bayuk, J. L., & Schutzer, D. (Eds.). (2009). *Enterprise information security and privacy.* Norwood, Massachusetts: Artech House, Inc.

Beaver, K., & Herold, R. (2003). *The practical guide to HIPAA privacy & security compliance.* Boca Raton, Florida: Auerbach Publications.

Bell, C., & Smith, C. (2009). *Critical evaluation of information sources.* Retrieved from the University of Oregon Web site at http://libweb.uoregon.edu/guides/findarticles/credibility.html

Berghel, H. (2005). The two sides of ROI: Return on investment vs. risk of incarceration. *Communications of the ACM, 48*(4), 15-20. doi: 10.1145/1053291.1053305 Retrieved from http://delivery.acm.org/10.1145/1060000/1053305/p15-berghel.pdf?key1=1053305&key2=0254295031&coll=DL&dl=ACM&ip=150.135.241.143&CFID=22462419&CFTOKEN=40524661

Brotby, K. (2009). *Information security governance: A practical development and implementation approach.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Brown, C. (2005). HIPAA programs: Design and implementation. *Information Systems Security, 14*(1), 10-20. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=mth&AN=16195637&site=ehost-live&scope=site

Brusil, P. J., & Harley, D. (2002). Medical records security. In S. Bosworth & M. Kabay (Eds.). *Computer security handbook* (4th ed.)(pp. 49.1-49.32). New York, New York: John Wiley & Sons, Inc.

Centers for Medicare & Medicaid Services. (n.d.). *HIPAA administrative simplification compliance deadlines.* Retrieved from http://www.cms.gov/HIPAAGenInfo/Downloads/HIPAAComplianceDeadlines.pdf

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in heath care industry: Implementation of HIPAA and the security rules. *Journal of Medical Systems, 30*(1), 57-64. Retrieved from http://www.springerlink.com/content/035317748wrk775t/fulltext.pdf

Chute, C. G., Beck, S. A., Fisk, T. B., & Mohr, D. N. (2010). The enterprise data trust at Mayo Clinic: A semantically integrated warehouse of biomedical data. *Journal of the American Medical informatics Association, 17*(2), 131-135. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3000789/pdf/jamia002691.pdf

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, California: Sage Publications, Inc.

Cushman, R. (2008, February 18). The hope of HIPAA 2. *Modern Healthcare, 38*(7), 28. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=bth&AN=31320979&site=ehost-live&scope=site

Engle, M., Blumenthal, A., & Cosgrave, T. (2011). How to prepare an annotated bibliography. In Olin Reference, Research & Learning Services, *Cornell University library.* Retrieved from http://olinuris.library.cornell.edu/ref/research/skill28.htm

Gartner, Inc. (2011a). IT: Information Technology. *IT Definitions and Glossary.* Retrieved from http://www.gartner.com/technology/research/it-glossary

Gartner, Inc. (2011b). Information/data governance. *IT Definitions and Glossary*. Retrieved from http://www.gartner.com/technology/research/it-glossary

Geffert, B. T. (2004). Incorporating HIPAA security requirements into an enterprise security program. *Information Security Journal: A Global Perspective, 13*(5), 21-28. Retrieved from http://dx.doi.org/10.1201/1086/44797.13.5.20041101/84906.4

Glaser, J., & Aske, J. (2010). Healthcare IT trends raise bar for information security. *Journal of the Healthcare Financial Management Association, 64*(7), 40-44. Retrieved from http://ezproxy.library.arizona.edu/login?url=http://proquest.umi.com/pqdweb?did=2080606411&sid=1&Fmt=6&clientId=43922&RQT=309&VName=PQD

Harman, L. B. (2005). HIPAA: A few years later. *Online Journal of Issues in Nursing, 10*(2), 95-110. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=17356284&site=ehost-live&scope=site

Hayden, L. (2009). Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies. *Information Security Journal*, *18*(6), 297-305. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=mth&AN=49232884&site=ehost-live&scope=site

Hill, D. G. (2009). *Data protection: Governance, risk management, and compliance.* Boca Raton, Florida: CRC Press.

Hoffman, S., & Podgurski, A. (2006). In sickness, health, and cyberspace: Protecting the security of electronic private health information. *The Berkley Electronic Press*. Retrieved from http://law.bepress.com/expresso/eps/1522

Hoffman, S., & Podgurski, A. (2007). Securing the HIPAA security rule. *Journal of Internet Law, Spring 2007*. Retrieved from http://ssrn.com/abstract=953670

Huston, T. (2001). Security issues for implementation of e-medical records. *Communications of the ACM, 44*(9), 89-94. doi: 10.1145/383694.383712. Retrieved from http://delivery.acm.org/10.1145/390000/383712/p89-huston.pdf?key1=383712&key2=7813765031&coll=DL&dl=ACM&ip=150.135.129.173&CFID=21865939&CFTOKEN=31223648

Information Security Manager. (2008, September 1). *Informatics Review.* Retrieved from http://www.informatics-review.com/jobdesc/infsec.html

Knapp, K., Morris, R., Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508. Retrieved from http://www.sciencedirect.com.libproxy.uoregon.edu/science?_ob=MImg&_imagekey=B6V8G-4WSHK03-2-5&_cdi=5870&_user=2148430&_pii=S0167404809000765&_origin=&_coverDate=10%2F31%2F2009&_sk=999719992&view=c&wchp=dGLzVzb-zSkWb&md5=d076cd08ac006744577a81a4b1842f8e&ie=/sdarticle.pdf

Leo, R., (Ed.). (2005). *The HIPAA program Reference Handbook.* Boca Raton, Florida: Auerbach Publications.

Lorence, D. P., & Churchill, R. (2005). Incremental adoption of information security in health-care organizations: Implications for document management. *IEEE Transactions on Information Technology in BioMedicine, 9*(2), 169-173. doi: 10.1109/TITB.2005.847137. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1435414

McKay, D. R. (2010). *Computer and information systems manager: Career information.* Retrieved from http://careerplanning.about.com/od/occupations/p/comp_sys_mgr.htm

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM, 47*(7), 25-28. Retrieved from http://delivery.acm.org.ezproxy1.library.arizona.edu/10.1145/1010000/1005840/p25-mercuri.pdf?key1=1005840&key2=1461423031&coll=DL&dl=ACM&ip=150.135.239.97&CFID=17050031&CFTOKEN=23246176

Raggad, B. G. (2010). *Information security management: Concepts and practice*. Boca Raton, Florida: CRC Press.

Scholl, M., & National Institute of Standards and Technology (U.S.). (2008). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Suleiman, J., & Huston, T. (2009). Data privacy and security: HIPAA and small business compliance. *International Journal of Information Security and Privacy, 3*(2), 42-53. Retrieved from http://find.galegroup.com.ezproxy2.library.arizona.edu/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T002&prodId=AONE&docId=A204309630&source=gale&srcprod=AONE&userGroupName=uarizona_main&version=1.0

Sullivan, J. M. (2004). *HIPAA: A practical guide to the privacy and security of health data.* Chicago, Illinois: American Bar Association Publishing.

Tipton, H. F., & Krause, M., (Eds.). (2000a). *Information security management handbook* (4th ed., Vol. 1). Boca Raton, Florida: Auerbach Publications.

Tipton, H. F., & Krause, M., (Eds.). (2000b). *Information security management handbook* (4th ed., Vol. 3). Boca Raton, Florida: Auerbach Publications.

Tipton, H. F., & Krause, M., (Eds.). (2003). *Information security management handbook* (5th ed.). Boca Raton, Florida: Auerbach Publications.

U.S. Department of Health & Human Services. (n.d.) *Health information privacy enforcement process*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html

Wu, S., (Ed.). (2007). *A guide to HIPAA security and the law*. Chicago, Illinois: American Bar Association Publishing.

Wylder, J. (2004). *Strategic information security.* Boca Raton, Florida: Auerbach Publications.

Yee, G., (Ed.). (2006). *Privacy protection for e-services*. Hershey, Pennsylvania: Idea Group Publishing.