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

# Securing Electronic Data Exchanges for HIPAA Covered Entities to Ensure Greater Compliance with Security Rules

CAPSTONE REPORT

**Sandesh Kuckian**
**Business Systems Analyst**
**MedImpact Healthcare Systems, Inc.**

University of Oregon
Applied Information
Management
Program

**July 2011**

Academic Extension
1277 University of Oregon
Eugene, OR  97403-1277
(800) 824-2714

Approved by

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

# Securing Electronic Data Exchanges for HIPAA Covered Entities to Ensure Greater Compliance with Security Rules

Sandesh Kuckian

MedImpact Healthcare Systems, Inc.

## Abstract

HIPAA requires covered entities to follow standards for protecting the security of electronic protected health information (e-PHI). This study examines the need to develop a secure data exchange in order to maintain compliance with the goals of the HIPAA Security Rule. Literature published between 2000 and 2011 is analyzed to ensure the confidentiality, integrity, and availability of e-PHI while allowing entities to adopt new technologies to improve the quality, safety, and efficiency of patient care.

*Keywords:* electronic data exchange, HIPAA security rule, HIPAA security violation, security vulnerability, protecting e-PHI, HIPAA breach, penalties, and HIPAA implications.

## Table of Contents

## List of Figures

# Introduction to the Annotated Bibliography

## Problem and Significance

The U.S. Department of Health and Human Services states:

> The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. (HHS, 2011, "Introduction," para. 1)

Smith (2003) provides further definition on HIPAA Security Rule in the ISSA journal:

> If security is the *vehicle*, privacy is the *payload*. The whole point of HIPAA security is to provide a foundation so that *covered entities* (those organizations that come under the span of authority of the HIPAA statute) are in a position to guarantee the privacy rights of patients and health plan members. (para. 8)

Within this environment, healthcare industries have greater security concerns than other industries because they must provide electronic access of patient medical information to a number of entities in a safe and confidential manner in order to meet security mandates (General DataComm, 2004). System vulnerabilities may increase the risk of exposing protected information to unauthorized personnel or malicious insiders who could misuse patient health information for personal gains. Increased mobility of patient data and the extended enterprise introduce a host of related enterprise security challenges (Juniper Networks, 2010). Covered entities have become more vulnerable to security threats mainly due to enhanced mobility of patient data, unbounded networks as a result of connectivity with hundreds of similar health care stakeholders, transmission of electronic health data and sharing of sensitive information.

As mentioned on the HHS website (2011), information security is achieved by ensuring the confidentiality, integrity, and availability of information. Covered entities can thus face serious problems if their members' sensitive data is stolen, misused or unavailable. Such problems cannot only affect the covered entities business due to bad reputation or penalties, but can also directly affect vital care of their patients.

When referring to the complexity of the HIPAA rule structure, Hall, Hoffman and Sobel (2008) state:

> There once was a happy time when HIPAA referred to insurance reforms that increased access and tried to reduce costs. Owing to its gargantuan privacy rule, HIPAA is now known mainly as the source of constant headaches and endless strife over whether patients' medical records are adequately protected. (pp. 7-8)

Collmann et al. (2004) point out the range of security issues within covered entities in this statement:

> While healthcare organizations find implementing *good industry practice* difficult enough to accomplish, other issues such as the safe patching of security vulnerabilities in the software of biomedical devices, safely sharing information across enterprise boundaries, organizing information security programs in competition with other organizational missions, and managing risk in networked

> environments loom large and often unnoticed, especially for networks of hospitals seeking to manage information resources as an enterprise. (pp. 113-118)

External security threats in the form of theft or misuse of confidential information can directly impact the integrity of patient information by corrupting records during electronic data exchanges. Lentz (2000) shares her views on the importance of HIPAA by stating:

> HIPAA, the Health Insurance Portability and Accountability Act of 1996, and its accompanying regulations, make it a violation to share patient information with anyone not authorized to know or who has no need to know that information. And patient information isn't limited to name, health status or date of birth. HIPAA says any information that could identify a patient must be protected. (para. 7)

Thus the assumption underlying this study is that the HIPAA security rule can be viewed as not merely a legal compliance formality, but also as a way to help develop and maintain measures to appropriately safeguard sensitive patient information, thereby improving the overall quality of patient care.

## Purpose

According to Scholl et al. (2008), "HIPAA required the Secretary to adopt, among other standards, security standards for certain health information. These standards, known as the HIPAA Security Rule (the Security Rule), were published on February 20, 2003" (p. 1). The Centers of Medicare and Medicaid Services (CMS) state:

> On July 27, 2009, the Secretary of Health and Human Services (HHS) delegated to the Director of OCR the authority to administer and enforce the HIPAA Security Rule. This action by Secretary Sibelius was expected to improve HHS ability to protect individuals [*sic*] health information by combining the authority for

> administration and enforcement of the Federal standards for health information privacy and security called for in the HIPAA legislation. (CMS, 2010, "HHS Secretary Delegates HIPAA Security to OCR," para. 2)

Bernstein, a partner with Manatt Health Solutions, states “pressure to invest in health IT, account for improved outcomes of care, and overcome projected lower reimbursement through greater efficiency are shaping a market for Health Information Exchange which didn't exist for many years” (as cited in Morrissey, 2011, pp. 24-25). In partial response to this goal, this study is designed to help HIPAA covered entities to expand security considerations and increase awareness surrounding exchange of sensitive health data, as currently mandated by the Security Rule. Stevenson (2007) in his published article in Healthcare Information and Management Society (HIMSS) website states "information security is achieved by implementing policies and procedures as well as physical and technical measures that deliver confidentiality, integrity and availability (CIA)". For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles of information security (Wikipedia, 2011).

A major goal of the Security Rule is to protect the privacy of an individual’s health information while allowing covered entities to adopt newer technologies to improve the quality and efficiency of patient care (HHS, 2011). In response, the focus of this study is on the need to develop a secure data exchange as a way to maintain compliance with the goals of the HIPAA Security Rule. The specific purpose of this scholarly annotated bibliography is to identify and summarize literature that examines ways to ensure the confidentiality, integrity, and availability of electronic protected health information (e-PHI) during data transmission and the need to provide protection against reasonably anticipated threats and hazards to the security or integrity of e-PHI.

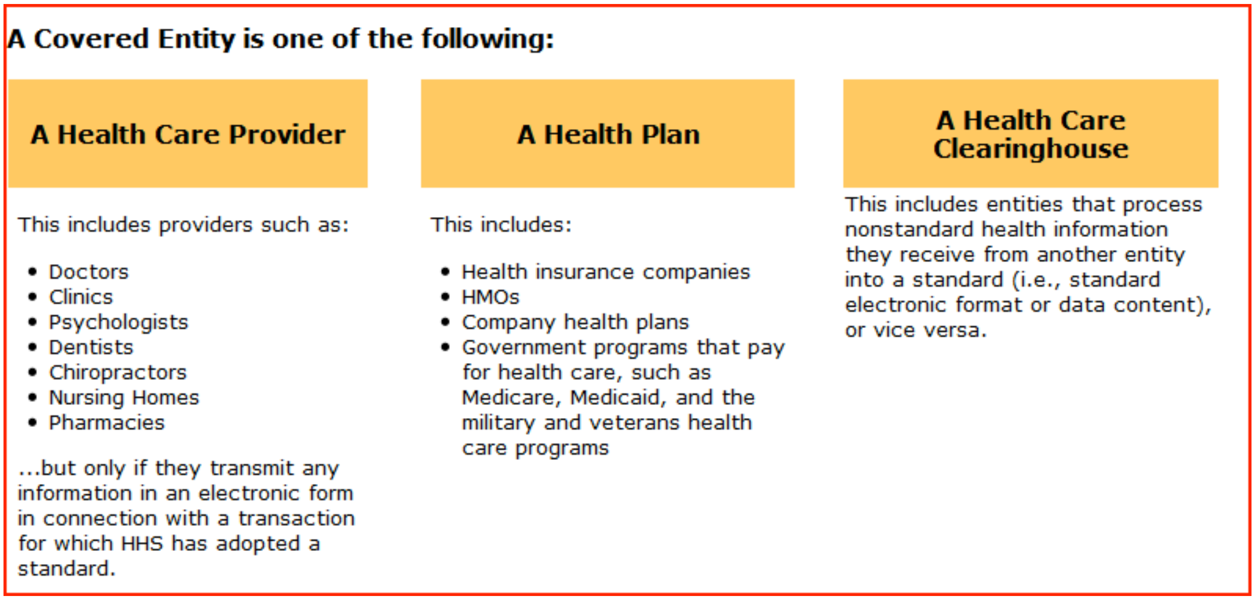
## Research Questions

Over the years, the industry trend among health care organizations has been on utilizing ever newer technologies, with the goal to be able to transmit and process electronic health data more effectively and securely. Today that trend includes the ability to comply with any Health Insurance Portability and Accountability Act (HIPAA) regulations.

The central research question in this study is "What changes can covered entities make to secure electronic data exchanges in order to ensure greater compliance with HIPAA Security Rule?" Four sub-questions guide this study: (a) how can HIPAA covered entities assess existing security frameworks in relation to the HIPAA security rule, (b) what are the potential risks and liabilities due to HIPAA violation during e-PHI data exchanges, (c) how can covered entities protect the confidentiality, integrity, and availability of e-PHI data exchanges, and (d) how can covered entities select appropriate emerging technologies purported to improve the security of e-PHI data exchanges.

## Audience

The annotated bibliography is primarily intended to serve the needs of two related groups: (a) HIPAA covered entities, and (b) a diverse audience of individuals who are responsible for HIPAA related security rule implementations, compliance efforts, management and oversight responsibilities related to the electronic exchange of PHI. This research assumes that the study will be most useful to individuals employed within a covered entity who have access to protected health information. HHS (2011) has provided a table defining the list of covered entities (see Figure 1).



**A Covered Entity is one of the following:**

**A Health Care Provider**

This includes providers such as:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

**A Health Plan**

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

**A Health Care Clearinghouse**

This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

*Figure 1.* Covered entities as shown in the U.S. Department of Health and Human Services website, HHS (2011).

This researcher is a business analyst at MedImpact, a company that manages pharmacy benefits. Knowledge of the current business environment and background of one particular company, MedImpact, may provide useful context for this annotated bibliography. MedImpact focuses on managing the drug benefit for its clients and their members. As a pharmacy benefit manager (PBM), MedImpact traditionally processes pharmacy claims and provides clinical support designed to manage the complexities of drug benefits. Because MedImpact stores and transmits sensitive patient information for business purposes, it is important for the organization to comply with both HIPAA privacy and security rules in order to improve the overall quality and efficiency of patient care. Currently serving more than thirty two million members nationwide, MedImpact is the PBM for eight of the top ten health maintenance organizations (HMOs) in the country, as rated by Consumer Reports in 2009 (MedImpact, 2011). MedImpact clients include corporations and employers, unions, managed care organizations, health plans, insurance carriers, and third-party administrators, as well as local, state and federal employee programs.

When an insured member requests a prescription at a pharmacy, the pharmacist validates the member's insurance with MedImpact's claim adjudication system in order to determine eligibility; this action also triggers over eight hundred clinical safety checks, such as potentially harmful medication interactions and restrictions. Once the prescription claim is approved, the pharmacist collects any required co-pay or coinsurance from the member. MedImpact then reimburses the pharmacy for the remainder of the drug cost and collects the total cost from the member's employer or health plan.

In order for all this to work seamlessly, MedImpact receives member insurance related information from the member's employer or health plan, which is then used to process and adjudicate pharmacy claims. In order to comply with federal laws, MedImpact must ensure that all inbound and outbound files containing sensitive member information (also known as protected health information, or PHI) are received and/or transmitted efficiently and securely.

## Research Delimitations

**Time frame.** The literature included for this study is published between 2000 and 2011. The final rule for the security standards was published on February 20, 2003 (Naughton-Travers, 2004, p. 53). As Litwak (2005) states, the deadline for compliance with the Security Rule is April 21, 2005 for covered entities and April 21, 2006 for small health plans. All covered entities, must adhere to security standards for securing the confidentiality, integrity and availability of electronic protected health information. According to Schoppmann and Sanders (2004), regulations will continue to undergo modifications; however they can still be managed without the need to undertake unrealistic, economically unfeasible, and wholly unnecessary changes to the practice of medicine. Security technologies have advanced considerably in such areas as cryptography, biometrics, intrusion detection, anti-viral protection, decoy environments, vulnerability scanning, and incident response (Denning, 2003, p. 13). New technologies and a rapidly changing landscape in computer platforms and World Wide Web thus provide ways to address security threats that loom over health care organizations.

**Selection criteria.** The references selected for this study provide background and guidance to covered entities for implementing security rules concerning e-PHI to ensure greater compliance with HIPAA. Selected literature is retrieved via Health Source: Nursing/Academic Edition, Business Source Complete, Business Source Premier and Academic Search Premier Databases, University of Oregon online libraries, as well as through professional publications and journals. Preference is given to literature that provides in-depth analysis related to the central research question or sub-questions (Leedy & Ormrod, 2005). References that provide general context for this study are also collected.

**Search scope.** Scholl et al. (2008) publish a chart that outlines various components under HIPAA regulations (see Figure 2).

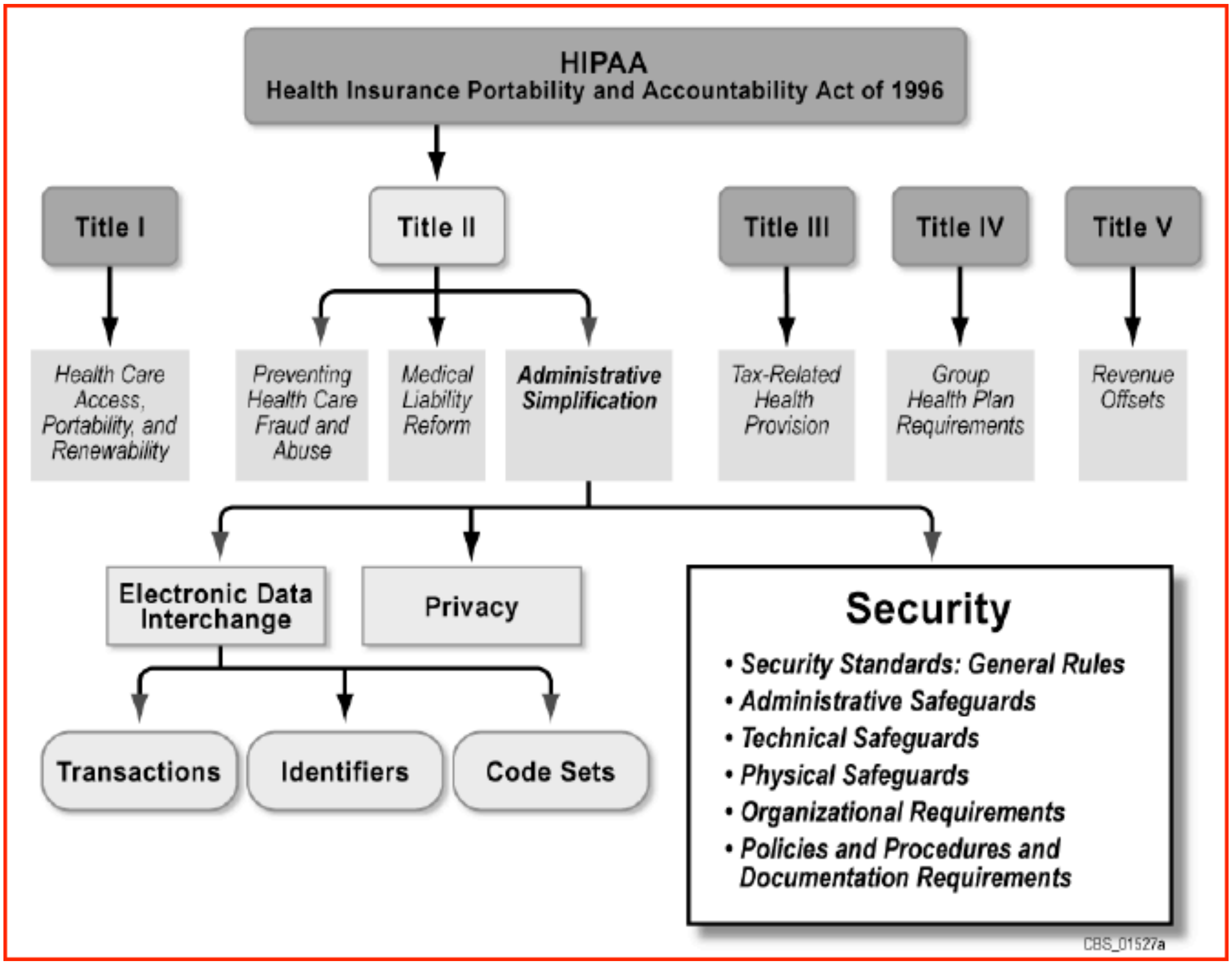

HIPAA
Health Insurance Portability and Accountability Act of 1996
Title I
Title II
Title III
Title IV
Title V
Health Care Access, Portability, and Renewability
Preventing Health Care Fraud and Abuse
Medical Liability Reform
Administrative Simplification
Tax-Related Health Provision
Group Health Plan Requirements
Revenue Offsets
Electronic Data Interchange
Privacy
Security
• Security Standards: General Rules
• Administrative Safeguards
• Technical Safeguards
• Physical Safeguards
• Organizational Requirements
• Policies and Procedures and Documentation Requirements
Transactions
Identifiers
Code Sets
CBS_01527a

*Figure 2.* HIPAA components by Scholl et al., 2008, p. 2.

The references included in this study are limited to providing guidance only around the security rule for covered entities. This study does not focus on the other areas under HIPAA as shown in Figure 2; however it must be noted that covered entities must address all areas outlined in the HIPAA regulations in order to be fully compliant with the HIPAA laws. Due to the close association between HIPAA privacy and security rules, references related to HIPAA privacy rules are subjected to secondary review for identifying any security related references.

**Intended audience.** This annotated bibliography is intended to serve a diverse audience of individuals with HIPAA security rule implementation, management, and oversight responsibilities and organizations, federal and nonfederal, considered to be a *Covered Entity* under 45 C.F.R. Sec.160.103 (Scholl et al., 2008, p. 4). If an entity is not a covered entity, it does not have to comply with the Privacy Rule or the Security Rule (HHS, 2011). Consequently, employers, marketers, websites dispensing medical advice or selling medical products and all other parties in possession of health information are exempt from the requirements of the HIPAA Privacy Rule in general and the HIPAA Security Rule in particular (Hoffman & Podgurski, 2007).

It must be noted that although some organizations may technically not fall under the HIPAA covered entity umbrella, they may still possess sensitive member health information. Such entities can be considered as the secondary audience for this literature. This study is not designed for individuals who want to optimize security standards within their organization with business goals other than complying with HIPAA security rule.

**Topic focus.** Although HIPAA encompasses a number of rules and regulations as shown in Figure 2, this study only focuses on meeting the goals of the HIPAA security rule in relation to the exchange of e-PHI. Covered entities need to electronically exchange a number of files that may contain protected member information for reasons such as enrollment, eligibility, payments, coordination of benefits and similar healthcare related transactions. Typically, security is addressed as it pertains to administrative, physical and technical safeguards (Choi et al., 2006, p. 60).

**Reading Plan Preview**

The plan for reading the selected literature is to scan for the presence of identified keywords relevant to the core concepts described in the purpose of the study, in a manner similar to a process known as conceptual analysis (Busch et al., 2005). According to Busch et al. (2005),

> Content analysis is a research tool used to verify the presence of certain words or concepts within texts or sets of texts. Researchers quantify and analyze the meanings, presence, and relationships of such concepts and words, then make inferences about the message within the texts, the audience, and the writers. (para. 1)

The abstract, introduction and conclusion in each reference are initially read for concepts that help to build the context for this study. The goal of this reading plan is to identify the presence of ideas that address the central research question / sub-questions or that provide recommendations or guidance to implement Security Rule for covered entities to ensure greater compliance with HIPAA. Busch et al. (2005) suggest eight steps for conducting conceptual analysis which are explained in detail in the Research Parameters section of this paper.

1. Decide the level of analysis.
2. Decide how many concepts will be coded.
3. Decide whether to code for existence or frequency of a concept.
4. Decide on how concepts will be distinguished from one another.
5. Develop rules for coding texts.
6. Decide what to do with irrelevant information.
7. Code the texts.
8. Analyze and report results.

## Organization Plan Preview

The organization plan describes how the selected literature is presented in the annotated bibliography. The flow of a piece of writing affects how readers interpret ideas and if the organization does not provide readers with the information they are looking for in an orderly manner, they will quickly lose interest (Reid, Barnes & Kowalski, 2011). This annotated bibliography is structured using the *thematic* pattern for organizing reference sources. Thematic reviews of literature are organized around a topic or issue, rather than the progression of time however; progression of time may still be an important factor in a thematic review (University of North Carolina, n.d.). Themes are directly related to the research questions established for this study. Theme one presents ideas on how HIPAA covered entities can assess their existing security frameworks in relation to the HIPAA security rule. Theme two identifies potential risks and liabilities due to HIPAA violation during e-PHI data exchanges. Theme three provides recommendations on how covered entities can protect the confidentiality, integrity, and availability of e-PHI data exchanges. Theme four focuses on appropriate emerging technologies purported to improve the security of electronic data exchanges.

## Definitions

According to Pickert (2009), the only thing more confusing than the health care reform debate is the vocabulary. Sternstein (2007) notes that according to the National Alliance for Health Information Technology and the Health and Human Services Department, a *cacophony* of competing and confusing definitions, with terms often used interchangeably, is hampering progress toward a nationwide health information network. A number of organizations may use the same terminology within their own internal business processes; however the context in which the terms are used may vary. Since acronyms and terms related to HIPAA privacy and security rules are used extensively in this annotated bibliography, the following list of definition is essential.

**Administrative safeguards.** These safeguards relate to administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information (Scholl et al., 2008, p. 7).

**Availability.** It is the property that data or information is accessible and usable upon demand by an authorized person (Scholl et al., 2008, p. 7).

**CIA.** Information security is achieved by implementing safeguards to provide confidentiality, integrity and availability (CIA) of health information and these three terms form the basis of the discipline of information technology security (Stevenson, 2007, p. 1).

**CMS.** The Centers for Medicare and Medicaid Services (CMS), previously known as the Health Care Financing Administration (HCFA), is a federal agency within the United States Department of Health and Human Services (DHHS) that administers the Medicare program and works in partnership with state governments to administer Medicaid, the State Children's Health Insurance Program (SCHIP), and health insurance portability standards (Wikipedia, 2011).

**Confidentiality.** It is the property that data or information is not made available or disclosed to unauthorized persons or processes (Scholl et al., 2008, p. 7).

**Covered entity.** A covered entity is either a health care provider or a health plan or a health care clearing house but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard (HHS, 2011).

**Electronic protected health information (electronic PHI, or e-PHI).** e-PHI stands for electronic protected health information. It is any protected health information (PHI) which is stored, accessed, transmitted or received electronically (Yale University, 2010).

**Health care clearinghouse.** This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa (HHS, 2011).

**HHS.** The Department of Health and Human Services (HHS) is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves (HHS, 2011).

**HIPAA.** It refers to the Health Insurance Portability and Accountability Act of 1996. The purpose of HIPAA is to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; and to improve access to long-term care services and coverage (North Carolina DHHS, 2011).

**HIPAA Security Rule.** The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information (HHS, 2011).

**Integrity.** It is the property that data or information have not been altered or destroyed in an unauthorized manner (Scholl et al., 2008, p. 7).

**OCR.** The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety (HHS, 2011).

**PHI.** PHI stands for protected health information. Individually identifiable health information becomes PHI when it can be used to identify an individual by itself or with another piece of information or from which there is a basis to believe the individual could be identified. Few examples include: name, Social Security number, address or date of birth (BlueCross BlueShield of Montana, 2011).

**Physical safeguards.** These safeguards related to physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion (Scholl et al., 2008, p. 7).

**Risk.** The net mission impact considering (1) the probability that a particular threat will exercise (accidentally triggers or intentionally exploits) a particular vulnerability; and (2) the resulting impact if this should occur (HHS, 2011, p. 4).

**Security.** This relates to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide availability, confidentiality and integrity (Scholl et al., 2008).

**Technical safeguards.** These safeguards related to the technology and policy and procedures for its use that protect electronic protected health information and control access to it (Scholl et al., 2008, p. 7).

**Threat.** It is the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability (HHS, 2011, p. 3).

**Virtual private network (VPN).** A virtual network built on top of existing networks that provides a secure communications mechanism for data and Internet Protocol information transmitted between networks (Frankel, Hoffman, Orebaugh & Park, 2011).

**Vulnerability.** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy (HHS, 2011, p. 3).

## Research Parameters

Research parameters provide details on the framework and approach employed for creating the scholarly annotated bibliography. This section begins with highlighting the key areas of literature that are aligned with the central research question and sub-questions. The section further outlines a detailed search report comprised of keywords, search engines and databases used to search and retrieve relevant literature. A complete list of evaluation criteria for selecting quality references is then presented followed by the documentation approach used in this study. The section ends with a detailed reading and organization plan. The reading plan describes how selected literature is read and the organization plan describes how the selected literature is organized for presentation in the Annotated Bibliography section of this document.

### Search Report

The selection of references to support this study focuses on four areas of literature. The first area includes literature on accessing existing security frameworks in relation to the security rule within a HIPAA covered entity. For example, as part of a Privacy and Security Toolkit to implement the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework), the Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) developed a guide intended to assist health agencies in reassessing their existing health information security practices as they consider adopting and implementing emerging health information technology  capabilities such as electronic health records and electronic health information exchange (HHS, 2010).

The second area includes literature which highlights risks and liabilities for HIPAA covered entities in relation to HIPAA regulations. For example, Pagliari, Detmer and Singleton

(2007) point out that patients of the US managed care organization Kaiser Permanente have access to HealthConnectOnline, which offers records of allergies, immunizations, future appointments, diagnoses, instructions from past visits, and laboratory results as well as allowing patients to book appointments, reorder prescriptions, and communicate with healthcare professionals by email. This one example is indicative of the enormous volume of sensitive data that is transmitted online with an obvious intent to increase accessibility. With massive amounts of critical personal health data being transmitted over the networks between covered entities, theft of sensitive information continue to escalate year by year and has thus highlighted the importance of information security and regulatory compliance in regard to limiting any operational risks, fraud, waste and abuse.

The third area includes literature that provides recommendations on protecting the confidentiality, integrity, and availability of e-PHI data exchanges. For example, Wilcox and Brown (2005) provide details on the provisions of the HIPAA security rule and offer guidelines for implementation of appropriate addressable specifications.

The fourth area includes literature that provides recommendations on selecting appropriate emerging technologies purported to improve the security of e-PHI data exchanges. For example, Hoffman and Podgurski (2007) propose recommendations on how to effectively follow the HIPAA Security Rule in order to meet the overall goals of HIPAA (p.3).

**Keywords.** Although this study primarily focuses on the security aspect under the HIPAA law, the privacy aspect is also considered during searches for obtaining relevant literature due to the close association between the HIPAA privacy and security rules. Initial searches on just *security* or *privacy* in OneSearch from UO Libraries produced close to a million results that mostly dealt with topics unrelated to HIPAA. According to Bazerman (2010), the secret to success in computer searches is to find the right descriptors and to combine them in an appropriate search strategy. The search strategy is narrowed to combine the keyword *HIPAA* with another related keyword such as *security* or *health data exchange* as a way to weed out unrelated search topics.

Subject searches are more complicated and are often more successful when done in combination with a keyword search (Connor, 2011). The initial search is done using UO online libraries in which the search results offer visibility to new combinations of related search terms and keywords. These keywords are then combined and searched again in an iterative manner, using OneSearch for narrowing down results pertaining to the topic. The following is a list of keywords:

- HIPAA Electronic Data Exchange
- HIPAA Security
- HIPAA Security Compliance Guidance
- HIPAA Security Requirements
- HIPAA Security Issue
- HIPAA Privacy Violation
- HIPAA Breach
- Managing Information Security in Healthcare
- Securing Electronic Health Records
- Protecting Electronic Personal Health Records
- HIPAA Security Vulnerabilities
- HIPAA Legal Implications
- HIPAA Penalties for Noncompliance

- Electronic Data Interchange (EDI) Healthcare Organizations
- Implementing HIPAA Security Rule

The selection of search terms is closely tied towards the needs of HIPAA covered entities for implementing Security Rule to ensure greater compliance with HIPAA. According to Creswell (2009), one approach is to locate an article that is close to your topic, and then look at the terms used to describe it, and use these terms in your search. The State Privacy Office of West Virginia (2011) states:

> Security and privacy are distinct, but go hand-in-hand such that the Privacy rule focuses on the right of an individual to control the use of his or her personal information and covers the confidentiality of PHI in all formats including electronic, paper and oral whereas the Security rule focuses on administrative, technical and physical safeguards specifically as they relate to electronic PHI. (State of West Virginia, para. 2)

**Search process.** The resources needed for this study are primarily retrieved from the UO online libraries which scan through a number of databases, journals, articles, books and magazines in order to produce context specific results. Resources are also accessed and collected from MedImpact's intranet site since the organization is a covered entity and by law; is required to comply with HIPAA privacy and security rules. Professional compliance officers at MedImpact are useful resources for getting relevant literature on HIPAA regulations. In addition to the UO online libraries, Google Scholar and CiteSeer$^x$ are also excellent resources in order to quickly find quality literature. The search engines used for obtaining references for this annotated bibliography are:

- OneSearch from UO online libraries

- UO WorldCat from UO online libraries
- Google Scholar Search
- CiteSeer$^x$

The databases used for obtaining references for this annotated bibliography are:

- Health Source: Nursing/Academic Edition
- Business Source Complete
- Business Source Premier
- Academic Search Premier
- SpringLink
- Jstor
- ScienceDirect

**Evaluation criteria.** The literature selected for use in this study are first retrieved by searching for topic specific keywords and then filtered by evaluating the topic based on quality and quantity of information, coverage of the topic and currency of work. Bell and Smith (2009) state:

> In evaluating the credibility of information source there are several key areas to consider: (a) the authority of the author and the publisher: Are they well qualified to speak to the topic at hand, (b) the objectivity of the author, (c) the quality of the work, (d) coverage of the work, and (e) currency: How recently were the research done and the work published? (para. 2)

According to Ormondroyd, Engle and Cosgrave (2009), bibliographic citations characteristically have three main components: author, title, and publication information which can help you determine the usefulness of this source for your paper. The following criteria have been used to evaluate references for this study:

- Relevancy of reference with respect to the search terms being used. This is determined by verifying if the terms used in the reference fall within the context of this study.
- Relevancy of reference in relation to the annotated bibliography. This is determined by verifying if the content addresses any part of the central question or sub-questions.
- Relevancy of databases. This is determined by reading the description and focus of the database.
- Credibility of author is checked by verifying author's professional background and education.
- Publication date of the resource. Publications older than January 1, 2000 are considered to be out-dated.
- Intended audience for whom the literature is written.
- The quantity of other relevant literature that have been cited in the resource.
- Quality of the resource. The quality is gauged by checking credible citations and / or bibliographies.

**Documentation approach.** Using the list of keywords identified for this study and the selected search engines / databases, a separate table is maintained in Excel that shows the total number of search results for each keyword under a specific search engine / database along with a quality rating. The search results, ratings and comments are reported in Appendix A. References found in the search results are first evaluated using the evaluation criteria stated in the above section. Literature in the form of documents, PDFs, web-pages, articles or journals that are determined to be viable for further research are then electronically saved using a tool called

Zotero. Zotero is an easy-to-use yet powerful research tool that helps gather, organize, and analyze sources (citations, full texts, web pages, images, and other objects), and shares the results of research in a variety of ways (Zotero, n.d.). It is a tool that resides in Firefox web browser as plug-in and stores reference information under four tabs: Info, Notes, Tags and Related. Under the Info tab, the tool extracts and saves key citation related information such as author, abstract, date, title and URL. Once this information is saved, the tool also has the ability to retrieve the literature offline without having the need to connect to the Internet. Under the Notes tab, any comments pertaining to the saved literature are documented. Keywords related to the saved literature are added under the Tags tab for quick future searches and retrieval. Under the Related tab, literature found from previous searches can be linked using the linking feature which helps to organize, categorize and associate multiple related references.

## Reading and Organization Plan

According to Busch et al. (2005), in order to conduct a content analysis on any text, the text is coded, or broken down, into manageable categories on a variety of levels--word, word sense, phrase, sentence, or theme--and then examined using conceptual analysis. Busch et al. (2005) further explain that content analysis is currently used in a dizzying array of fields, ranging from marketing and media studies, to literature and rhetoric, ethnography and cultural studies, gender and age issues, sociology and political science and many other fields of inquiry.

The resources gathered for this study are interpreted using conceptual analysis. A combination of keywords, themes, ideas and own experiences in health care industry are used to obtain relevant literature from UO libraries, articles, journals, government websites and databases for conceptual analysis. As introduced in the reading plan preview section, the following eight steps guide the coding process.

1. Decide the level of analysis – The analysis for this study is done by coding for both words and phrases. The concept of assessing existing security framework is determined by coding for words or phrases such as HIPAA security, HIPAA privacy, e-PHI and analyzing HIPAA security requirements. The concept of assessing risks and liabilities is determined by coding for words or phrases such as HIPAA security issues, HIPPA violations, HIPAA failures, HIPA breaches and HIPAA legal implications. The concept of security improvements for e-PHI data exchanges is determined by coding for words or phrases such as implementing HIPAA security rule, protecting e-PHI, HIPAA security rule compliance, and managing security in healthcare.

2. Decide how many concepts will be coded – There are three concepts coded in this study. They are the concept of assessing existing security for HIPAA compliance, understanding risks/liabilities due to non-compliance of HIPAA Security Rule and security improvements for e-PHI data exchanges. These concepts and categories may evolve and thereby may be modified as they emerge during the conceptual analysis process.

3. Decide whether to code for existence or frequency of a concept – The concept is coded for existence rather than frequency. As long as any one of the three concepts exist in the identified resource, it is considered to be sufficient for further analysis.

4. Decide on how concepts will be distinguished from one another – As long as the words or phrases identified in step 1 appear to be related to HIPAA Security Rule, they are all recorded for further analysis.

5. Develop rules for coding texts - Translation rules give coding process a crucial level of consistency and coherence (Busch et al., 2005). The table below shows the translation rules applied in this study (see Figure 3):

| **HIPAA** | **Risks** | **Security Improvements** |
|---|---|---|
| Security | HIPPA breach | Implementing Security Rule |
| Privacy | Security Issue | Protecting e-PHI |
| e-PHI | Violation | Managing Security |
| Privacy Rule | Security Failure | Security Compliance |
| Security Rule | Legal Implication | HIPAA Security Guidance |

*Figure* 3. Translation rules for coding texts.

6. Decide what to do with irrelevant information – The topics not related to this study are excluded from further analysis.

7. Code the texts - When coding is done manually, a researcher can recognize errors far more easily as opposed to a computer program which can only code based on given information and thus poses problems when coding for any implicit information (Busch et al., 2005). For this study, the concepts are coded manually using words and phrases which are then saved in to Zotero for all identified and evaluated resources. Any other information including concepts, appropriate tags and relationships with other resources are added using the tool's in-built features.

**8.** Analyze and report results – The resources are examined together for all possible conclusions and inferences which are organized and presented in the scholarly annotated bibliography section of this document.

The annotated bibliography is structured using the *thematic* pattern for organizing reference sources. In a thematic review, sources are grouped and discussed in terms of the themes they cover as it helps in demonstrating the types of topics that are important to the research (Saint Mary's University, 2009). The plan is to organize the selected literature into four thematic categories that align with this study’s central research question and its sub-questions. An outline of the four categories along with potential sub-themes is shown below:

Category one presents ideas on how HIPAA covered entities can assess their existing security frameworks in relation to the HIPAA security rule. Sub-themes include:

- Assessing confidentiality, integrity and accessibility of sensitive health data.
- Assessing existing administrative, physical and technical safeguards.
- Assessing organization’s policy, procedures and documentation requirements.

Category two identifies potential risks and liabilities due to HIPAA violation during e-PHI data exchanges. Sub-themes include:

- Potential risks during health data exchanges.
- Vulnerabilities within covered entities during health data exchanges.
- Threats that may exploit vulnerability within covered entities during health data exchanges.

Category three provides recommendations on how covered entities can protect the confidentiality, integrity, and availability of e-PHI data exchanges. Sub-themes include:

- Standard guidelines of HIPAA security rule.
- Required and addressable specifications.
- Training needs for covered entities.

Category four focuses on appropriate emerging technologies purported to improve the security of electronic data exchanges. Sub-themes include:

- Types of secure transmissions.
- HHS recommended technologies.

## Scholarly Annotated Bibliography

An annotated bibliography is an organized list of references (may be any variety of materials, books, documents, videos, articles, web sites, etc.) with an accompanying paragraph that describes, explains, and/or evaluates each entry in terms of quality, authority, and relevance (Skidmore College, n.d.). References presented in this bibliography are organized within the following categories in order to address the central research question: *What changes can covered entities make to secure electronic data exchanges in order to ensure greater compliance with HIPAA Security Rule?*

Category #1*:* How to assess existing security framework in relation to the security rule within a HIPAA covered entity.

Category #2*:* Potential risks/liabilities due to HIPAA violation during electronic data exchanges.

Category #3*:* How covered entities can protect the confidentiality, integrity, and availability of e-PHI data exchanges.

Category #4*:* Selection of appropriate emerging technologies purported to improve the security of electronic data exchanges.

Each annotation consists of three elements: (a) an excerpt from the published abstract; (b) an assessment of the credibility of the reference; and (c) a summary of ideas most relevant to this study. The ideas presented in the summary are paraphrased or quoted from selected references and are not claimed to be this researcher's views.

### How to Assess Existing Security Framework in Relation to the Security Rule within a HIPAA Covered Entity

**Gallagher, A.L., & Barrett, W.C. (2004).** An assessment of HIPAA security preparedness. *Medical Benefits, 21*(11), 8-9. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=13461666&site=ehost-live&scope=site

**Abstract.** Over a period of 18 months, URAC staff consulted with hundreds of organizations; only a small percentage had implemented a comprehensive security management program to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The barriers that hamper the ability of organizations to address the HIPAA Security Rule are listed.

**Summary.** This article focuses on the assessment of existing security practices within covered entities and highlights barriers to full compliance with HIPAA security rules. The authors outline four key barriers: (a) incomplete or inappropriately scoped risk analysis efforts, (b) inconsistent and poorly executed risk management strategies, (c) limited or faulty information system activity reviews, and (d) ineffective security incident reporting and responses. Identifying and assessing these risks are important to protect electronic health information against reasonably anticipated threats or hazards as organizations adopt and implement electronic health records and participate in electronic health information exchange. Risk analysis and risk management serve as tools to develop and maintain a strategy to protect the confidentiality, integrity, and availability of e-PHI. These four barriers must be fully addressed by covered entities to maximize efficiency, protect from liability exposures and realize cost savings.

**Credibility.** Lisa Gallagher is Senior Director of Privacy and Security for the HIMSS; the largest U.S. cause-based, not-for-profit healthcare association focused on the optimal use of information technology and management systems. Claire W. Barrett is an accreditation reviewer at URAC, which is an independent, nonprofit organization that promotes health care quality through accreditation, education and measurement programs.

**HHS. (2010).** *Reassessing your security practices in a health IT environment*. Retrieved April 5, 2011, from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848086_0_0_18/SmallPracticeSecurityGuide-1.pdf

**Abstract.** Health information security is an iterative process driven by enhancements in technology as well as changes to the health care environment. Identifying risks and protecting electronic health information can be challenging for small health care practices. This guide is designed to help practitioners assess risks and develop appropriate security policies to protect electronic health information.

**Summary.** This document provides guidance in reassessing existing health information security policies as organizations consider embracing and implementing emerging health information technology capabilities such as electronic health records (EHR) and electronic health information exchange. Information security is defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of protected data. Examples are provided to assess EHR risks followed by identification of administrative, physical and technical safeguards for addressing these risks. Covered entities may consider the following administrative safeguards (a) continual risk assessment of health IT environment, (b) continual assessment of the effectiveness of safeguards for electronic health information, (c) detailed processes for viewing and administering electronic health information, (d) employee training on the use of health IT to appropriately protect electronic health information, and (e) appropriately reporting security breaches (e.g., to those entities required by law or contract) and ensuring continued health IT operations. Physical safeguards may include (a) office alarm systems, (b) locked offices containing computing equipment that store electronic health information, and (c) security guards. An example of a technical safeguard is securely configured computing equipment (e.g., virus checking, firewalls).

**Credibility.** The Department of Health and Human Services (HHS) is principal agency for protecting the health of all Americans. The Office of the National Coordinator for Health Information Technology (ONC) is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and is organizationally located within the Office of the Secretary for HHS. ONC and the Office for Civil Rights (OCR) developed this document as part of the privacy and security toolkit to implement the nationwide privacy and security framework for electronic exchange of individually identifiable health information.

**Naughton-Travers, P.J. (2004).** Here comes the latest HIPAA deadline. *Behavioral Health Management, 24*(6), 53-58. Retrieved from Health Source: Nursing/Academic Edition database:http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=15524152&site=ehost-live

**Abstract.** This article presents information on the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Topics include (a) key changes from the original proposed Security Rule; (b) description of the general requirements for organizations under the HIPAA security standards; and (c) groups that categorize implementation specifications.

**Summary.** This article examines changes introduced in the final rule of security standards to which covered entities needed to comply by April 21, 2005. The key changes noted are that the security standards are scalable and technology neutral. They more closely follow the privacy standards, using the same terms and definitions. The new standards define protected health information (PHI) as individually identifiable health information that is transmitted in an electronic media, maintained in an electronic media, or transmitted or maintained in any other form or media. Based on this definition of PHI, covered entities can identify the scope of elements to be considered for compliance within the HIPAA security rule. The article describes specifications that are *required* and *addressable* as per the HIPAA security standards. Required specifications must be implemented by all entities covered under HIPAA laws. Addressable specifications must be addressed by covered entities by assessing whether each specification is a reasonable and appropriate safeguard for the organization. If the organization deems the specification to be not reasonable and appropriate, it must document why and implement an equivalent alternative measure.

**Credibility.** This article is published in the Behavioral Health Management journal, which is a private company based in Cleveland, OH categorized under News Publications-Trade/Association Manufacturers. This publication appears in Health Source: Nursing/Academic Edition database from UO libraries that provides nearly 550 scholarly full text journals, including nearly 450 peer-reviewed journals focusing on many medical disciplines. Joseph Naughton-Travers was the Vice-President at Open Minds, an organization that provides payers and providers in the health and human service industry with management solutions designed to improve operational and strategic performance.

**Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, D. & Steinberg, D. (2008).** *An introductory resource guide for implementing health insurance portability and accountability act (HIPAA) security rule*. Retrieved March 31, 2011, from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

**Abstract.** This Special Publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. It was written to help to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication does not supplement, replace, or supersede the HIPAA Security Rule itself.

**Summary.** This publication is intended to serve a diverse audience of individuals with HIPAA Security Rule implementation, management, and oversight responsibilities and organizations, federal and nonfederal, considered to be a *Covered Entity* under 45 C.F.R. Sec.160.103. It provides guidance to support the compliance efforts of covered entities in many ways, including: (a) ensuring that each organization is selecting methods and controls which adequately and appropriately protect e-PHI of which they are the steward, (b) informing the development of compliance strategies that are in concert with the size and structure of the entity, (c) providing guidelines on best practices for developing and implementing a risk management program, and (d) creating appropriate documentation that demonstrates effective compliance with the HIPAA Security Rule. The document highlights the three rules that covered entities must follow in order to comply with the HIPAA security rule. They are (a) ensure the confidentiality, integrity, and availability of e-PHI that it creates, receives, maintains, or transmits, (b) protect against any reasonably anticipated threats and hazards to the security or integrity of e-PHI, and (c) protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy

Rule.

**Credibility.** The document is published by the Computer Security division at NIST. The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. This document has been authorized by both U.S. Department of Commerce and National Institute of Standards and Technology.

**Wilcox, S., & Brown, B. (2004).** Risk assessment, risk management, and the HIPAA security rule: A matter of life and death? *Journal of Health Care Compliance, 6*(4), 43-45. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14951524&site=ehost-live&scope=site

**Abstract.** Focuses on issues related to the implementation of the Health Insurance Portability and Accountability Act (HIPAA) security rule in assessing and managing risks of handling medical records. Includes (a) an overview of section 164.306 of the HIPAA security rule; (b) implementation specifications of the rule; and (c) recommendations for providers who are using electronic systems to collect and process critical health care data.

**Summary.** The authors define the purpose of the Health Insurance Portability and Accountability Act (HIPAA) rule is to improve the efficiency and effectiveness of the health care system. This goal can be achieved by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information. Two implementation specifications of the security rule are presented: (a) risk analysis – to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity, and (b) risk management – to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The authors recommend performing a comprehensive risk assessment requiring systematic identification and classification of critical assets, critical processes, and existing threats and vulnerabilities and also developing a comprehensive risk management plan.

**Credibility.** This article is published in the Journal of Health Care Compliance, which provides articles written by health care professionals and industry experts on how to avoid government inquiries and stay in compliance with health care laws and regulations. Spence Wilcox and Bob Brown are nationally known HIPAA experts with HealthCare Information Solutions in Kalamazoo, Michigan; a private company that provides services in corporate information technology and governance, particularly in Sarbanes Oxley and HIPAA. They are also HIPAA consultants and the developers of the HIPAA compliance software, HIPAASays.

**Potential Risks/Liabilities Due to HIPAA Violation During Electronic Data Exchanges**

**American Medical Association. (n.d.).** *HIPAA violations and enforcement*. Retrieved April 30, 2011, from http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.shtml

**Abstract.** The American Medical Association website provides tools to assist physicians to understand and comply with the different components of HIPAA. This article provides details on the implications due to non-compliance with HIPAA which can result in civil and criminal penalties (42 USC § 1320d-5).

**Summary.** This article focuses on the civil and criminal penalties that could be enforced on covered entities due to non compliance of HIPAA regulations. The Office of Civil Rights (OCR) enforces the privacy standards, while the Centers for Medicare and Medicaid (CMS) enforces both the transaction and code set standards and the security standards (65 FR 18895). This article details a tiered civil penalty structure for HIPAA violations and highlights criminal penalties for covered entities and in certain specific situations for individuals, in accordance with principles of corporate criminal liability. A tiered civil penalty structure for HIPAA violations is provided as established by the "American Recovery and Reinvestment Act of 2009" (ARRA) that was signed into law on February 17, 2009. If covered entities and specified individuals knowingly obtain or disclose individually identifiable health information then they can be held criminally liable under HIPAA. Depending on the nature of the crime, fines may range from $50,000 to $250,000 and could also include imprisonment for up to ten years.

**Credibility.** This article appears in the American Medical Association (AMA) website which provides physicians, residents, medical students and group practices access to invaluable resources ranging from medical ethics and exploration of legal issues to practice management. AMA was founded in 1847 and currently has about 250,000 members. It is America's largest and most powerful physician organization and purportedly has more influence than any other group in the health care industry.

**Boerner, M.C. (2010).** View HIPAA breaches affecting 500 or more individuals online. *Journal of Health Care Compliance*, *12*(3), 31-68. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=50320776&site=ehost-live&scope=site

**Abstract.** The article provides an overview of the impact of Health Insurance Portability and Accountability Act (HIPAA) breaches on individuals in the U.S. When a HIPAA breach involves 500 or more persons, covered entities should notify them using the Department of Health and Human Services (HHS) Web site.

**Summary.** This article focuses on HIPAA breaches on individuals. The author provides examples on how HIPAA breaches could occur due to insufficient safeguards that may exist within a HIPAA covered entity. The HHS website provides several case examples of HIPAA violations which are categorized into ten types of issues including: access, authorizations, business associates, conditioning compliance with the privacy rule, confidential communications, disclosures to avert a serious threat to health or safety, impermissible uses and disclosures, minimum necessary information, notice and safeguards. These case examples provide a clear picture of how covered entities may knowingly or unknowingly violate HIPAA laws. Depending on the nature of the violation, Office for Civil Rights can provide corrective actions that organization must undertake. The article also outlines next step procedures upon discovery of a HIPAA breach, articulated through a resolution agreement signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years. When HHS is not able to reach a satisfactory resolution through the covered entity’s demonstrated compliance or corrective action through other informal means, civil money penalties (CMPs) may be imposed for noncompliance.

**Credibility.** The article is published in the Journal of Health Care Compliance, which is a peer-reviewed publication that provides articles written by health care professionals and industry experts on how to avoid government inquiries and stay in compliance with health care laws and regulations. Catherine Boerner is president of Boerner Consulting (BC), LLC. Boerner's expertise is in Health Insurance Portability and Accountability Act and her responsibilities include maintaining audits, assisting corporate compliance and security officers. BC provides hospitals cost-effective compliance program effectiveness assessments.

**Conn, J. (2009).** New sheriff in town. *Modern Healthcare*, *39*(33), 13. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=43864577&site=ehost-live

**Abstract.** The article reports on the move by the U.S. Department of Health and Human Services (HHS) to consolidate authority for both security and privacy rule enforcement under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with the Office for Civil Rights at HHS. According to some industry observers, this action could result in a stricter enforcement of both federal rules.

**Summary.** This article highlights the government's role in dictating the significance of both HIPAA privacy and security rule violations and depicts examples of HIPAA covered entities taken to task for violating rules. HHS Secretary Kathleen Sebelius shifted the duties of security rule enforcement from the CMS by consolidating authority for both security and privacy rule enforcement with the Office for Civil Rights. The consolidation is a signal that the federal government is stepping up enforcement in these areas, and is spurred in part by the tighter privacy and security provisions mandated by Congress in the healthcare information technology sections of the American Recovery and Reinvestment Act of 2009. For example, the CMS and civil rights office reached a settlement agreement with Providence Health and Services, Seattle, capping a 2008 investigation of a medical records breach that included a $100,000 resolution amount. In another example, pharmacy chain CVS Caremark agreed to pay HHS $2.25 million to settle a joint enforcement action taken by HHS and the Federal Trade Commission after television news reports were aired about patient identifiable prescription information being tossed into trash bins behind several CVS drugstores scattered across the country. Susan

McAndrew, deputy director for health information privacy at the Office for Civil Rights, however points out that from an administrative standpoint a negotiated settlement is quicker and potentially more effective than taking the longer procedural route required for imposing a civil monetary penalty.

**Credibility.** The article is published in Modern Healthcare journal, which is the industry's leading source of healthcare business and policy news, research and information. Joseph Conn is a Modern Healthcare reporter, who covers healthcare information technology, privacy and security issues. Conn has a BA in English and his background includes twenty four years of reporting and editing with various news publications, teaching journalism at Valparaiso (Ind.) University and working as a Peace Corps volunteer in Sierra Leone.

**Lentz, R. (2000).** Privacy matters. *Modern Physician*, *4*(5), 39. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=3177643&site=ehost-live

**Abstract.** This article deals with patient privacy regulations under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the United States. Topics include patient information; amount of fines per violation of the regulations; why Congress outlined privacy and security rules for the transmission of health care information; and features of the HIPAA privacy regulations. Provides a snapshot of recommended implementation steps, timetable and the audience to which HIPAA rules apply.

**Summary.** This article focuses on the importance of following HIPAA security rules and the amount of fines a covered entity may risk paying due to a violation. Fines can reach up to $25,000 per violation and those who knowingly break the law can spend up to 10 years in prison for each error. One case example is Rick Skinner, the CIO of Providence Health Systems based in Tigard, Oregon who brought in consultants to look at his organization's technical security measures and its security and confidentiality policies and then compared them with what HIPAA was expected to require. Skinner found most of the identified security issues had to do with how the group managed information technology rather than exposure to external security threats. Another example describes efforts by the covered entity Palo Alto Medical Foundation, a 200-physician organization, which has been working to improve patient privacy and confidentiality protection by launching an extensive education program.

**Credibility.** This article is published in Modern Physician magazine, which is the *go-to* business publication for physician executives, leaders and entrepreneurs and reaches more than 24,000 healthcare professionals. This publication appears in Health Source: Nursing/Academic Edition database from UO libraries that provides nearly 550 scholarly full text journals, including nearly 450 peer-reviewed journals focusing on many medical disciplines. Rebecca Lentz was then a reporter for Modern Physician magazine in Chicago, Illinois, Wilmington Morning Star magazine in Wilmington, North Carolina, and Bismarck Tribune magazine in Bismarck, North Dakota. She received the 2001 Jesse H. Neal Award for her articles on HIPAA and an award in 1997 from the Pew Charitable Trusts for health care reporting.

**Sloane, T. (2003).** A HIPAA has its day. *Modern Healthcare*, *33*(15), 21. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=9608291&site=ehost-live

**Abstract.** Topics include: (a) the implementation of the privacy regulations for medical records of the Health Insurance Portability and Accountability Act of 1996 in the U.S. Concerns about the implementation of the regulations; (b) civil and criminal penalties for the violation of the regulations; and (c) estimated cost of conforming with the regulations.

**Summary.** This article provides information on implications and penalties for covered entities due to a HIPAA privacy violation. Includes examples of patient experiences such as standing at a pharmacy counter and being asked out loud which drug he or she is taking, or having a personnel manager in an office lobby ask how a medical problem is going. Civil and criminal penalties range from $50,000 to $250,000 in fines and one to 10 years in prison may be levied by HHS civil rights division and the U.S. Justice Department if patient information is used for commercial advantage, personal gain or malicious harm. Other aspects include requirements for computerized insurance transactions, security regulations governing access to electronic medical records and the appointment of security officers at every medical practice.

**Credibility.** This article is published in Modern Healthcare journal, a national business magazine read by 72,000 executives and clinical leaders of hospitals, health systems, medical groups and insurers, as well as officials of associations and health policy organizations. Todd Sloane is assistant managing editor. He has been a lecturer in government journalism at Columbia College in Chicago and has also has been a free-lance writer, published in many daily newspapers and journals on a range of topics.

**Pagliari, C., Detmer, D., & Singleton, P. (2007).** *Potential of electronic personal health records*. Retrieved from Jstor database: http://www.jstor.org/stable/25690019

**Abstract.** This article presents the authors' reaction to new systems for helping patients to access and manage their personal electronic health data in the United Kingdom and internationally. Arguments suggest that many patients have concerns about security and confidentiality and that patient and doctors should be involved in the design, development implementation and evaluation of any electronic health data system.

**Summary.** This article focuses on the benefits and risks of having access to electronic personal health records. Topics include a number of benefits of using electronic health records such as the potential to empower patients through greater access to personal data, health information and communication tools which may aid self care, shared decision making and clinical outcomes. Electronic personal data may also reduce geographical barriers to patient care and act as a point of record integration, particularly in fragmented health systems thus improving continuity of care and efficiency. The emergence of mobile and wireless applications that allow remote submission of data to a shared record offer new possibilities for patient monitoring and real time decision support. Electronic records may help to promote partnership between care-givers and health professionals through sharing information, or allow relatives to monitor the care and progress of elderly parents or children in hospital from a distance. The author considers privacy and security while allowing patients to manage their health data and acknowledges the challenge of balancing security against utility and integrating diverse data sources and systems. Although encryption technologies can help to prevent unauthorized access, the risk of privacy invasions may be greatest at the family level, whether the intent is to support or malign. EHR may improve the quality, safety, and efficiency of care however key challenges include balancing security against utility and integrating diverse data sources and systems.

**Credibility.** This article is published in British Medical Journal. Claudia Pagliari is a senior lecturer in primary care, Division of Community Health Sciences, University of Edinburgh. Don Detmer is professor of medical education, Public Health Sciences, University of Virginia and Peter Singleton is principal research fellow at Centre of Health Informatics and Multi-professional Education, University College of London.

**Withrow, C.S. (2010).** How to avoid a HIPAA horror story. *Healthcare Financial Management, 64*(8), 82-88. Retrieved from Business Source Complete database: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=52842270&site=ehost-live&scope=site

**Abstract.** The article offers information on the expansion of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and its financial risks for hospitals in order to meet the privacy and security requirements under HIPAA. HIPAA related penalties can be prevented by following appropriate compliance procedures.

**Summary.** This article focuses on the financial risk of HIPAA violations and notes that the HITECH Act of 2009 extends the security provisions and penalties beyond covered entities (such as hospitals and physicians) to include all business associates (such as electronic medical record vendors and IT services). HIPAA makes distinctions regarding security and privacy rules in order to encourage the realization of administrative efficiencies through healthcare information technologies. According to enforcement statistics of CMS, the two most commonly violated security provisions are information access management and access control. Information access management includes specifications for granting access to electronically protected information through access to a workstation, transaction, program, or process. Access control encompasses specifications for unique user identification, automatic logoff, and encryption of electronic protected information, both in motion and at rest. A summarized outline of civil and criminal monetary penalties for HIPAA violations shows that financial risks have significantly increased. Covered entities such as hospitals, physicians and their business associates must continue to focus on their compliance efforts on high-risk areas, including information access management, access control, and impermissible disclosures of protected health information to ensure privacy and security provisions are appropriately adopted. The author concludes that a HIPAA horror story within covered entities can be avoided by following sound compliance methods that can mitigate culpability and reduce any potential civil or criminal monetary penalties.

**Credibility.** This article is published in Healthcare Financial Management journal, which is a leading membership based publication for healthcare financial management and executives. Scott Withrow has practiced corporate and healthcare law for 24 years and his practice includes mergers and acquisitions, public and private securities offerings, public securities and Sarbanes-Oxley compliance, franchises, taxation, corporate finance, partnerships, limited liability companies, and joint ventures.

**Ways To Protect the Confidentiality, Integrity, and Availability of E-PHI Data Exchanges**

**de Wolf, A.V., Sieber, E.J., Steel, M.P., & Zarate, A.O. (2006).** Part II: HIPAA and disclosure risk issues. *IRB: Ethics & Human Research, 28*(1), 6-11. Retrieved from Psychology and Behavioral Sciences Collection database: http://search.ebscohost.com/login.aspx?direct=true&db=pbh&AN=19384905&site=ehost-live

**Abstract.** This article discusses how data is prepared for sharing by the Institutional Review Boards (IRBs). This article is the second in a series of three articles to assist IRBs in providing guidance to investigators and research administrators who need to comply with data sharing requirements.

**Summary.** This article provides guidance to investigators and research administrators on preparing data for sharing especially when made available for public use. Although this article does not provide information on secure data exchanges, it provides valuable insight on filtering protected data if such information is to be released to certain non-covered entities for research purposes. For example, the Inter-university Consortium for Political and Social Research (ICPSR) provides extensive instructions for persons who plan to deposit data in its repository. Instructions include details on how to plan for sharing at the research stage, how to ensure confidentiality, and how to document the data. Data documentation consists of describing the data so that users can understand and use the data correctly. The purpose of documentation is to make data as user-friendly as possible for the secondary user while minimizing the risk of disclosure of identifying data. De-identification is an important step towards rendering the data anonymously. Once identifiers have been removed, the remaining data must be checked for possible risk of re-identification through matching with other records that contain identifiers.

This is why the mere removal of names and addresses may be insufficient to de-identify data and would, therefore, preclude data sharing under HIPAA and the National Institutes of Health (NIH) confidentiality provisions.

**Credibility.** This article is published in IRB: Ethics and Human Research journal and is written by Virginia A. de Wolf, Joan E.Sieber, Philip M. Steel and Alvan O. Zarate. Virginia A. de Wolf, PhD, is a United States Federal Statistician (retired); Joan E. Sieber, PhD, is Professor of Psychology, Emerita, at California State University East Bay, Hayward, CA; Philip M. Steel, MS, is Disclosure Avoidance Staff Member at the United States Census Bureau, Washington, DC; and Alvan O. Zarate, PhD, is Confidentiality Officer at the National Center for Health Statistics, Hyattsville, MD.

**HHS. (2010).** *The HIPAA privacy rule and health IT*. Retrieved March 29, 2011, from http://healthit.hhs.gov/portal/server.pt?open=512&objID=1174&parentname=CommunityPage&parentid=26&mode=2&in_hi_userid=10732&cached=true

**Abstract.** The Office for Civil Rights (OCR) has published new Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rule guidance documents as part of a privacy and security toolkit to implement the nationwide privacy and security framework for electronic exchange of individually identifiable health information.

**Summary.** This website offers a security information series of educational papers designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. The security series provides guidance from the Centers for Medicare and Medicaid Services (CMS) on the rule titled "Security Standards for the protection of e-PHI" and includes these Security Rule topics: (a) administrative safeguards, (b) physical safeguards, (c) technical safeguards, (d) organizational policies, (e) basics of risk analysis and risk management, (f) Implementation for the Small Provider, and (g) HIPAA security guidance for remote use of and access to e-PHI. It must be noted that while there is no one approach that will guarantee successful implementation of all the security standards, this series aims to explain specific requirements, the thought process behind those requirements, and possible ways to address the provisions. Security implementation is not a one-time project; instead it is an on-going, dynamic process with the understanding that it can create new challenges as organizations and technologies change. The security requirements are designed to be technology neutral and scalable from the very largest of health plans to the very smallest of provider practices. Compliance with the Security Rule requires an evaluation of security measures that are currently in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of complex factors unique to each organization.

**Credibility.** The educational papers are posted in the official government website of the Department of Health and Human Services (HHS) which is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. HHS represents almost a quarter of all federal outlays, and it administers more grant dollars than all other federal agencies combined. HHS' Medicare program is the nation's largest health insurer, handling more than one billion claims per year.

**Joyce, M. (2005).** HIPAA security rule implementation in home care -- Closing the gaps. *Journal of Health Care Compliance, 7*(5), 51-52. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=18085377&site=ehost-live&scope=site

**Abstract.** This article looks at the role of the Health Insurance Portability and Accountability Act in the transmission of electronic protected health information (e-PHI). Topics include (a) prevalence of the use of electronic medical records; (b) implications of e-PHI for confidentiality and individual privacy; and (c) key elements to be considered in allowing the receipt of electronic signatures.

**Summary.** HIPAA covered entities continue to face challenges with identifying and controlling the inappropriate transmission of e-PHI due to the ease with which sensitive data can be stored or transmitted. Personally owned hand-held devices, USB ports on key chains, and renegade use of home computers to complete patient records provide an ongoing security challenge to protecting the integrity, availability, and confidentiality of e-PHI. Moreover, the growth of virtual offices makes it more difficult to effectively address the security gaps. Several recommendations are provided in order to alleviate some of the concerns caused due to these challenges. They are (a) continued education and training reinforcing company policies related to the appropriate use of technology, (b) continued education to broaden understanding of the potential security gaps in the transmission process, (c) availability of a centralized process to provide direction without retribution (for example, utilizing help desk as gatekeepers to assist in preventing the inappropriate downloading of company information on to personally owned equipment), (d) development or purchase of alternate software solutions that offer added layers of protection that would allow for secure electronic transmissions, and (e) continual evaluation of real and potential gaps and their level of risk and then determining the most appropriate solutions. These recommendations help to not only protect e-PHI but also allow the business to continue to function and thrive.

**Credibility.** This article was published in the Journal of Health Care Compliance, which provides articles written by health care professionals and industry experts on how to avoid government inquiries and stay in compliance with health care laws and regulations. Joyce Marks is Assistant Vice President of corporate compliance at Gentiva Health Services, a consulting organization with 40 years of clinical experience in the homecare industry that helps clients navigate the increasingly complex regulatory and reimbursement business environment.

**Kelly, C. J. (2005).** HIPAA compliance in 30 days or less. *Computerworld, 39*(15), 36. Retrieved from Vocational and Career Collection database: http://search.ebscohost.com/login.aspx?direct=true&db=voh&AN=16700489&site=ehost-live&scope=site

**Abstract.** This article focuses on implementing the Health Insurance Portability and Accountability Act (HIPAA) within covered entities and shares examples of how the author managed the HIPAA implementation process at an undisclosed state agency.

**Summary.** This article presents an example of how to execute the security rule implementation plan for HIPAA compliance within a reasonable timeframe. The author highly recommends the website of National Institute of Standards and Technology (NIST) as a source for the latest available documents related to HIPAA security and compliance. A special publication 800-66, titled "An Introduction Resource Guide for Implementing HIPAA Security Rule" is a step-by-step guide for planning security rule implementations. It is highly advisable that organizations implementing HIPAA security rule have security expertise for any infrastructure changes. For instance, technical expertise is needed for understanding the vulnerabilities of a networked computing environment in order to perform a thorough risk assessment. Similarly, covered entities must understand what constitutes a true security breach and how to detect one in order to develop comprehensive security incident response procedures. In regards to contingency planning and disaster recovery, the organization needs a background in conducting an impact analysis and testing a disaster recovery plan. The organization must fully understand technical and physical aspects of the security ruling. For example, in the area of device and media controls, the covered entities must develop policies on how to keep someone from carrying off e-PHI using portable USB flash devices. The organization must determine the types of audit controls to be deployed and types of activities to be tracked for auditing purposes in addition to the storage of audit trails, its access levels and securing audit records from tampering.

**Credibility.** This article is published in Computerworld, which is leading source of technology news and information for IT industry practitioners worldwide. Computerworld's website and print publication have won more than 100 awards in the past five years alone. C.J. Kelly has worked in IT for close to 20 years and in security for the past 8 years. She holds the CISSP and CISM designations among other technical certifications and a Master of Science degree.

**Oatway, D (2004).** A road map to HIPAA compliance. *Nursing Homes: Long Term Care Management*, *53*(5), 65-69. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=13224803&site=ehost-live

**Abstract.** This article details the steps needed by nursing homes to comply with the Heath Insurance Portability and Accountability Act of 1996. Topics include (a) information on how to assign security responsibility; (b) tools that can help initiate security reminders to the facility; and (c) explanation on the Risk Analysis.

**Summary.** In this article the author assists covered entities with planning for the steps needed to comply with the HIPAA Security Rule. The author notes that while the Privacy Rule covers all protected health information (PHI), paper or electronic, the Security Rule applies only to electronically stored or transmitted PHI. The focus of the article is on necessitating a deliberate effort to identify vulnerabilities and threats to the confidentiality, integrity, and availability of e-PHI. Every covered entity must have a designated security official who needs to ensure that the security analysis is performed comprehensively for their facility. Any documentation related to Security Rule analysis must be maintained in a written record (which may be electronic) and must include the risk analysis and reports of actions, policies, and procedures. Each standard must be identified as being *required* or *addressable* in accordance with the final rule along with a suggestion of the timing (either *now* or *later*). It must be noted that while it would be desirable to implement everything *now*, the reality of limited resources and the need to collect and analyze data before taking some actions dictate a phased approach. The timing suggestions must be evaluated by each facility, as it is not part of the rule. The facility's security official must use a comprehensive HIPAA security matrix to ensure that each requirement is addressed and to document all issues related to the security of e-PHI.

**Credibility.** This article is published in Nursing Homes: Long Term Care Management journal and appeared in Health Source: Nursing/Academic Edition database that provides nearly 550 scholarly full text journals, including nearly 450 peer-reviewed journals focusing on many medical disciplines. David Oatway has been the President of Care-Track Systems LLC and Vice Chairman of the American Association of Nurse Assessment Coordinators. He has also been a consultant on healthcare automation, clinical systems development and regulatory affairs for more than twenty years.

**Oatway, D (2004).** HIPAA security is next. *Nursing Homes: Long Term Care Management, 53*(1), 37-40. Retrieved from Vocational and Career Collection database: http://search.ebscohost.com/login.aspx?direct=true&db=voh&AN=12118757&site=ehost-live&scope=site

**Abstract.** This article presents advice on the implementation of data security component for health care facilities to meet the Health Insurance Portability and Accountability Act security requirements deadline before April 21, 2005. Topics include (a) factors to consider for determining appropriate and reasonable security measures; (b) types of Security Rule specifications; and (c) compliance-related activities pertaining to the Security Rule.

**Summary.** This article presents an interpretation of how the HIPAA security rule can be implemented by covered entities in order to be compliant with HIPAA laws. The article provides guidance on the following compliance related activities pertaining to the Security Rule: (a) administrative safeguards; (b) physical safeguards; (c) technical safeguards; (d) organizational requirements; and (e) policies, procedures or documentation requirements.

Covered entities planning to acquire new software or hardware that may contain or manage e-PHI should study the rule as part of the acquisition process and ensure that their selected vendor(s) can support its requirements. As the word *reasonable* appears 57 times in the rule, it clearly demonstrates government's willingness to scale solutions according to facilities different sizes and degrees of sophistication. Although this leaves a lot of room for interpretation, certain factors must be considered for determining appropriate and reasonable security measures. They are (a) the size, complexity, and capabilities of your organization; (b) its technical infrastructure, hardware, and software security capabilities; (c) what reasonable security measures might cost; and (d) the probability and criticality of potential risks to the facility's e-PHI. There are two types of Security Rule specifications (a) required where the entity must implement the specification; and (b) addressable where the entity must assess whether the specification is a *reasonable* and *appropriate* safeguard for its particular environment and secondly as applicable, implement the specification, if reasonable and appropriate, or document why its implementation is not reasonable and appropriate, and document any alternatives taken as being reasonable and appropriate.

**Credibility.** This article is published in Nursing Homes: Long Term Care Management journal. David Oatway has been the President of Care-Track Systems LLC and Vice Chairman of the American Association of Nurse Assessment Coordinators. He has also been a consultant on healthcare automation, clinical systems development and regulatory affairs for more than twenty years.

**Satinsky, M. (2005).** HIPAA security rule compliance for procrastinators. *Review of Ophthalmology, 12*(2), 38-41. Retrieved from Academic Search Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=16190666&site=ehost-live&scope=site

**Abstract.** This article focuses on the benefits and pitfalls of the Health Insurance Portability and Accountability Act and the U.S. deadline for Security Rule implementation. Topics include (a) means of protecting personal health information; and (b) details on the changes necessary for compliance with the Privacy Rule.

**Summary.** This article focuses on covered entities that are not yet fully compliant with the HIPAA regulations. The author acknowledges the close association between the Privacy and Security Rules and clarifies that while the Privacy Rule protects all forms of personal health information, the Security Rule is designed to protect a subset of PHI, electronic personal health information such as electronic data transactions, email communications, practice management systems, personal digital assistants and website portals. The author provides recommendations to comply with the Security Rule that include (a) designating a security official who may be the same person as privacy official; (b) forming a security team comprising of members from different parts of the organization; (c) analyzing potential risks and vulnerabilities by evaluating the likelihood and cost of each; (d) determining the priorities for the practice; (e) developing a budget that includes cost of allowing your current employees to spend time on implementation, budget for external consultants, cost of software and the cost of any physical modifications needed to be made at work; (f) developing, implementing and maintaining security measures; (g) training staff; and (h) monitoring implementation on an ongoing basis. The author stresses the need to make the compliance process participatory by engaging the entire staff in the process.

**Credibility.** This article is published in the Review of Ophthalmology journal. Margie Satinsky is the President of Satinsky Consulting, LLC, a medical practice consulting firm that provides services to healthcare providers throughout North Carolina. Her areas of expertise include information technology planning, HIPAA Privacy and Security Rule training, and medical practice start-up. She was formerly the President of the ReXMeD Physician Hospital Organization, and the Director of Managed Care Contracting and Operations for the Duke Health System. She has a BA in history from Brown University, an MA in political science from the University of Pennsylvania, an MBA from the Wharton School at the University of Pennsylvania, and advanced training in healthcare negotiation and conflict resolution from the Harvard School of Public Health.

**Wilcox, S., & Brown, B. (2005).** Responding to security incidents -- Sooner or later your systems will be compromised. *Journal of Health Care Compliance, 7*(2), 41-48. Retrieved from Business Source Complete database: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=16717526&site=ehost-live

**Abstract.** This article deals with security standards for the federal Health Insurance Portability and Accountability Act that established administrative procedures to guard data integrity, confidentiality and availability. Topics include (a) components of a comprehensive security plan; (b) requirements for effective response to security incidents; (c) role descriptions of computer security incident response team (CSIRT); (d) CSIRT incident response sequence; and (e) CSIRT initial setup and preparation.

**Summary.** This article focuses on policies and procedures to address security related incidents. The author recommends creating a computer security incident response team and clearly defining their roles and responsibilities in a document containing the response sequence of each defined roles.

Most attempts to compromise systems, such as virus attacks, spyware, phishing, and social engineering attacks can be prevented by employing up-to-date virus checkers and firewalls and by properly training users in safe computing practices; however even with good protections in place systems are still vulnerable to new types of attacks against which existing tools are ineffective. Effective response to security incidents requires quick recognition of problems and fast mobilization of skilled staff to counter threats, mitigate damage, and return systems to normal. Effective response requires complete advance documentation of response procedures and precise enumeration of responsibilities of everyone who needs to respond to the emergency. In addition, effective response requires that these procedures be tested and refined based on a thorough review of the results of the testing (or responses to actual security incidents). It should be noted that security incident response should never include retaliation as it's wise to let the appropriate law enforcement or other administrative authorities handle all punitive or other actions directed at perpetrators of computer crimes. If there is an attack or intrusion, the response should focus on containing and eradicating the problem, plugging the security hole, and getting back to business.

**Credibility.** This article is published in the Journal of Health Care Compliance, which provides articles written by health care professionals and industry experts on how to avoid government inquiries and stay in compliance with health care laws and regulations. Spence Wilcox and Bob Brown are nationally known HIPAA experts with HealthCare Information Solutions in Kalamazoo, Michigan; a private company that provides services in corporate information technology and governance, particularly in Sarbanes Oxley and HIPAA. They are also HIPAA consultants and the developers of the HIPAA compliance software, HIPAASays.

## Selection of Appropriate Emerging Technologies Purported to Improve the Security of Electronic Data Exchanges

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

**Abstract.** This article presents the degree of success of operating within the rules of Title II of the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA); success depends upon the ability of the organization to establish a program that ensures thoughtful and consistent execution of the requirements of HIPAA.

**Summary.** This article focuses on a program approach to deal with the security and privacy standards required by HIPAA. The significant ongoing requirements of these two standards set both security and privacy apart from the other standards. In the traditional approach, HIPAA compliance is the single driving reason for information security and privacy program redesign, followed by the addition of any other factors considered prudent into the redesign. The advantage to this approach is that since HIPAA is the law, staffs generally accommodate any operational changes whether or not they understand those rules. The disadvantage to this approach is by just following HIPAA, the covered entity may not provide a complete security–privacy program as it merely establishes the minimum requirements across an organization and is likely to leave gaps.

The second approach, known as the progressive approach, requires the organization to look at all the gaps to ensure the privacy and confidentiality of patient data as well as the general security of all other data of importance to the organization and its constituents. The organization's Chief Privacy Officer (CPO) and Chief Security Officer (CSO) must play an important role in this effort. The advantage of using the progressive approach is that the officers can look beyond what is required by HIPAA and make use of their experience with information security, best practices and at technologies that solve more than just the HIPAA *problem*. Once the organization has made an initial decision on the approach to be employed, the next steps with the HIPAA implementation include: (a) establishing department ownership, (b) defining education and training needs, (c) developing a schedule, (d) designing a program that includes risk assessment, (e) documenting roles and responsibilities, (f) developing policies, and (g) getting outside consulting help for certain HIPAA implementation phases. When the program is up and running, the covered entity must perform an evaluation preferably by a third party to document findings and observations on any HIPAA non compliance issues.

**Credibility.** This article is published in Information Systems Security journal, which is a peer-reviewed publication. Chris Brown is the Information Security Program Administrator for Independent Health, a healthcare solutions company in Buffalo, New York.

**Choi, B.Y., Capitan, E.K., Krause, S.J., & Streeper, M.M. (2006).** *Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules*. Retrieved from SpringerLink database: http://www.springerlink.com/content/035317748wrk775t/fulltext.pdf

**Abstract.** This paper discusses the challenges associated with privacy in health care in the electronic information age based on the Health Insurance Portability and Accountability Act (HIPAA) and the Security Rules. Topics include current outstanding issues that act as impediments to the successful implementation of security measures and possible avenues of future research.

**Summary.** Electronic Data Interchange (EDI) has been a crucial element in helping covered entities meet the demands of high volume patient loads, maintain efficient business partner relationships, and expand market reach. In addition, organizations such as the American National Standards Institute (ANSI) have led the effort towards standardization of electronic data in order to facilitate ease of use of electronic information within and across different organizations. HIPAA seeks to validate and assist with the inevitability of electronic data transactions, while also addressing privacy and security issues that may stem from converting to the use of vulnerable electronic transactions. The Security Rule requires compliance actions in the following categories: (a) administrative safeguards—formal practices to manage security and personnel; (b) physical safeguards—protection of computer systems and the facilities within which they reside; (c) technical safeguards— means to control and monitor information access, including technology to secure data-in-transit; (d) organizational requirement—business associate contracts; and (e) policies and procedures and documentation requirements.

Compliance with the Security Rule entails identifying areas that must be changed in order to support the standards, quantifying risk areas, and devising pro-active solutions to those risk areas.

Ensuring security requires assessment and mitigation of security and privacy risks, policy and procedures development, incident response and recovery, evaluation of business associate contracts, hiring and termination impacts, compliance and awareness training, access control and authentication, auditing, and periodic review. The struggle to ensure the security of private health information can only be solved by a compromise between ease and efficiency and privacy protection. Organizations must be diligent in maintaining and improving HIPAA standards of privacy and security which will help them to improve patient care and provide peace of mind that will contribute to the overall success of a better health care system.

**Credibility.** This article is published in the Journal of Medical Systems, which is a peer-reviewed publication and is written by Choi, Capitan, Krause and Streeper from James Madison University, Harrisonburg, Virginia. The authors have thoroughly cited credible sources in various sections of the article and provided a top quality reference list at the end.

**Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2011).** *Guide to SSL VPNs*. Retrieved April 10, 2011, from, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800113.pdf

**Abstract.** This publication seeks to assist organizations in understanding secure socket layer (SSL) virtual private network (VPN) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. This document provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also provides a comparison with other similar technologies such as IPsec VPN's and other VPN solutions.

**Summary.** This guide provides guidance on secure transmission over communication networks. It focuses on SSL VPN that provides remote users with secure access to web applications and client/server applications, and secure connectivity to internal networks. A VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and other information transmitted between two endpoints. Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The document provides several recommendations and considerations for organizations planning SSL VPN deployments and states that they should first identify and define requirements, and evaluate several products to determine their fit into the organization. Despite the popularity of SSL VPNs, they are not intended to replace Internet Protocol Security (IPsec) VPN's as the two VPN technologies are complementary and address separate network architectures and business needs. IPsec has emerged as the most commonly used network layer security control for protecting communications, while SSL is the most commonly used transport layer security control.

**Credibility.** The document is published by the Computer Security Division at the National Institute of Standards and Technology (NIST). NIST is an agency of the U.S. Department of Commerce and is the nation's first federal physical science research laboratory. This guidance document has been authorized by both U.S. Department of Commerce and National Institute of Standards and Technology.

**Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A., Ritchey, R., & Sharma, S. (2011).** *Guide to IPsec VPNs*. Retrieved April 17, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80077.pdf

**Abstract.** This publication seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec). This document presents information that is independent of particular hardware platforms, operating systems, and applications, other than providing real-world examples to illustrate particular concepts.

**Summary.** The guide provides an overview of the types of security controls that can provide protection for Transmission Control Protocol/Internet Protocol (TCP/IP) network communications, which are widely used throughout the world. IPsec is a network layer security protocol that provides encryption and integrity protection for data packets during sensitive data transmissions and exchanges. It has become the most common network layer security control, typically used to create a virtual private network (VPN). A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks. VPN's are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control. The four key layers that work together in Transmission Control Protocol/Internet Protocol (TCP/IP) network communications are application, transport, network, and data link. The guide presents a phased approach to IPsec planning and implementation that helps in achieving successful IPsec deployments. Organizations should also implement additional technical, operational, and management controls that support and complement IPsec implementations.

**Credibility.** The document is published by the Computer Security Division at the National Institute of Standards and Technology (NIST). NIST is an agency of the U.S. Department of Commerce and is the nation's first federal physical science research laboratory. This guidance document is highly credible and has been authorized by both U.S. Department of Commerce and National Institute of Standards and Technology.

**Hoffman, S., & Podgurski, A. (2007).** *Securing the HIPAA security rule*. Retrieved March 15, 2011, from http://ssrn.com/abstract=953670

**Abstract.** The threat to data security associated with the electronic storage and transmission of health information is serious enough that it has merited regulatory intervention, which came in the form of the HIPAA Security Rule, promulgated as part of the HIPAA Privacy Rule on April 20, 2005. The article develops recommendations for revisions to the Rule, focusing on a proposed *best practices* standard.

**Summary.** This article provides recommendations on how the proposed HIPAA Security Rule can be enhanced to provide meaningful compliance guidance to covered entities. The authors recommend an establishment of a *best practices* standard for Security Rule compliance. The Rule's *general requirements* section 56 reads as follows:

> Make reasonable efforts to identify and employ best practices relating to security measures, software development, validation, maintenance, and software system administration that are either commonly used by similarly-situated business entities and governmental institutions or can be clearly demonstrated to be superior to best common practices. (p. 10)

The best current practices requirement must apply to all standards and implementation specifications. Thus, the language of the standards and specifications must be read to require covered entities to employ the best current practices concerning the subject matter of each provision (for example: access control and validation, encryption and decryption mechanisms). The most effective tool for Security Rule compliance is to employ the assistance of security product vendors who can conduct risk analysis, choose appropriate security mechanisms, and follow up with covered entities periodically to ensure that their technology is updated. The vendors must have expertise with respect to both security products and the legal requirements of the HIPAA Security Rule, and a certification mechanism must be established to ensure that they are qualified. Some covered entities may not have the expertise or resources to determine best practices on their own, and in such cases the development of an industry of security product vendors is essential to the achievement of consistent HIPAA Security Rule compliance. These recommendations help to tighten security standards during health data exchanges, which can significantly bolster the protection offered by the federal regulations to data subjects and will empower the HIPAA Security Rule to provide meaningful security in the realm of e-PHI.

**Credibility.** This paper is written by Sharona Hoffman and Andy Podgurski. Hoffman is Associate Dean, Co-Director of Law-Medicine Center, Professor of Law, and Professor of Bioethics at Case Western Reserve University School of Law. Podgurski is Associate Professor of Electrical Engineering and Computer Science at Case Western Reserve University. The paper is published in the Journal of Internet Law which is a peer-reviewed publication.

**Lerner, S., & Koh, J. (2004).** HIPAA compliance: Step-by-step approach to security rules deadline in April. *Benefits & Compensation Digest, 41*(10), 1-21. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14615716&site=ehost-live&scope=site

**Abstract.** This article presents the steps needed by multiemployer health plan sponsors to comply with the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. Topics include: (a) deadline for compliance; (b) safeguards that must be maintained by health plans to ensure that their electronic protected health information is protected against any reasonably anticipated threats; and (c) documentation required under the HIPAA security rules.

**Summary.** This article provides a step-by-step approach for covered entities to comply with the HIPAA Security Rule. The rules require group health plans and other covered entities to protect the confidentiality, integrity and availability of e-PHI that they create, receive, maintain or transmit, either internally or to external entities. The necessary steps needed to comply with the regulations must begin as soon as possible since security compliance is complex and plans may need time to change systems, policies and procedures periodically. In addition, as changes are made to the systems, they may become vulnerable to external threats and thus security related issues must be reviewed to establish secure methods of communication with trading partners at the same time. Risk analysis must be performed to assess potential risks of e-PHI and evaluate (a) assets such as information systems and the infrastructure that contains or transports e-PHI, (for example: claims processing software, personal data, e-mail and the fund office's Internet connection.); (b) threats such as hackers or a disgruntled member of the fund office staff who could cause damage to the fund's system; and (c) vulnerabilities such as inadequate virus protection and/or a weak firewall that can make e-PHI vulnerable to unauthorized access. In addition to risk analysis, plans must conduct a security assessment, which includes comparing current practices and technology to the HIPAA security requirements in order to identify any potential gaps. Covered entities must also develop policies and procedures for managing e-PHI, review business associate agreements, amend plan documents, train office staff and document findings based on the risk analysis, HIPAA security gap analysis and policies and procedures required by the regulations.

**Credibility.** This article is published in the Benefits and Compensation Digest, a publication of the Healthcare Performance Management Institute, described as a research and education organization. It is written by Stuart Lerner and Jane Koh. Both authors are consultants with Segal's Administration and Technology Consulting Practice. Segal provides multiemployer benefit plans with practical solutions to their benefits administration and technology needs. Segal has more than 30 years of experience in improving the efficiency and cost-effectiveness of multiemployer benefits administration functions. The authors have worked with many multiemployer plans and assisted them in complying with the HIPAA security rules.

**Morrissey, J. (2011).** *HIE: Health information exchange*, *85*(2), 22-27 Retrieved from Business Source Complete database: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=58793660&site=ehost-live&scope=site

**Abstract.** The article reports on the increasing number of U.S. hospitals that develop health information exchange programs as a result of the 2011 passage of the Health Information Technology for Economic and Clinical Health Act. A discussion of the benefits that are associated with health information exchange is presented.

**Summary.** This article highlights the increasing use of health information exchange due to the dangling financial incentives associated with meaningful use of electronic health records as a result of 2011 passage of the Health Information Technology for Economic and Clinical Health Act. Health Information Exchange (HIE) is the collection of activities and technologies for sharing data generated from separate sources of clinical information to manage both individual patients and groupings of people with similar clinical conditions. This Act encourages an increasing number of covered entities to get involved in health information exchanges to improve the quality and outcome of the patient. The key requirements of meaningful use of HIE, for hospitals as well as for providers, are to record the information in organization's electronic health record and to allow and facilitate that information to follow the patients when they seek care. Federal funding has boosted the viability of HIE which covers both start-up costs and ongoing operations. The federal government's approach is to work with existing HIE efforts rather than fund them from scratch, providing the connective technology and shared services that make a wide-ranging HIE. The article provides several examples of hospitals taking part in the health information exchange initiative to support the best possible patient care. This in turn helps hospitals to set themselves up for government incentives by forming an effective and accountable care organization.

**Credibility.** This article is published in Hospitals and Health Networks, which is a leading publication for hospital and system executives and is written by John Morrissey. Morrissey has more than 20 years of experience covering and participating in issues related to the use of information to deliver healthcare better, cheaper and faster. As an editor and reporter for Modern Healthcare magazine from 1987 to 2005, Morrissey produced more than one thousand articles and gained an expertise in areas of quality improvement, performance measurement, and the impact of IT strategy on healthcare delivery and efficiency. Since May 2010 he has written articles on a freelance basis for a number of publications in the healthcare field, including Government Health IT, Modern Healthcare, Hospitals and Health Networks and Trustee.

**Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, D. & Steinberg, D. (2008).** *An introductory resource guide for implementing health insurance portability and accountability act (HIPAA) security rule*. Retrieved March 31, 2011, from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

**Abstract.** This Special Publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. It was written to help to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule.

**Summary.** This publication is intended to serve a diverse audience of individuals with HIPAA Security Rule implementation, management, and oversight responsibilities and organizations, federal and nonfederal, considered to be a *Covered Entity* under 45 C.F.R. Sec.160.103. HIPAA Security Rule focuses on implementing effective risk management to adequately and effectively protect e-PHI. The assessment, analysis, and management of risk provides the foundation of a covered entity’s Security Rule compliance efforts, serving as tools to develop and maintain a covered entity’s strategy to protect the confidentiality, integrity, and availability of e-PHI. Under the Security Rule, covered entities are required to evaluate risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities. NIST Risk Management Framework provides the covered entity with a disciplined, structured, extensible, and repeatable process for achieving risk-based protection related to the operation and use of information systems and the protection of e-PHI. It represents an information security life cycle that facilitates continuous monitoring and improvement in the security state of the information systems within the organization. The activities that compose the NIST RMF are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of a system development life cycle. A risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations.

**Credibility.** The document is published by the Computer Security division at the National Institute of Standards and Technology (NIST). The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation’s measurement and standards infrastructure. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. This document has been authorized by both U.S. Department of Commerce and National Institute of Standards and Technology.

**Schoppmann, M. J., & Sanders, D. L. (2004).** *HIPAA compliance: The law, reality, and recommendations*. Retrieved from ScienceDirect database: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B7CWD-4DDNR0X-8-1&_cdi=18104&_user=2148430&_pii=S1546144004001516&_origin=search&_zone=rslt_list_item&_coverDate=10%2F01%2F2004&_sk=999989989&wchp=dGLbVtz-zSkzV&md5=0f11dd3c9ce80360a0969a17ffde6ade&ie=/sdarticle.pdf

**Abstract.** Through the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal government regulates three of the most controversial issues in medical practice management: privacy, electronic transactions, and security. Through practical insights, the authors' goal is to introduce physicians to HIPAA's basic tenets, the evolutionary nature of the regulations, and the concept that they can manage HIPAA without bankrupting their practices or sealing themselves away from their patients.

**Summary.** This article provides recommendations to physicians who fall under the covered entity bracket and thus need to comply with HIPAA Security Rule. The author provides guidance on security that is designed to address safeguards and set uniform, minimum standards for *electronic* related issues such as access authorization, encryption and decryption, data backup and storage, disaster recovery plans, facility security plans, contingency operations, maintenance records, security reminders, password management, workforce security, termination procedures and safe disposal. Physician practices must continue to follow specific steps and develop policies and procedures to comply with the security standards, implementing at least the requirements such as designating a security officer responsible for the development and implementation of security policies and procedures, safeguarding and limiting access to e-PHI, training staff members on security rules, establishing and imposing sanctions for staff members who break the rules, maintaining a log of certain disclosures, adopting a complaint process that identifies a contact person for complaints and developing procedures to permit individuals to inspect, copy, and/or amend their own records. The author assures that in carrying out these simple steps, physicians not only will be a long way towards compliance with HIPAA but also will find themselves far removed from those who will face the inevitable focus of the federal government.

**Credibility.** This article is published in the Journal of the American College of Radiology, which is a peer-reviewed publication and is written by Michael J. Schoppmann and Denise L. Sanders. Schoppmann is a healthcare attorney regarded nationally for devoting his career to the defense of healthcare professionals in actions brought before state licensing authorities, federal healthcare agencies (i.e., the Office of Inspector General, Medicare, Medicaid, DEA, OSHA) hospital review boards (credentialing and disciplinary), billing/coding/fraud investigative units (both public and private) and in the myriad forms of complex healthcare litigation involving physicians and medical practices. Schoppmann has served as a faculty member of the Cornell University, Johnson Graduate School of Management, Executive Program in Health Care Delivery Management and The University of Rochester, Simon School of Graduate Studies, Executive Program in Health Care Delivery Management. Ms. Sanders is a healthcare attorney and her practice focuses on assisting clients with a wide range of health care regulatory and compliance matters including counseling physicians and other practitioners on federal and state health care program compliance, Medicare reimbursement, self-referral, fraud and abuse, privacy and security issues, transactions, and licensure.

**Vogt, V., & Wittwer, D. (2007).** Open standards for data exchange in healthcare systems. Retrieved March 12, 2011, from http://diuf.unifr.ch/main/is/sites/diuf.unifr.ch.main.is/files/file/studentprojects/reports/eGov_HS07_E-Health_Platforms_Architectures_%28DanielWittwer_JoelVogt%29.pdf

**Abstract.** The objective of this seminar thesis is to illustrate the need for comprehensive information management and technical integration strategies as one of the important steps towards efficient intra and inter-organizational and IT-supported healthcare processes. This thesis focuses on Health Level 7 (HL7) and Service Oriented Architecture (SOA). The combination of the HL7 standard together with the principles of SOA provides a basis and possible solution for automated, efficient and collaborative e-health processes.

**Summary.** This thesis focuses on information management and technical integration to build an efficient health care process. The definition of e-health and the need for information management is discussed in detail including the characteristics of the term *e-health,* which is helpful as a basis for designing an improved collaboration and data exchange between health care organizations, individuals and patients. The 10 *e's* of e-health presented are: (a) e-fficiency; (b) enhancing quality; (c) evidence based e-health interventions; (d) empowerment of consumers and patients; (e) encouragement of a new relationship between the patient and health professional towards a true partnership; (f) education for healthcare providers and consumers; (g) enabling information exchange and communication in a standardized way between health care establishments; (h) extending the scope of health care beyond its conventional boundaries; (i) ethics; and (j) equity. Data standardization and technical integration strategies are of high importance for successful e-health initiatives. In order to be able to electronically share patient-related information among stakeholders in the healthcare system, decision making institutions need to agree upon common data standards and integration technologies. Both HL7 and SOA standards and technologies can be used as a building block of a national healthcare system to ensure the stability of a successful electronic health system.

**Credibility.** This thesis is written by Joel Vogt and Daniel Wittwer for the Department of Informatics at University of Fribourg, Switzerland. The authors cite credible sources and provide a top quality reference list at the end of the document.

## Conclusion

Information technology continues to play an important role in improving the quality, safety and efficiency of health care. Health care organizations are using information technology to promote evidence-based care, add value to health care services, and empower consumers through access to information and decision tool (AHIP, 2005). Health insurance providers report a commitment to the goal of creating an interconnected health care system in which health information can be exchanged electronically, so that doctors and hospitals have patients' information in the right place, at the right time (AHIP, 2008). According to Bogen (2001),

> Nevertheless, increased computerization of medical information requires increased surveillance of policies and procedures to protect the confidentiality of private medical data. Failure to develop, implement, audit, and document information security procedures could result in serious consequences, such as penalties and loss of reputation, market share, and patient trust. (p. 6)

According to Lentz (2000), the 1996 Health Insurance Portability and Accountability Act makes it a violation to share patient information with anyone not authorized to know that information. The implications of HIPAA related security breaches can be serious and covered entities must have a greater stake in ensuring information security at all levels. HIPAA guidelines must be followed to not only comply with the federal laws, but more importantly to protect customer data and improve patient care.

Complying with the Security rules not only protects covered entities from internal or external security threats but also safeguards organizations from any potential federal civil and / or criminal penalties that may be imposed upon them due to a violation. Appropriate security measures must therefore be carefully implemented to protect e-PHI within covered entities to comply with the law and to also ultimately improve the overall quality of patient care. This annotated bibliography examines literature that addresses four aspects of securing electronic data exchanges for covered entities to ensure greater compliance with the HIPAA Security Rule: (a) assessing security frameworks; (b) potential risks and liabilities of violation; (c) ways to protect CIA; and (d) selecting appropriate new technologies. Each aspect is summarized below.

## Assess Existing Frameworks in Relation to the Security Rule

Haas (2006) has depicted the various stakeholders involved in a typical health care system (as cited in Vogt and Wittwer, 2007, p. 4) (see Figure 4).

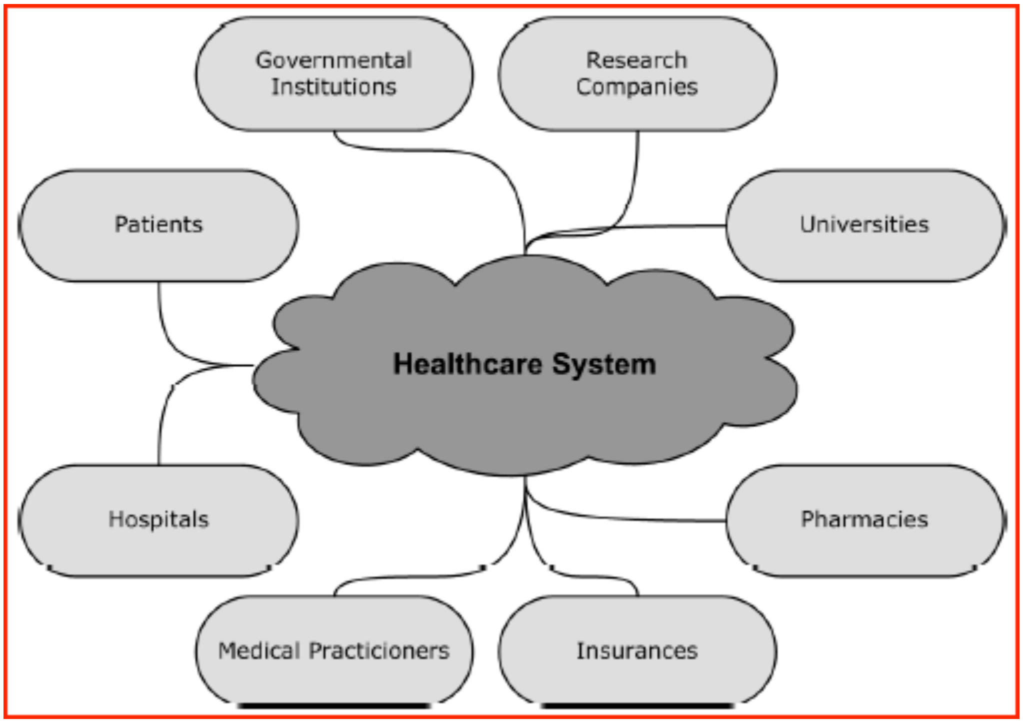
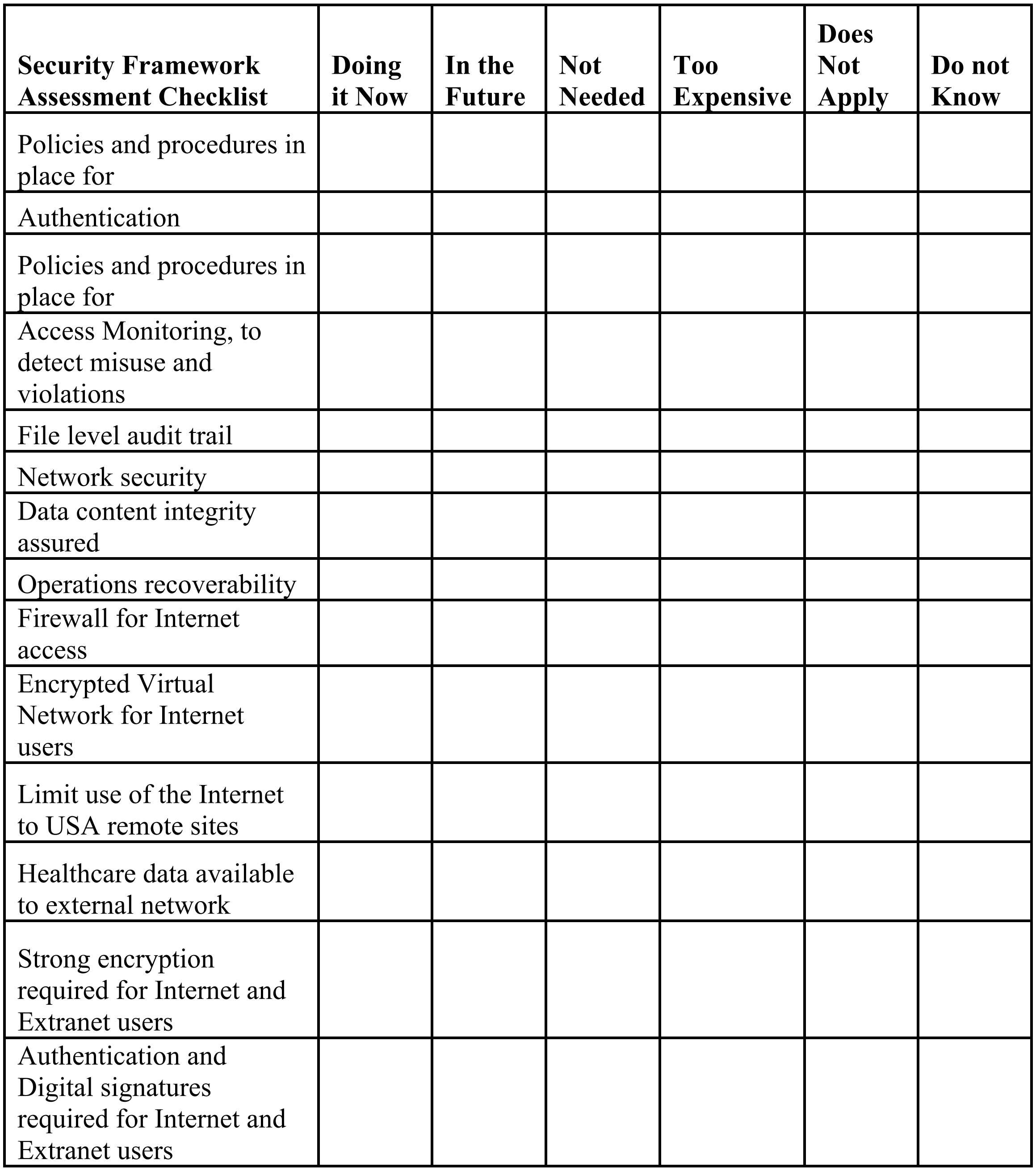


*Figure 4.* Stakeholders in a healthcare system, adapted from Haas (2006) (as cited in Vogt & Wittwer, 2007, p. 4).

Figure 4 reveals the potential complexities of electronic data exchanges that transmit sensitive health data between stakeholders. Covered entities are obligated to comply with the law to securely transmit data and continue to protect confidential patient information. MedDocs Central (2011) provides a security checklist for health care providers (see Figure 5). This checklist is intended to assist healthcare providers in an assessment of their existing security framework prior to implementing health information technology capabilities such as electronic health information exchange.



| **Security Framework Assessment Checklist** | **Doing it Now** | **In the Future** | **Not Needed** | **Too Expensive** | **Does Not Apply** | **Do not Know** |
|---|---|---|---|---|---|---|
| Policies and procedures in place for | | | | | | |
| Authentication | | | | | | |
| Policies and procedures in place for | | | | | | |
| Access Monitoring, to detect misuse and violations | | | | | | |
| File level audit trail | | | | | | |
| Network security | | | | | | |
| Data content integrity assured | | | | | | |
| Operations recoverability | | | | | | |
| Firewall for Internet access | | | | | | |
| Encrypted Virtual Network for Internet users | | | | | | |
| Limit use of the Internet to USA remote sites | | | | | | |
| Healthcare data available to external network | | | | | | |
| Strong encryption required for Internet and Extranet users | | | | | | |
| Authentication and Digital signatures required for Internet and Extranet users | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Dial-in protections (e.g. Caller-ID, callback, and encryption) | | | | | | |
| Mobile access (laptop/handheld) physical protection and data encryption | | | | | | |
| Healthcare data over Infrared or Radio links encrypted and authenticated | | | | | | |
| Control IP addresses, prevent IP spoofing | | | | | | |
| Periodic verification / maintenance of security measures | | | | | | |
| Policies and procedures in place for | | | | | | |
| Protection of remote / external access | | | | | | |
| Policies and procedures strictly enforced (even fines) | | | | | | |
| Periodic user training on required procedures | | | | | | |
| Virus checking all files | | | | | | |
| Digital signatures applied to documents | | | | | | |
| Security / confidentiality committees | | | | | | |
| Scalable confidentiality and security procedures | | | | | | |
| Written security policies and documentation | | | | | | |

*Figure 5.* HIPAA security checklist for healthcare providers - Self-evaluation checklist as shown in MedDocs Central (2011).

## Identify Potential Risks and Liabilities During Electronic Data Exchanges

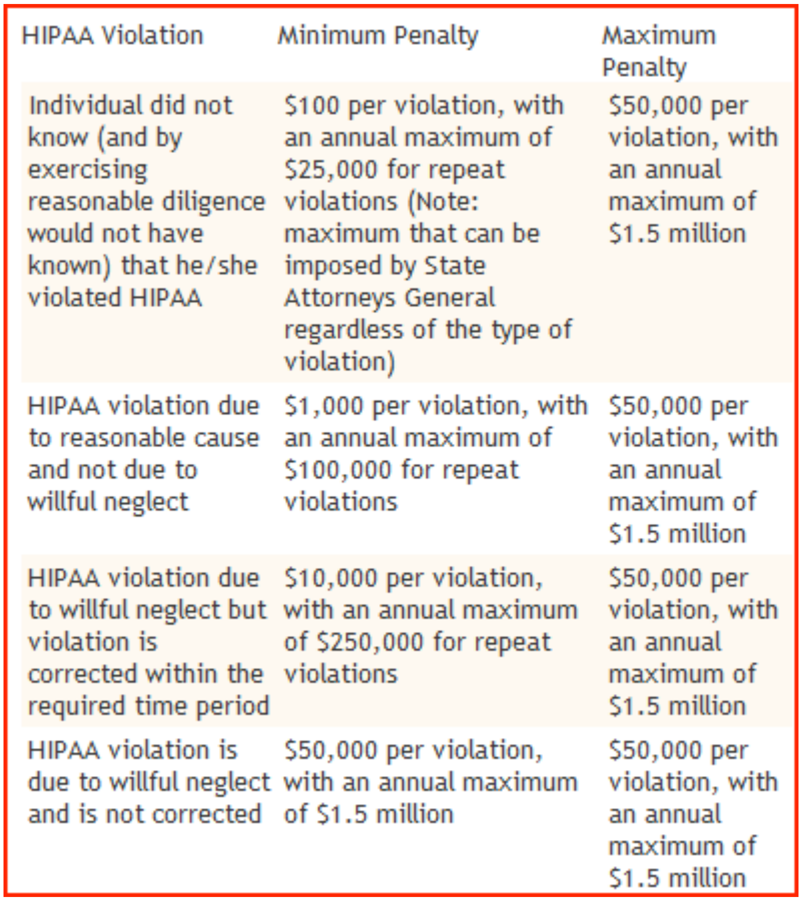
Once the covered entity has gathered and documented relevant data on e-PHI, it is necessary to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the e-PHI. Risk analysis and risk management are on-going processes that should provide the covered entity with a detailed understanding of the risks to e-PHI and the security measures needed to effectively manage those risks (HHS, 2011). HHS (2011) provides a process to perform risk analysis, outlined as follows:

> (a) identify the scope of the analysis, (b) gather data, (c) identify and document potential threats and vulnerabilities, (d) assess current security measures, (e) determine the likelihood of threat occurrence, (f) determine the potential impact of threat occurrence, (g) determine the level of risk and (h) identify security measures and finalize documentation. (p. 5)

Sloane highlights the liabilities for covered entities due to HIPAA non-compliance:

> Civil and criminal penalties ranging from $50,000 to $250,000 in fines and one to 10 years in prison will be levied by HHS' civil rights division and the U.S. Justice Department if patient information is used for commercial advantage, personal gain or malicious harm. (Sloane, 2003, para. 7)

The American Medical Association (2011) provides a detailed chart of civil penalties for a HIPAA violation (see Figure 6). Civil penalties range from $100 to $50,000 per violation.



| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA | $100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation) | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to reasonable cause and not due to willful neglect | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to willful neglect but violation is corrected within the required time period | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation is due to willful neglect and is not corrected | $50,000 per violation, with an annual maximum of $1.5 million | $50,000 per violation, with an annual maximum of $1.5 million |

*Figure 6.* Civil penalties for HIPAA violation as shown in American Medical Association (2011).

## Protect the Confidentiality, Integrity, and Availability of E-PHI Data Exchanges

In order to comply with HIPAA security rules, covered entities are required to implement appropriate security measures to protect e-PHI from anticipated threats or vulnerabilities to the security of sensitive patient information. Lerner and Koh (2004) describe three larger types of safeguards, including:

> (a) administrative safeguards involving the business processes for managing e-PHI, (b) technical safeguards applicable to software and hardware used to store and transmit e-PHI, and (c) physical safeguards addressing facilities that house software and hardware used to store and transmit e-PHI, as well as facilities that serve as working space for staff who handle e-PHI. (para. 9)

Scholl et al. (2008) outline a comprehensive list of HIPAA Security Rule *standards* and an associated list of *implementation specifications* which are grouped under the administrative, physical, and technical safeguard sections. HIPAA covered entities are required to comply with all standards of the Security Rule with respect to e-PHI (Scholl et al., 2008, p. 8). Covered entities are encouraged to maintain a comprehensive security matrix to document these standards and implementation specifications. Oatway (2004) states that each implementation specification must be identified as *required* or *addressable* in accordance with the final rule along with a suggestion of the timing (either now or later). According to Oatway (2004), a covered entity must take in to account the following factors in deciding which standard to use:

> “(a) the size, complexity, and capabilities of the covered entity; (b) the covered entity's technical infrastructure, hardware, and software security capabilities; (c) the costs of security measures; and (d) the probability and criticality of potential risks to e-PHI.” (p. 1)

## Select Appropriate Emerging Technologies to Secure Electronic Data Exchanges

The promise of emerging technologies is that electronic data exchanges can be adequately made secure by employing them. One common approach is to use a secure socket layer virtual private network (SSL VPN). A VPN is a virtual network, built on top of existing physical networks designed to provide a secure communications mechanism for data and other information transmitted between two endpoints (Frankel, Hoffman, Orebaugh & Park, 2011). Another commonly used network layer security control is the Internet Protocol Security (IPsec) which provides protection without the need of modifying any applications on the client side or the servers (Frankel, Kent, Lewkowski, Orebaugh, Ritchey & Sharma, 2011). Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection: (a) confidentiality, (b) integrity, (c) peer authentication, (d) replay protection, (e) traffic analysis protection and (f) access control (Frankel, Kent, Lewkowski, Orebaugh, Ritchey & Sharma, 2011).

These technologies are designed to enhance covered entities' capabilities to protect the confidentiality, integrity and availability of e-PHI that are created, received, maintained or transmitted to internal and external trading partners. With their use, covered entities can continue to be in greater compliance with HIPAA Security Rules during electronic data exchanges, thus minimizing any risk of exposing protected and sensitive health information to unintended recipients.

# References

AHIP. (2005). *Innovations in health information technology.* Retrieved June 11, 2011, from http://www.ahipresearch.org/pdfs/AHIP_InvHealthIT_05.pdf

AHIP. (2008). *Trends and innovations in health information technology.* Retrieved June 11, 2011, from http://www.ahipresearch.org/pdfs/AHIP_InvHealthIT_05.pdf

American Medical Association. (n.d.). *HIPAA violations and enforcement*. Retrieved March 29, 2011, from http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.shtml

Bazerman, C. (2010). *The Informed Writer: Using sources in the disciplines*. Writing@CSU. Colorado State University. Retrieved April 23, 2011 from http://writing.colostate.edu/textbooks/informedwriter/chapter10.pdf

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

BlueCross BlueShield of Montana. (2011). *HIPAA Blue book*. Retrieved April 23, 2011, from https://www.bcbsmt.com/SiteCollectionDocuments/employer/HIPAABlueBook.pdf

Boerner, M.C. (2010). View HIPAA breaches affecting 500 or more individuals online. *Journal of Health Care Compliance*, *12*(3), 31-68. Retrieved from Business Source Premier database:

http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=50320776&site=ehost-live&scope=site

Bogen, J. (2001). *HIPAA challenges for information security: Are you prepared?* Retrieved June 11, 2011, from http://www.healthcio.com/white%20papers/hipaa%20security.pdf

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

Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., Saunders, M., White, R., & Palmquist, M. (2005). *Content analysis*. Writing@CSU. Colorado State University. Retrieved April 23, 2011 from http://writing.colostate.edu/guides/research/content/pop2a.cfm

Choi, B.Y., Capitan, E.K., Krause, S.J., & Streeper, M.M. (2006). *Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules*. Retrieved from SpringerLink database: http://www.springerlink.com/content/035317748wrk775t/fulltext.pdf

CMS. (2010). *HIPAA overview*. Retrieved March 29, 2011, from https://www.cms.gov/hipaageninfo

CMS. (2010). *Privacy and security standards*. Retrieved April 30, 2011, from http://www.cms.gov/HIPAAGenInfo/04_PrivacyandSecurityStandards.asp#TopOfPage

Collmann, J., Lambert, D., Brummett, M., DeFord, D., Coleman, J., Cooper, T., . . . Dorofee, A. (2004). Beyond good practice: Why HIPAA only addresses part of the data security problem [Abstract]. *International Congress Series, 1268*, 113-118. Retrieved from

Academic Search Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=13327283&site=ehost-live&scope=site

Conn, J. (2009). New sheriff in town. *Modern Healthcare*, *39*(33), 13. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=43864577&site=ehost-live

Connor, P. (2011). *Searching electronic databases*. Writing@CSU. Colorado State University. Retrieved April 23, 2011 from http://writing.colostate.edu/guides/researchsources/electronicresearch/searchingdatabase.cfm

Denning, D. (2003). *Information Technology and Security*. Retrieved May 14, 2011, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA485002

de Wolf, A.V., Sieber, E.J., Steel, M.P., & Zarate, A.O. (2006). Part II: HIPAA and disclosure risk issues. *IRB: Ethics & Human Research, 28*(1), 6-11. Retrieved from Psychology and Behavioral Sciences Collection database: http://search.ebscohost.com/login.aspx?direct=true&db=pbh&AN=19384905&site=ehost-live

Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2011). *Guide to SSL VPNs*. Retrieved April 30, 2011, from, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800113.pdf

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A., Ritchey, R., & Sharma, S. (2011). *Guide to IPsec VPN*. Retrieved April 17, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80077.pdf

Gallagher, A.L., & Barrett, W.C. (2004). An assessment of HIPAA security preparedness. *Medical Benefits, 21*(11), 8-9. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=13461666&site=ehost-live&scope=site

General DataComm. (2004). *Connectivity and internetworking in the healthcare industry HIPAA Compliance*. Retrieved April 5, 2011, from http://www.gdc.com/pubs/0224_schippa_ab04.pdf

Hall, M., Hoffman, S., & Sobel, R. (2008). *The HIPAA headache.* Retrieved from Jstor *database*: http://www.jstor.org/stable/25165283

HHS. (2011). *About HHS*. Retrieved April 30, 2011, from http://www.hhs.gov/about/index.html

HHS. (2011). *Basics of risk analysis and risk management*. Retrieved June 11, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

HHS. (2011). *For covered entities*. Retrieved April 5, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

HHS. (2011). *Guidance on risk analysis requirements under the HIPAA security rule*. Retrieved April 23, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

HHS. (2011). *Health information privacy*. Retrieved April 30, 2011, from http://www.hhs.gov/ocr/privacy/

HHS. (2010). *Reassessing your security practices in a health IT environment*. Retrieved April 5, 2011, from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848086_0_0_18/SmallPracticeSecurityGuide-1.pdf

HHS. (2011). *Summary of the HIPAA security rule*. Retrieved April 5, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

HHS. (2010). *The HIPAA privacy rule and health IT*. Retrieved April 30, 2011, from http://healthit.hhs.gov/portal/server.pt?open=512&objID=1174&parentname=CommunityPage&parentid=26&mode=2&in_hi_userid=10732&cached=true

HHS. (2011). *Understanding health information privacy*. Retrieved April 23, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Hoffman, S., & Podgurski, A. (2007). *Securing the HIPAA security rule*. Retrieved March 15, 2011, from http://ssrn.com/abstract=953670

Joyce, M. (2005). HIPAA security rule implementation in home care -- Closing the gaps. *Journal of Health Care Compliance, 7*(5), 51-52. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=18085377&site=ehost-live&scope=site

Juniper Networks. (2010). *Unified access control addresses HIPAA compliance*. Retrieved April 5, 2011, from http://www.juniper.net/us/en/local/pdf/solutionbriefs/3510296-en.pdf

Kelly, C. J. (2005). HIPAA compliance in 30 days or less. *Computerworld, 39*(15), 36. Retrieved from Vocational and Career Collection database: http://search.ebscohost.com/login.aspx?direct=true&db=voh&AN=16700489&site=ehost-live&scope=site

Leedy, P. D., & Ormrod, J. E. (2005). *Practical Research*. Upper Saddle River, NJ: Pearson Education.

Lentz, R. (2000). Privacy matters. *Modern Physician*, *4*(5), 39. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=3177643&site=ehost-live

Lerner, S., & Koh, J. (2004). HIPAA compliance: Step-by-step approach to security rules deadline in April. *Benefits & Compensation Digest, 41*(10), 1-21. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14615716&site=ehost-live&scope=site

Litwak, P. (2005). Security of health information--the latest HIPAA deadline. *Mental Health Weekly.* Retrieved April 17, 2011, from http://find.galegroup.com/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=HRCA&docId=A128245637&source=gale&srcprod=HRCA&userGroupName=s8492775&version=1.0

MedDocs Central. (n.d.). *HIPAA security checklist for healthcare providers.* Retrieved June 11, 2011, from http://www.meddocscentral.com/resources/articles/hipaa-security-checklist.pdf

MedImpact. (2011). *About Medimpact.* Retrieved April 30, 2011, from http://www.medimpact.com/about_us/faq.asp#clients

Michael, P., & Pritchett, E. (2003). *The impact of HIPAA electronic transmissions and health information privacy standards*. Retrieved from ScienceDirect database: doi: 10.1016/S0002-8223(01)00132-8

Morrissey, J. (2011). *HIE: Health Information Exchange*, *85*(2), 22-27 Retrieved from Business Source Complete database: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=58793660&site=ehost-live&scope=site

Naughton-Travers, P.J. (2004). Here comes the latest HIPAA deadline. *Behavioral Health Management, 24*(6), 53-58. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=15524152&site=ehost-live

North Carolina. DHHS. (2011). *Purposes of HIPAA*. Retrieved March 09, 2011, from http://hipaa.dhhs.state.nc.us/hipaa2002/whatishipaa/whatishipaa.html

Oatway, D (2004). A road map to HIPAA compliance. *Nursing Homes: Long Term Care Management*, *53*(5), 65-69. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=13224803&site=ehost-live

Oatway, D (2004). HIPAA security is next. *Nursing Homes: Long Term Care Management, 53*(1), 37-40. Retrieved from Vocational and Career Collection database:

http://search.ebscohost.com/login.aspx?direct=true&db=voh&AN=12118757&site=ehost-live&scope=site

Ormondroyd, J., Engle, M., & Cosgrave, T. (2009). *Critically analyzing information sources*. Retrieved from Cornell University, Olin & Uris Libraries Web site: http://olinuris.library.cornell.edu/ref/research/skill26.htm

Pagliari, C., Detmer, D., & Singleton, P. (2007). *Potential of electronic personal health records*. Retrieved from Jstor *database*: http://www.jstor.org/stable/25690019

Pickert, K. (2009). Glossary. *Time, 174*(8), 26-27. Retrieved from Middle Search Plus database: http://search.ebscohost.com/login.aspx?direct=true&db=mih&AN=43886325&site=ehost-live&scope=site

Reid, S., Barnes, L., & Kowalski, D. (2011). *Definition of organization*. Writing@CSU. Colorado State University. Retrieved April 23, 2011 from http://writing.colostate.edu/guides/processes/organize/pop2a.cfm

Saint Mary's University (2009). *Writing a literature review.* Retrieved May 07, 2011 from http://www.smu.ca/administration/library/litrev.html

Satinsky, M. (2005). HIPAA security rule compliance for procrastinators. *Review of Ophthalmology, 12*(2), 38-41. Retrieved from Academic Search Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=16190666&site=ehost-live&scope=site

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, D. & Steinberg, D. (2008).

*An introductory resource guide for implementing health insurance portability and accountability act (HIPAA) security rule*. Retrieved March 31, 2011, from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Schoppmann, M. J., & Sanders, D. L. (2004). *HIPAA compliance: The law, reality, and recommendations*. Retrieved from ScienceDirect database: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B7CWD-4DDNR0X-8-1&_cdi=18104&_user=2148430&_pii=S1546144004001516&_origin=search&_zone=rslt_list_item&_coverDate=10%2F01%2F2004&_sk=999989989&wchp=dGLbVtz-zSkzV&md5=0f11dd3c9ce80360a0969a17ffde6ade&ie=/sdarticle.pdf

Skidmore College. (n.d.). *Annotated bibliographies*. Retrieved April 11, 2011, from http://ucblibraries.colorado.edu/how/evaluate.htm

Sloane, T. (2003). A HIPAA has its day. *Modern Healthcare*, *33*(15), 21. Retrieved from Health Source: Nursing/Academic Edition database: http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=9608291&site=ehost-live

Smith, H. (2003). *The HIPAA final security rule - More than a new security standard.* Retrieved March 12, 2011, from https://www.issa.org/Library/Journals/2003/October/Smith%20-%20The%20HIPPA%20Final%20Security%20Rule%20-%20More%20Than%20a%20New%20Security%20Standard.pdf

Sternstein, A. (2007). *Confusing terms prompt call for health IT glossary*. Retrieved from National Journal's Technology Daily http://www.govexec.com/dailyfed/1107/110907tdpm1.htm

Stevenson, G. (2007). *Managing information privacy & security in healthcare: A primer on health information security.* Retrieved May 07, 2011, from http://www.himss.org/content/files/CPRIToolkit/version6/v7/D03_Security_Primer.pdf

The George Washington University. (n.d.). *Tools for preparing Literature Reviews*. Retrieved from The George Washington University at Washington D.C., http://www.gwu.edu/~litrev/s01.html

University of North Carolina. (n.d.). *Writing center: Literature reviews*. Retrieved from University of North Carolina at Chapel Hill, Writing Center Web site: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Vogt, V., & Wittwer, D. (2007). *Open standards for data exchange in healthcare systems*. Retrieved March 12, 2011, from http://diuf.unifr.ch/main/is/sites/diuf.unifr.ch.main.is/files/file/studentprojects/reports/eGov_HS07_E-Health_Platforms_Architectures_%28DanielWittwer_JoelVogt%29.pdf

West Virginia State Privacy Office. (2011). *HIPAA privacy & HIPAA security*. Retrieved April 5, 2011, from http://www.privacy.wv.gov/tips/Pages/HIPAAPrivacyHIPAASecurity.aspx

Wikipedia. (2011). *Centers for Medicare and Medicaid services*. Retrieved April 18, 2011, from http://en.wikipedia.org/wiki/Centers_for_Medicare_and_Medicaid_Services

Wikipedia. (2011). *Information security*. Retrieved May 07, 2011, from http://en.wikipedia.org/wiki/Information_security

Wilcox, S., & Brown, B. (2005). Responding to security incidents -- Sooner or later your systems will be compromised. *Journal of Health Care Compliance, 7*(2), 41-48. Retrieved from Business Source Complete database:

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=16717526&site=ehost-live

Wilcox, S., & Brown, B. (2004). Risk assessment, risk management, and the HIPAA security rule: A matter of life and death? *Journal of Health Care Compliance, 6*(4), 43-45. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14951524&site=ehost-live&scope=site

Withrow, C.S. (2010). How to avoid a HIPAA horror story. *Healthcare Financial Management, 64*(8), 82-88. Retrieved from Business Source Complete database: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=52842270&site=ehost-live&scope=site

Yale University. (2010). *HIPAA guidance*. Retrieved April 23, 2011, from http://hipaa.yale.edu/guidance/index.html

Zotero. (n.d.). *About*. Retrieved April 30, 2011, from http://www.zotero.org/about/

## Appendix A

| Search Engine / Database | Search Terms | Results: # | Quality | Comments |
|---|---|---|---|---|
| Academic Search Premier Index – EBSCO HOST (UO Libraries) | HIPAA + Security | 68 | Good | This index is a great resource for exploring HIPAA Security topics in detail. |
| | HIPAA + Electronic + Data + Exchange | 291 | Fair | |
| | HIPAA + Security + Breach | 1 | Good | |
| | Managing + Information + Security + in +Healthcare | 19011 | Fair | |
| | Protecting +Electronic +Personal Health +Records | 6160 | Good | |
| | HIPAA +Security + Vulnerabilities | 177 | Good | |
| | HIPAA + Security +Requirements | 11 | Good | |
| | HIPAA +Legal + Implications | 109 | Good | |
| | Implementing + HIPAA + Security + Rule | 301 | Good | |

| Search Engine / Database | Search Terms | Results: # | Quality | Comments |
|---|---|---|---|---|
| ACM Digital Library | HIPAA + Security | 663 | Good | This library is good starting resource to search for this literature review. |
| | HIPAA + Electronic + Data + Exchange | 206 | Fair | |
| | HIPAA + Security + Breach | 180 | Fair | |
| | Managing + Information + Security + in +Healthcare | 1227 | Poor | |
| | Protecting +Electronic +Personal Health +Records | 689 | Fair | |
| | HIPAA +Security + Vulnerabilities | 165 | Poor | |
| | HIPAA + Security + Requirements | 508 | Good | |
| | HIPAA +Legal + Implications | 134 | Fair | |
| | Implementing + HIPAA + Security + Rule | 154 | Good | |

| **Search Engine / Database** | **Search Terms** | **Results: #** | **Quality** | **Comments** |
|---|---|---|---|---|
| CiteSeer$^x$ Search Index | HIPAA + Security | 594 | Poor | There are not many focused resources available; however it is worth pursuing those few ones that closely match the topic in question. |
| | HIPAA + Electronic + Data + Exchange | 153 | Fair | |
| | HIPAA + Security + Breach | 137 | Fair | |
| | Managing + Information + Security + in +Healthcare | 3029 | Poor | |
| | Protecting +Electronic +Personal Health +Records | 2662 | Poor | |
| | HIPAA +Security + Vulnerabilities | 153 | Fair | |
| | HIPAA + Security + Requirements | 578 | Poor | |
| | HIPAA +Legal + Implications | 88 | Poor | |
| | Implementing + HIPAA + Security + Rule | 301 | Fair | |

| **Search Engine / Database** | **Search Terms** | **Results: #** | **Quality** | **Comments** |
|---|---|---|---|---|
| ERIC | HIPAA + Security | 5 | Poor | This search tool is not useful for conducting research for this literature review. |
| | HIPAA + Electronic + Data + Exchange | 0 | Poor | |
| | HIPAA + Security + Breach | 0 | Poor | |
| | Managing + Information + Security + in +Healthcare | 0 | Poor | |
| | Protecting +Electronic +Personal Health +Records | 0 | Poor | |
| | HIPAA +Security + Vulnerabilities | 0 | Poor | |
| | HIPAA + Security + Requirements | 0 | Poor | |
| | HIPAA +Legal + Implications | 1 | Poor | |
| | Implementing + HIPAA + Security + Rule | 0 | Poor | |

| Search Engine / Database | Search Terms | Results: # | Quality | Comments |
|---|---|---|---|---|
| Google Scholar Advanced | HIPAA + Security | 18400 | Fair | This is a good resource worth pursuing. |
| | HIPAA + Electronic + Data + Exchange | 8680 | Fair | |
| | HIPAA + Security + Breach | 3660 | Fair | |
| | Managing + Information + Security + in +Healthcare | 73100 | Good | |
| | Protecting +Electronic +Personal Health +Records | 94700 | Fair | |
| | HIPAA +Security + Vulnerabilities | 2370 | Good | |
| | HIPAA + Security + Requirements | 14500 | Good | |
| | HIPAA +Legal + Implications | 7390 | Fair | |
| | Implementing + HIPAA + Security + Rule | 6630 | Good | |

| Search Engine / Database | Search Terms | Results: # | Quality | Comments |
|---|---|---|---|---|
| Health Source: Nursing/Academic Edition– EBSCO HOST (UO Libraries) | HIPAA + Security | 38 | Good | This index is a great resource for this literature review. |
| | HIPAA + Electronic + Data + Exchange | 142 | Fair | |
| | HIPAA + Security + Breach | 1 | Good | |
| | Managing + Information + Security + in +Healthcare | 2331 | Fair | |
| | Protecting +Electronic +Personal Health +Records | 1643 | Good | |
| | HIPAA +Security + Vulnerabilities | 21 | Good | |
| | HIPAA + Security + Requirements | 8 | Good | |
| | HIPAA +Legal + Implications | 65 | Good | |
| | Implementing + HIPAA + Security + Rule | 172 | Fair | |

| **Search Engine / Database** | **Search Terms** | **Results: #** | **Quality** | **Comments** |
|---|---|---|---|---|
| IEEE Computer Science Digital Library | HIPAA + Security | 100 | Good | This is a good resource for this literature review. The searches are however limited to a maximum of 100 results. |
| | HIPAA + Electronic + Data + Exchange | 100 | Fair | |
| | HIPAA + Security + Breach | 100 | Poor | |
| | Managing + Information + Security + in +Healthcare | 100 | Fair | |
| | Protecting +Electronic +Personal Health +Records | 100 | Fair | |
| | HIPAA +Security + Vulnerabilities | 100 | Fair | |
| | HIPAA + Security + Requirements | 100 | Fair | |
| | HIPAA +Legal + Implications | 100 | Poor | |
| | Implementing + HIPAA + Security + Rule | 100 | Fair | |

| Search Engine / Database | Search Terms | Results: # | Quality | Comments |
|---|---|---|---|---|
| Project Muse (UO Libraries) | HIPAA + Security | 27 | Poor | This e-journal may not be a helpful resource for this literature review. |
| | HIPAA + Electronic + Data + Exchange | 8 | Poor | |
| | HIPAA + Security + Breach | 4 | Poor | |
| | Managing + Information + Security + in +Healthcare | 106 | Poor | |
| | HIPAA +Security + Vulnerabilities | 2 | Poor | |
| | HIPAA + Security + Requirements | 14 | Poor | |
| | HIPAA +Legal + Implications | 20 | Poor | |
| | Implementing + HIPAA + Security + Rule | 5 | Poor | |

| **Search Engine / Database** | **Search Terms** | **Results: #** | **Quality** | **Comments** |
|---|---|---|---|---|
| Pub Med | HIPAA + Security | 840 | Fair | This index does not contain relevant resources pertaining to this literature review. |
| | HIPAA + Electronic + Data + Exchange | 9 | Poor | |
| | HIPAA + Security + Breach | 9 | Fair | |
| | Managing + Information + Security + in +Healthcare | 42 | Poor | |
| | Protecting +Electronic +Personal Health +Records | 9 | Fair | |
| | HIPAA +Security + Vulnerabilities | 4 | Fair | |
| | HIPAA + Security + Requirements | 87 | Fair | |
| | HIPAA +Legal + Implications | 21 | Poor | |
| | Implementing + HIPAA + Security + Rule | 4 | Poor | |

| **Search Engine / Database** | **Search Terms** | **Results: #** | **Quality** | **Comments** |
|---|---|---|---|---|
| World Cat<br>(Summit Libraries) | HIPAA + Security | 675 | Good | This search engine is helpful for this literature review |
| | HIPAA + Electronic + Data + Exchange | 17 | Fair | |
| | HIPAA + Security + Breach | 10 | Fair | |
| | Managing + Information + Security + in +Healthcare | 89 | Poor | |
| | Protecting +Electronic +Personal Health +Records | 47 | Fair | |
| | HIPAA +Security + Vulnerabilities | 7 | Fair | |
| | HIPAA + Security + Requirements | 113 | Fair | |
| | HIPAA +Legal + Implications | 32 | Fair | |
| | Implementing + HIPAA + Security + Rule | 10 | Good | |