A CROSS CASE ANALYSIS OF DATA SECURITY MEASURES BEFORE AND AFTER THE 1996 HIPAA ENACTMENT

Jacqueline H. Phillips

Submitted to the faculty of the School of Informatics
in partial fulfillment of the requirements
for the degree
Master of Science in Health Informatics
Indiana University
May 2009

Accepted by the Faculty of Indiana University,
in partial fulfillment of the requirements for the degree of Master of Science
in Health Informatics

Master’s Thesis Committee

____

Josette Jones, R.N., PhD
Committee Chair

____

Anna Mc Daniel, R.N., D.N.S.

____

George Allen, M.S.

____

Harold, J. Grimes

TABLE OF CONTENTS

ABSTRACT

Jacqueline H. Phillips

A CROSS CASE ANALYSIS OF DATA SECURITY MEASURES BEFORE AND AFTER THE 1996 HIPAA ENACTMENT

The protection of sensitive healthcare information has been a concern since the Common Law of Confidentiality and its protection of the doctor-patient relationship. Although there was no legislation specifically mentioning electronic healthcare data disclosure until The Health Insurance Portability and Accountability Act (HIPAA) of 1996, there was other legislation related to personal data security such as the Freedom of Information Act of 1966, the Privacy Act of 1974, and laws protecting the medical records of alcohol and drug abuse patients in 1983. The enactment of HIPAA in 1996 and the following Privacy and Security Standards that were an outgrowth of the original legislation, became the impetus for more comprehensive and specific legislation and standards relating to healthcare data security. As technology and data sharing has advanced exponentially, it would seem the need for improved security measures, standards and policies would also increase. Although there are still inconsistencies between some state and federal statutes, standardization of messaging, access, and data transmission in all aspects of healthcare has become the norm, allowing the rapid identification and implementation of best practices based on outcomes and patient safety, and the improvement of public healthcare through real-time trending and bio-surveillance. Nationally there are now certification procedures for specific vendor products, based on suggested interoperability standards, including data security. The development and implementation of interoperability standards between the Electronic Health Record (EHR) and the Personal Health Record (PHR) will enable any patient to control the provider access to personal medical information and still enable rapid access to accurate information from multiple healthcare entities. The documents selected reflected the presence of 21 specific data security measures, in legislation or standards, prior to, and after HIPAA enactment in 1996. A cross case analysis was conducted to determine if these measures have increased or decreased since enactment. Measures were grouped into related categories of legislation, access, breach, enforcement, security, policy, and communication. Results show that most of the same measures existed prior to HIPAA enactment, but the number of documents containing these measures, either in legislation or standards, has markedly increased. The greatest increase was in the categories of breach and enforcement.

LIST OF TABLES

Word/Code Definitions

Word/Code	Definition
Access	the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. HIPAA Section 164.304
Act	Synonyms - law, piece of legislation, statute, decree, enactment, measure, bill Thesaurus: English (U.S.) Microsoft Word 2003
Audit	a methodical examination and review (referring to determining who had accessed or what had been done to data- e.g. audit trail) audit. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/audit
Authorization	to prove or serve to prove the authenticity : see confirm**:** to give new assurance of the validity of (referring to the validity of the person/organization attempting to access data) confirm. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/confirm
Breach	loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data- Also: security incident, intrusion Title IX of Public Law 109-461 of Veteran's Benefits
Communicate	to convey knowledge of or information about **:** make known to cause to pass from one to another (referring to the sharing of information among entities) communicate. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/communicate
Confidentiality	the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. FIPS 140-2 preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Title IX of Public Law 109-461 of Veteran's Benefits
Consent	to give assent or approval **:** AGREE (referring to approval from owner for someone else to access their information) consent. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-

	webster.com/dictionary/consent
Disclose	to make known or public :REVEAL (referring to making known private information) disclose. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/disclose
Enforce	to give force to **:** STRENGTHEN 2**:** to urge with energy 3**:** CONSTRAIN 5**:** to carry out effectively (referring to the ability to levy penalties for non-compliance with law) enforce. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/enforce
Law	a binding custom or practice of a community **:** a rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority (2)**:** the whole body of such customs, practices, or rules (3)**:** COMMON LAW (relating to data security, privacy or confidentiality) law. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/law
Penalty	the suffering in person, rights, or property that is annexed by law or judicial decision to the commission of a crime or public offense: the suffering or the sum to be forfeited to which a person agrees to be subjected in case of nonfulfillment of stipulations penalty. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/penalty
Policy	a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions b**:** a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body policy. (2008). In *Merriam-Webster Online Dictionary*. Retrieved November 7, 2008, from http://www.merriam-webster.com/dictionary/policy
Private	1 a**:** intended for or restricted to the use of a particular person, group, or class -personal b**:** belonging to or concerning an individual person, company, or interest **c** (1)**:** restricted to the individual or arising independently of others -not known or intended to be known publicly **:** SECRET (referring to personal information) private. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-

	webster.com/dictionary/private
Procedure	a traditional or established way of doing things b**:** PROTOCOL a particular way of accomplishing something or of acting b**:** a step in a procedure (referring to data security) procedure. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/procedure
Risk	possibility of loss or injury- (referring to loss or unauthorized access to data) risk. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/risk
Security	protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. Section 164.34 HIPAA
Standard	something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality- sometimes called specifications or protocols (referring to data security) standard. (2008). In *Merriam-Webster Online Dictionary*. Retrieved October 22, 2008, from http://www.merriam-webster.com/dictionary/standard
Store	to place or leave in a location (as a warehouse, library, or computer memory) for preservation or later use or disposal store. (2008). In *Merriam-Webster Online Dictionary*. Retrieved November 7, 2008, from http://www.merriam-webster.com/dictionary/store
Threat	an expression of intention to inflict evil, injury, or damage (referring to unauthorized data or system breach) threat. (2008). In *Merriam-Webster Online Dictionary*. Retrieved November 7, 2008, from http://www.merriam-webster.com/dictionary/threat

Introduction

The global concern for human health is as prevalent as the historical documentation of loss of human life from disease. Physicians from national medical associations formed the World Medical Association in 1947, and the World Health Organization (WHO), a specialized agency of the United Nations, came into existence in 1948, both to collaborate internationally to improve world health. Use of computers in healthcare began as early as 1958 in the United States, (Stead, 2006) with computerized collection of insurance information about patients. It has become a tidal wave of technology since then, expanding from local to regional and national networks, increasing to international proportions. The security of healthcare data is defined as, "a defined set of physical, administrative or technical actions used or taken to protect the confidentiality, availability or integrity of health information". (HITSP Webinar, Accessed September 29, 2008) Initial computer healthcare applications were proprietary, with no concern for interaction or integration among other applications or organizations. Security of the data collected was also confined to single corporations using simple security measures, such as passwords, at the corporate or application level.

The security of healthcare information was mandated by HIPAA, but state security rules can preempt Federal rules. State laws differ in access rights, the degree of privacy offered, or mention that records should be private, but don't address the degree of protection needed. (Hodge et al., 1999, Gostin et al., 2001)

As the use of computerized data and computerized imaging has increased in the healthcare setting, more and more vendors have developed integrated and scalable products for specific specialties and environments. With the increasing use and transmission of these electronic data, including, but not limited to, charting, lab values, patient demographic information, order and medication entry, images and insurance information, there is also an increasing demand for interfaces or integration that will join disparate electronic applications to enable the rapid sharing of data. With increased sharing comes increased chance of intentional or unintentional breaches, necessitating increased need for security.

With the national focus on the sharing of electronic healthcare data, the scope of information systems is ever widening from hospitals to regional and national networks, to international usage. (Kuhn et al., 2007). With many more organizations handling sensitive data, there is an increased chance that it will be accessed by unauthorized personnel and used in a detrimental way. Legislation and the standards developed to combat unauthorized access to, or sharing of, data has been the driving force in data security measures, and has been gradually enacted or mandated by local, state, and/or national bodies, sometimes without great success.

If the goal for healthcare is to provide the highest quality of clinical service and research, the collection of medical data is essential (British Medical Journal, 2007) In order to keep good clinical practice developing at the same rate as technology, medico-legal and safety issues must be globally addressed and agreed upon. (Pinnock et al., 2007) As more and more data and different data formats are being developed and exchanged on a regular basis, data security has also had to become more diverse. Data, and ways they has been accessed, stored and transmitted, have come under scrutiny. Many of these changes in data security are influenced by changes in legislation, technology and in healthcare delivery (Cruz-Correia et al., 2007). This cross case analysis, accompanied by frequency distribution of content related to data security, will examine data security measures prior to, and after HIPAA enactment in 1996.

Importance of Subject

It is believed that the increasing implementation of electronic records has the ability to make great improvements in healthcare. These systems may have the capability to ," decrease healthcare costs, increase the quality of healthcare, facilitate better departmental communication, create less paper confusion, allow use with authorized access only, allow storage of digital images, and increase overall efficiency in the healthcare system." (Steward, 2005) The increasing electronic implementation must not be at the cost of data security. Data security will become more and more important as the healthcare community moves toward a mandated electronic health record in 2014. The use of electronic records (EHR), (Electronic Medical Record-EMR) and (Personal Health Record-PHR) is increasing. Public reporting of healthcare data and rating of healthcare institutions based on these data will impact cost, revenue, treatment, and patient outcomes. Electronic data will be the ultimate method of data collection and sharing and submission of these data to agencies such as Center for Medicare and Medicaid Services (CMS) will become the source of physician bonuses or penalties and institution recognition. Providing secure text, laboratory values, and images necessitates different security methods. The legislation and standards that facilitate, or offer challenges in providing data security, originate from various sources, cover multiple data types, and targeting different entities. The development of healthcare technology systems will continue with the growth of regional and national healthcare networks sharing personal data. The law can determine what data can ultimately be collected, combined and transmitted for public use. (Rosenbaum et al., 2005) The secure, validated, standardized data in all areas of healthcare will be of paramount importance.

History

The modernization of the healthcare industry has been predicated on the use of electronic technology. The increased storage and use of electronic healthcare data has created a healthcare revolution (Choi et al., 2006). Policies and procedures relating to privacy of paper records were rendered obsolete with the advent of electronic records. It was quickly recognized that the gains of ease of access and transmission should not be at the cost of losing security.

Computer use in healthcare began as early as 1958, (Stead, 2006) with computerized records for collection of insurance information about patients. Security of healthcare data began as an ethical concept with a body of common law, but always subject to legal and ethical rules that were enforced by legal lawsuits. But over a fairly short period of time, it evolved into a legislative mesh governing data flow inside and outside organizations in addition to healthcare networks, healthcare insurers and governmental agencies. (Magnusson, 2004) As the use of computers and computerized imaging has increased in the hospital setting, more and more vendors have developed secure products for specific specialties in healthcare, such as operating and emergency rooms. Initially these vendor-developed applications were proprietary and departmentally specific, with no concern or provision for, interaction or integration with other applications or other institutions, so data security was only needed within each department, organization, or institution.

Legislation

Prior to HIPAA, there were many instances where legislation concerning data security singled out only certain populations. The Freedom of Information Act 1966 established privacy for health information, but only for members of the executive branch of the federal government. The Privacy Act of 1974 only addressed information collected by the federal government and its agencies, adding additional amendments in 1988 and 1990. The need for security for healthcare data was initially focused on certain groups of patients, such as those with HIV, or specific disease conditions. Regulations were issued in 1983, providing security for medical records of alcohol and drug abuse patients obtained by federally assisted programs. Electronic medical records continued to gain prominence, but there were certain inconsistencies noted in protection of any electronic records. For instance, video rental records were protected, but electronic healthcare records were not. (Cantor, 2001) The Health Insurance Portability and Accountability Act (HIPAA) enactment in 1996 became the impetus for providing security for all healthcare data types, no matter what population, but only for “covered entities”, defined as health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form.

When Congress couldn’t meet its self-imposed deadline of August 21, 1999 for passing comprehensive federal privacy legislation, President Clinton announced privacy regulations without any federal legislation in October of 1999. (Hussong, 2000) The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirements of HIPAA. The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule, called “covered entities”, as well as standards for individuals' privacy rights to understand and control how their health information is used. It acknowledged that fact that individuals’ health information had to be secure, but that public health and well-being also had to be protected by allowing the secure flow of that information. In essence, it defined the ways that health information could be used or disclosed. (http://www.hhs.gov/ocr/hipaa -Accessed 08/18/08)

Data security, as described by HIPAA, can be addressed in the terms of integrity, the prevention of unauthorized modifications of information, availability, the prevention of unauthorized withholding of information, and confidentiality, the prevention of unauthorized disclosure of information. (Susilo et al., 2006) HIPAA was divided into four very broad categories: transaction and code sets, which require the creation of standards, privacy, data security and provider identifiers, which requires the creation of digital labels. (Krohn, 2002) Although Healthcare providers were supposed to provide and comply with these security measures, HIPAA did not delineate how they were to be adopted and, initially, over what time frame. (Amatayakul, 2002) HIPAA also allowed each entity to determine how it would protect sensitive information. (Steward, 2005) Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the Administrative Simplification provisions.

On July 6, 2000 the National Committee on Vital and Health Statistics published; A Report to the Secretary of the U.S. Department of Health and Human Services on Uniform Data Standards for Patient Medical Record Information as Required by the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996. It documented calls for action, citing the 1991 Institute of Medicine (IOM) vision for the computer-based patient record, the 1993 General Accounting Office (GAO) recommendation to accelerate message format and healthcare terminology standards development, and the 1999 IOM attention to medicine errors from incomplete or illegible orders. It also noted that it wasn’t until December 1999 that President Clinton directed these recommendations to be evaluated by the Quality Interagency Coordination Task Force (QuIC), which responded with another action plan in February 2000. The report states,” Despite these and other calls to action, the nation still has not adopted the laws, standards, business practices, and technologies necessary to create a health information infrastructure. …To achieve further administrative simplification, it is essential that the healthcare delivery system adopt uniform standards for patient medical record information” The report went on to recommend that all standards that resulted should be consistent with HIPAA legislation, that there should be an adoption of “guiding principles” for selecting standards, that there should be funding provided to accelerate development, that international standards should be promoted, and that there should be governmental participation in standards development, just to name a few. The final rule for adopting HIPAA standards for security was published February 20th, 2003.

Standards

Organizations setting national standards have been in existence since 1918, when the American National Standards Institute (ANSI) was formed. By definition, a standards organization is any entity whose primary activities are “developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users” (Wikipedia – Accessed 08/18/2008). In this case, the users are the healthcare community. There are many standards organizations that are now developing standards for the healthcare industry. American Society for Testing and Materials (ASTM) - ASTM E31, International Standards Forum (ISF), and World Wide Web Consortium (W3C) are some bodies that now address standards relating to the security of electronic data.

In 1991 “The Computer-based Patient Record: An Essential Technology for Health Care” became the information technology vision of the Institute of Medicine (IOM). The acceleration of message format standardization was urged by the General Accounting Office (GAO) in 1993. The GAO also promoted healthcare terminology standards development in the document “Automated Medical Records: Leadership Needed to Expedite Standards Development”. (Report to the Secretary of the U.S. Department of Health and Human Services on Uniform Data Standards for Patient Medical Record Information, 2000) With the increasing use of electronic data in the hospital setting, there was also an increasing demand for interfaces that would join different electronic applications. Vendors now realized that applications needed to be secure, in addition to being scalable, functional, integratable, fast, efficient and user-friendly. In 2004 Certification Commission for Healthcare Information Technology (CCHIT) was established as an independent, nonprofit organization that has been recognized by the federal government as an official certification body for electronic health record products. It was formed by three leading industry associations in healthcare information management and technology - American Health Information Management Association (AHIMA), Healthcare Information and Management

Systems Society (HIMSS), and The National Alliance for Health Information Technology (Alliance). Its mission is to accelerate the adoption of health information technology by creating a credible, sustainable product certification program. The certification requirements are based on widely accepted industry standards and involve the work of hundreds of expert volunteers and input from a variety of stakeholders throughout the health care industry. The certification standards CCHIT is developing rely to a significant degree on the general standards being developed by HL7. (Pashel, 2008) One of the CCHIT work groups is specifically concerned with security. "The Task Force agreed that, in order to address consumers' concerns about using personal health records, PHR, patient privacy should be the primary goal of certification. The work we're doing now will enhance patients' trust that their personal health information will be protected when using a certified product." said Paul Tang, M.D. (http://www.cchit.org/about/news/releases/2008/Personal-Health-Records-PHR-Patient-Privacy-Focus-Task-Force.asp) Health and Human Services Secretary Michael Leavitt's vision is to "allow EHRs to be linked through a system that protects privacy while ensuring care providers have the data they need to deliver care of the highest quality with safety, cost-efficiency and convenience." (http://www/cchit.org/about/faq/general.asp)

With the national focus on electronic healthcare, the scope of information systems is ever widening from hospitals to regional networks, national infrastructures and beyond (Kuhn et al., 2007). As these data are shared between institutions and networks, there is an increasing emphasis on making sure the data remain secure throughout any transaction, whether in actual medical records, in insurance information, electronic order entry, diagnostic images, remote record access or e-mails between medical personnel and their patients. Data entry and access is now frequently web-based, again increasing the chance that it may be subject to unauthorized intrusion. The complexity of web-access data management was unveiled with the enactment of HIPAA. (Covich, 2002)

The object of the cross case analysis was to document the history and change, if any, of the security measures affecting individual patient healthcare data before and after HIPAA enactment. The documents in the cross case analysis discussed legislation, enacted or pending, as well as standards, enacted or in progress, relating to data security. Standards and standards organizations, their origins and purposes, were the topics of some documents. Frequently these standards discussed related legislative efforts, or a particular piece of legislation or standard. The articles pointed out that data security was often ineffective, due to being directed at specialized populations or organizations, while ignoring others. The fact that state law could pre-empt federal legislation, further reducing consistency in many cases, was discussed. Also mentioned was the lack of enforcement of some data security legislation even though enforcement and penalties for non-compliance were a part of the law. Several of the articles discussed data security in the context of individual privacy vs. disclosure for the improvement of public health and welfare. Data and individual information security has been a topic of discussion from the common law of confidential physician-patient relationships to the complex web of the current electronic healthcare information. This study will document and compare, by validated word/code frequency, single and related data security measures in legislation and standards prior to, and after, HIPAA enactment.

Current Practice or Understanding

Legislation

The enactment of national legislation concerning the security of healthcare information should help to ensure that the infrastructure protecting health information is functioning properly. Ideally, collection, access, storage, and communication of person health information, as well as penalties for its non-compliance, should be spelled out clearly and concisely in any national legislation.

The National Research Council in the mid 1990s decided that, with the advent of the electronic medical record (EMR), there would be an increase in the chance that patient health information might be inappropriately disclosed from within an organization or accessed, illegally, from without. The Council's recommendation was that healthcare organizations should ensure this not occur by designing appropriate security policies and procedures and using secure technology. As a result, at the state and Federal level, regulations were enacted to provide security during the transmission of electronic health data The European Union has also enacted similar legislation. (Malin and Airoldi, 2007) The beginning of HIPAA (Health Insurance

Portability and Accountability Act) was in 1995 in an insurance reform bill introduced by Senator Edward Kennedy and former Senator Nancy Kassebaum. The workgroup for Electronic Data Interchange (WEDI), a group called to together in 1991 by President Bush, made recommendations relating to the lowering of healthcare costs. These recommendations were found in a House bill which passed 421-2 and were to become the "administrative simplification" provisions of HIPAA which was introduced in March 1996. President signed the HIPAA bill into law on August 21, 1996. (Conn, 2006) HIPAA divided the medical record into: identified data, de-identified data, and limited data. Identified data include "any data that could be used by a recipient to uniquely identify the person from an individual patient record." It defined "electronic protected health information as "individually identifiable health information transmitted by electronic media and maintained in electronic media, subject to certain exceptions such as employment records held by a covered entity in its role as employer information covered by Federal Education Records Protection Act-FERPA." Access to these data speaks to data security; controlling of the disclosure of data, whether it is limiting access by not allowing the viewing of certain data elements, or by destroying or modifying the data's identifiable characteristics. (Krishna et al., 2006) The legislation enumerates names, addresses, identity numbers, date of birth and other dates, and genetic profiles as some of the data items that must be excluded from a data set to de-identify it. HIPAA requires that hospital risk managers, IT directors and others who handle health information, to apply reasonable and appropriate safeguards to protect against disclosure. Unfortunately, HIPAA placed some restrictions on the scope of federal rules. HHS regulates electronic records even though the majority of records are still in paper form. “Covered entities” are the organizations affected by the HIPAA rule, but there are other ancillary entities, such as pharmacies and organizations that help process medical claims that are not subject to it. The early response to this rule was mixed. There were those that believed it provided a good foundation for best practices in providing security for protected health information, but others were not so pleased. Law enforcement personnel were required to get a search warrant, subpoena, or permission from a judge or administrative hearing office to obtain medical records. This was viewed as a significant barrier in some situations, such as getting the mental health history of a person holding others hostage. The American Medical Association (AMA) wanted stronger security restrictions, stating that health plans could use medical information without the patient’s consent for many broadly defined reasons. The insurance industry felt that they were being singled out while some of their business partners were exempt from liability. Under federal rules a Health Maintenance Organization (HMO) could be held liable for a drug store that sold information to a pharmaceutical company. Ten years after HIPAA implementation, in 2006, one hospital administrator acknowledged that HIPAA had certainly increased the focus on patient data security in the hospital setting, but he wasn’t sure if the benefit outweighed the cost in the hospital or nationally. He cited the heavy costs of ongoing training and compliance and the lack of increased efficiency in simplifying the amount of paperwork in healthcare. (Conn, 2006) Currently, application for certification by the Certification Commission for Healthcare Information Technology (CCHIT), using the HITSP standards has become the "gold standard" for acceptance and vendors are rushing to get their products for EMR and ambulatory patients certified

HIPAA provisions for administration simplicity were to "improve the efficiency and effectiveness of the healthcare system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." Section 263 of these provisions requires the National Committee on Vital and Health Statistics (NCVHS) to "study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information" and report to the Secretary of HHS by August 21, 2000 on recommendations and legislative proposals for such standards." (Report to the Secretary of the U.S. Department of Health and Human Services on Uniform Data Standards for Patient Medical Record Information, 2000) The International Standardization Organization, 2700 series provides some of these. (Goedart, 2007)

The ISO 2700 series provided, in part, the best practices of control objectives and controls for security policy, organization of information security, physical and environmental security, access control and information security incident management and compliance

Although HIPAA compliance was originally a main concern for application purchasers from 2000-2004, it is not as much of a concern. The new focus in HIPAA seems to be related to security issues for healthcare networks, such as regional health information organizations (RHIO) (Conn, 2006)

With the improvement in technology, patient records can be moved more rapidly and more freely. Rapid access is a necessity when information from multiple organizations is needed to make healthcare decisions in a short time frame. However, while paper charts containing healthcare information were originally in the hands, and under the protection, of only the patients' physician, electronic data may be handled by, and accessible to, many. The public is concerned that sensitive medical data might be used in a discriminatory manner, such as in hiring practices. Before HHS privacy rules, an employer was able to obtain a prospective employee's entire medical record, perhaps basing employment on conditions or history found. In addition, this fear of disclosure may keep patients from confiding in their physicians, actually compromising their medical care. (Hussong, 2000).

In 2001 an initiative began to build a National Health Information Infrastructure. The objective for this initiative is to make health information available to everyone and necessitates, ideally, having technology available in all communities and to all patients. The principles of the initiative would be used in "making possible the appropriate use of data, information, and knowledge in support of optimal health and quality of life for all Americans. (Information for Health: A Strategy for Building the National Health Information Infrastructure, 2001) As a framework the initiative began with laws and regulations. The Health and Human Services (HHS) regulations on security of health information, and the related privacy and confidentiality, delineating the conditions under which personal health information may be collected, stored and shared, form a good foundation.

In conjunction with the Privacy Rule, the HIPAA Security Rule was promulgated in 2003 and was solicited for comments. The article from the Federal Register stated, "As many commenters (on the HIPAA Security Rule of 2003) recognized, security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information."

(http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf-Accessed 08/29/2008)

HIPAA legislative history until 2006 is as follows

July 13, 1995 Health Insurance Reform Act of 1995 is introduced by Senators Nancy Kassebaum (R-Kan.) and Edward Kennedy (D-Mass.)

March 18, 1996 Health Coverage Availability and Affordability Act of 1996 introduced in House by Rep. Bill Archer (R-Texas)

Aug. 1, 1996 House passes conference report on combined bill, renamed Health Insurance Portability and Accountability Act of 1996, by a 421-2 vote

Aug. 2, 1996 Senate passes conference report on HIPAA on a 98-0 vote

Aug. 21, 1996 President Clinton signs HIPAA into law

Aug. 21, 1999 Deadline passes for Congress to enact separate privacy legislation as specified under HIPAA

Nov. 3, 1999 In absence of congressional action, HHS issues proposed privacy rule in which patient consent is not required for disclosure of protected health information, (PHI)

Aug. 17, 2000 Transactions and code sets final rule implemented

Dec. 28, 2000 Responding to public comments, HHS implements an amended final privacy rule that includes a provision requiring patient consent for most disclosures

April 14, 2001 Privacy rule re-implemented after review by HHS Secretary Tommy Thompson; patient consent requirement is retained

Aug. 14, 2002 HHS implements revised privacy rule replacing patient consent with regulatory permission to disclose PHI without patient permission

April 14, 2003 Privacy rule compliance deadline (except small health plans, which have until April 2004)

Oct. 16, 2003 Transactions and code sets compliance deadline

April 20, 2005 Security rule compliance deadline (except small health plans, which have until April 2006)

Aug. 1, 2005 National employer identifier compliance deadline (except small health plans, which have until August 2006)

Dec. 28, 2006 Security guidance for remote use of, and access to, electronic protected health information

In 2006 the House of Representatives passed a modification of HIPAA originally authorizing the HHS secretary to pre-empt any state privacy laws viewed to be barriers to interoperability. Due to concentrated pressure from a coalition of privacy groups, the pre-emption part of the modification was stripped from the final version of the that bill passed by the House on June 27th., Still remaining in the bill was the requirement that HHS study the variances between the state and federal laws and make recommendations regarding the impact on health information exchange, in addition to making recommendations to Congress about modifying current legislation. The senate had its own version of the bill and both needed to be reconciled. In addition to HIPAA, there has been other legislation that impacts data security.

The USA Patriot Act is one example of how national laws can shape these security concerns. It was signed into law by President George W. bush on October 26th, 2001 and the acronym stands for “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. (Public Law 107-56). Specifically, it increases the ability of law enforcement agencies to search telephone, e-mail communications, medical, financial and other records. It has become very controversial because the public perceives it to be a threat to the security of their private information.

The Graham, Leach, Bliley Act was published in 1999. Sections 6801-6109 cover the protection of nonpublic personal information, addressing privacy policy obligations, obligations with respect to disclosures of personal information and policy enforcement.

The Sarbanes-Oxley Act of 2002, officially the U.S. Public Company Accounting Reform and Investor Protection Act of 2002, (SOX) impacts organizational technology as well as security systems, practices and controls. Although is doesn't spell out what security requirements are needed, effective data security is viewed as one of the primary facets of compliance. Non-compliance could result in a prison sentence for organization executives. SOX section 404 requires that businesses have methods to ensure the security of vital information in the enterprise infrastructure.

In the area of patient safety, the Patient Safety and Quality Improvement Act of 2005 (PSQIA) establishes a voluntary reporting system. This act addresses the assessment and resolution of safety and healthcare issues related to quality issues. PSQIA provides security in the form of Federal privilege and confidentiality protections for patient safety work product. Patient safety work product includes patient, provider and reporter identifying information that is collected, created or used for patient safety activities. If unauthorized disclosures are discovered, civil money penalties (CMPs) may be imposed. Office of Civil Rights (OCR) has been delegated the authority to enforce the security protections of the PSQIA.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §

1232g; 34 CFR Part 99) is a Federal law that addresses security by protecting the privacy of student education records. This act allows parents or eligible students access to student education records for the purpose of inspection and review. Parents may also contest information in these records. Generally, schools must have consent, in the form of written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, under certain conditions.

The E-Government Act (Public Law 107-347) of 2002, addressed information security and its importance related to national economic and security interests. It establishes the Office of Management and Budget (OMB) an office of Electronic Government to set the strategic direction for implementing “electronic Government”. This is to be accomplished by abiding by relevant statutes such as the Privacy Act and Federal Information Security Management Act of 2002 (FISMA). The administrator was to oversee the E-government areas including information security, privacy, access to, and dissemination and preservation of government information.

Title III of the E-Government Act, the Federal Information Security Management Act (FISMA) requires the development and documentation and implementation of agency-wide programs to provide information security for federal information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The Federal Information Processing Standard 140 (FIPS) are series of publications numbered 140 which are U.S. government computer security standards that specify requirements for cryptography modules. The first module, FIPS 140-1, was issued in 1994, while the most recent, FIPS 140-2, was issued in 2005.The scope of the most pertinent of the eleven modules covered by FIPS include:

Roles, services and authentication - (who can do what with the module, and how this is checked)

Physical security - (tamper evidence and resistance, and robustness against extreme environmental conditions)

Cryptographic key management - (generation, entry, output, storage and destruction of keys)

Mitigation of other attacks - (if a module is designed to mitigate against an attack, then its documentation must say how)

Standards

When President Bush in 2004 mandated the development of a national health record by 2014, the disparity of electronic healthcare applications was magnified. Each vendor promoted his own product and, even though scalability and interoperability had increased, there were no national standards to even begin to identify what type or method of security was needed for a national health record.

There are many working groups that are focusing on data standards, data elements, data interchange, and knowledge representation of the EMR and PHR.

Because technology is constantly evolving and often precedes the law, it is necessary to keep abreast of new legislation, new technical standards or developments affecting the security of any new communication method. Often the process of developing standards is so slow that the resulting published efforts are already irrelevant. This has necessitated new classes of standard-setting bodies, the industry consortia, or Standards Setting Organization (SSO). The World Wide Web Consortium (W3C) whose standards for HTML, CSS and XML are internationally accepted, is an example. Large corporations such as Microsoft and Sun Microsystems also develop industry-driven standards, even without a formal organizational structure for standard-setting. (http://en.wikipedia.org/wiki/standards_organization)

Electronic data storage systems have been created in the past few years, often becoming the center for information sought and shared by different groups of users. The “life cycle” of these data can depend on national regulations, but can vary between 20 and 100 years. The same challenges for storing paper data securely can exist with electronic data. They can disappear, lose integrity, or lose the ability to have content read and understood. It is possible that the lifespan of the technology and tools to preserve data may be outlived by the useful lifetime of the data stored.

Security and Research

In the United States, as in Europe, there is sometimes conflict relating to the security of using identifiable healthcare data for research. Legislation relating to data security has had an effect on the type, or feasibility of types, of research being done.

The question arises if the interpretation of the law is focused on protecting the research subjects, so that they come to no harm, or only decreasing the risk that the organization will be more carefully, or frequently, scrutinized. (Davies et al., 2008). For research purposes, all patients should be fully informed about kind of data that will be collected, extracted and possibly transmitted, and the security measures in place to protect it. The risks and benefits of data disclosure relating to security and individual privacy versus the public good should be meticulously examined. (Souhami, 2006) In health care, the collection and storage of sensitive personal data is essential for delivering a high quality clinical service and for research. (Blobel, 2005) Singleton and Wadsworth 2006 believed that there are guidelines that could be nationally promoted to establish a consensus for researchers and the public.

Security Breaches

The existence of policies and legislation that enable the sharing of data between organizations also can increase the chance of security breaches. (BMJ, Dec. 2007) The goal for electronic healthcare is security that will protect patient privacy, in the framework of legal constraints, without impacting efficient operations or the effective management of the system.(Lovis et al., 2007) As technology develops and allows the ability to transfer more medical data access more institutions, so does the potential to have greater chances of security breaches.(Matthews, 2007, BMJ, 2007)

As early as the 1990s, there was the realization that the advent of a shared EMR would increase the possibility of security breaches. As a result of the recommendation by the National Research Council of the United States for the development of policies and technology to combat this, the Role-Based Access Control (RBAC) was added to many off-the-shelf vendor products. But this access security was not often enforced at point-of–care; rather, institutions provided clinicians with very broad-based privileges, stressing instead, the harsh punishments for improper use of, or unauthorized access to, privileged patient data. (Arnoldi et al., 2007). Legislative changes are also a reason for organizations to re-examine their compliance with healthcare data security. One of the changes in legislation was a "notice of breach" law, requiring the potentially affected customers and, under certain circumstances, law enforcement, to be notified when this type of intrusion may have occurred. There have been frequent security breaches in the United States. Seventeen breaches have been reported in 46 hospitals since 2003 (Grey, 2008), perhaps the most publicized being the theft of a laptop that contained over 26 million military records from the Veterans Administration. Following this security incident, certain provisions of Title IX of Public Law 109-461 of the Veterans Benefits, Health Care, and Information Technology Act of 2006 were implemented, addressing procedures to follow in the event of a breach.

Project

The thesis is a cross case analysis of national legislation relating to data security, including articles mentioning national legislation relating to the security of healthcare data during its access, transmission, storage or breach. It will also include standards or standards-making bodies that address data security. The following, commonly cited, twenty-six pieces of legislation were chosen; Common Law of Confidentiality, The Freedom of Information Act of 1966, The Privacy Act of 1974, Federal Education Records Protection Act-FERPA of 1994, Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), Graham-Leach-Bliley Act of 1999, The US Patriot Act of 2001, The Sarbanes -Oxley Act of 2002, The Homeland Security Act of 2002, Federal Information Security Management Act of 2002 (FISMA), Medicare Modernization Act of 2003, Patient Safety and Quality Improvement Act of 2005 (PSQIA), Federal Family Health Information Technology Act of 2006, and The Information Technology Act of 2006, Title IX of Public Law 109-461 of Veteran's Benefits. In addition, five pieces of pending legislation were reviewed. The PRO(TECH)T Act, Health Information Privacy and Security Act, Health Information Technology Act, Independent Health Record Trust Act, and Wired for Healthcare Quality Act.

There were eleven frequently referenced standards, or standard organizations, reviewed: The National Institute of Standards and Technology (NIST), formed in 1901, American National Standards Institute (ANSI), formed in 1918, American Society for Testing and Materials (ASTM) - ASTM E31, formed in 1971, FDA Guidelines-21 CFR Part 11, Logical Observation Identifiers Names and Codes – (LOINC), formed in 1994, Health Level 7 (HL7), formed in 1997,   Certification Commission for Healthcare Information Technology – (CCHIT), formed in 2004, Healthcare Information Technology Standards Panel –Interoperability Standard for Security(HITSP IS 5), formed in 2005, the International Organization for Standardization (ISO) 27000 series of 2005 and the International Electrotechnical Commission (IEC) 27000 series, HIPAA Standards for Privacy of Individually Identifiable Health Information 2000 (Privacy Rule), Federal Information Processing Standards Publication 140-2 0f 2002, HIPAA Security Standard 2005 (Security Rule), and the Payment Card Industry Data Security Standard-PCI DSS of 2006.

Methods

Documents and articles were selected from a multitude of sources, as described below. The majority were from bibliographic databases accessed in Indiana University Medical Library and interlibrary requests. Articles were selected online from OVID, Cinahl, Medline, and PubMed by using keywords data security, clinical information systems, data integration, data standards, data breach, and healthcare data legislation. Also used are copies of national legislation that mandate certain security measures related to healthcare data and any standards addressing the same measures. In addition, current newspaper articles, legal and data security blogs, and individual interviews were also reviewed. Only those articles with abstracts in English were selected.

167 articles were originally selected, related to national legislation and standards addressing healthcare data security. Relevant articles were legislation or standards that included specific data security measures, or articles discussing

healthcare data security measures, or the standard-making bodies or legislation responsible for making them. Governmental legislative documents and standards from the Federal Register were also used. Thirty-seven documents addressing national data security legislation and standards or standards-making organizations from 1890 until the present were ultimately selected, based on content containing terminology and/or measures relating to data security. A database was created with Microsoft Access (see Appendix A), including the main table with text fields; document name, document date, document type, document content, the notation of the selected words in the document, and any miscellaneous notes.

The initial word selection was done manually, choosing the words in each document for lexical mapping only. There were 14 words selected; access, privacy, security, confidentiality, communication, interoperability, architecture, transmission, storage, certification, policies, breach, consent and audit. By definition, transmission and communication are synonymous. Each document was read and lexical mapping completed for each word.

The text management and coding program, Atlas.ti, by Scientific Software Development of Berlin, Germany, was used to automatically to choose and calculate the frequency of security-related words in the 37 primary documents and to relate chosen word/codes to selected quotations from these documents. This application was chosen because of its ability to rapidly calculate word frequencies in multiple documents, to select quotations and codes related to each document, assign relationships to those codes, and create reports relating to the codes and the quotations containing them. The same documents used in the database were loaded as primary documents and the Word Cruncher attribute of the application used to find the frequency of all repeated words, and their related forms, (e.g. access, accessing, accessed) in each document, as well as the total number of separate documents in which the word was found. A total of 8947 words were initially found. (See Appendix B) A list of 328 words was made containing any words that were related to data security or data security measures. This list was reduced to 165 words that were related to data security and found more frequently in the documents and these 165 consolidated into 68 by combining the derivatives of each word into only one. These 68 were again reduced to 35 of the word/codes found in the greatest amount of separate documents. (See Appendix D) Only the 23 word/codes found in close to 25% of the 37 separate documents were chosen for the final list. The ones not used were either not reflective of a data security measure, such as interoperable, or not as evenly distributed before and after HIPAA, each of these words found primarily in the post-HIPAA years. These final words were entered as codes in Atlas.ti, based on the number of separate documents in which they were found. These include the word/codes: Act, access, audit, authorize, breach, communicate, confidential, consent, disclose, enforce, HIPAA, identify, law, penalty, policy, private, procedure, risk, secure, standard, store, threat, and unauthorized. 78% of the manually chosen words were also in the list developed by frequency in Atlas.ti. The Atlas.ti word/codes were validated by first numbering the primary 37 documents in the manual database from 1 to 37. Ten of the document numbers were randomly chosen by an independent rater to compare the manually chosen words in each document with those selected by Atlas.ti. 80% of the manually chosen words in the documents were also found in the Atlas.ti word/code frequency calculations.

Definitions of these word/codes, related to data security, were taken from their primary documents or, if there was no definition in any of the documents, the online version of the Merriam-Webster Dictionary.(See Definitions).

The Altas.ti method of cross-case analysis, while effectively allowing the calculation of word/code frequency, also involved the personal discretion of the investigator in choosing quotations from each entire primary document. Word/code presence was determined by the defined word/code, its derivative, synonyms, or concepts located anywhere in the document.

The final 23 words/codes were again located in each document in which they appeared, to confirm they were used in a context conforming to the given definition. Synonyms were also taken from the documents or the online version of the Merriam-Webster Dictionary. The codes authorized and unauthorized were combined because there were only two documents in which the word/code unauthorized was found that didn’t also include the word/code authorized. The word/code identify was removed because its definition in all the documents did not refer to any form of data security. This left the final list with 21 word/codes. The total 37 documents used in the final selection were divided into two subgroups; the years prior to the HIPAA enactment of 1996, and those following it. The frequency of the word/codes for these subgroups was calculated and compared to the total document list.

To contextually validate the Atlas.ti word/code list, two independent raters were given the list of word/codes, with definitions and synonyms. They were also given the quotations, selected from the primary documents, containing these word/codes. Raters were then were asked to read all the selected quotations and determine if the word/codes found in them conformed to the definitions, concepts or synonyms. Rater one validated 99.6% of the 642 instances of word/codes and definitions in the quotations, and rater two also validated 99.6%. Each rater disagreed with two of the word/codes in separate quotations, but they were different word/codes. Rater one disagreed with the use of the word/codes "privacy" and "security" in a quote from the HIMSS Interoperability Standards, while rater two agreed with the usage. They were unable to reach a consensus on these word/codes. Rater two disagreed with the word/code "access" in a quotation from the Homeland Security Act of 2002 and the Privacy Act of 1974, while rater one agreed with its usage. They were able to reach consensus on the quotation from the Privacy Act of 1974, agreeing that the word/code "access" did match the definition, but were unable to reach consensus with its use in the quotation from the Homeland Security Act of 2002. The resulting frequency data, documenting validated word/code frequency totals for separate documents, were graphed by year. These frequencies were graphed for the total list of 37 documents, as well as pre and post HIPAA (1996) documents.

Barriers

Legislation containing provisions or measures relating to data security was often written as a guideline, containing general terminology, and without specific requirements, so it was difficult to do an exact comparison of word/codes between all of the documents selected. The word/codes are a combination of general terms and specific ones. There were definitions of the word/codes included in some of the documents that facilitated the comparison between documents, such as “confidentiality”, but others, like “risk” and “standard”, more general in nature, had to be selected form the online Merriam Webster Dictionary with definitions related to data security chosen. The assignment of word/codes was made by assigning the word definition itself, the synonym, or the concept reflecting the definition, to a selected quotation. Some of the word/codes describe specific measures to be taken to enhance data security, while others are broader in nature, as are the laws and standards in which they are used. Using a combination of these kinds of terms may not be the best way to look at specific measures to ensure data security, but was able to be compared and measured.

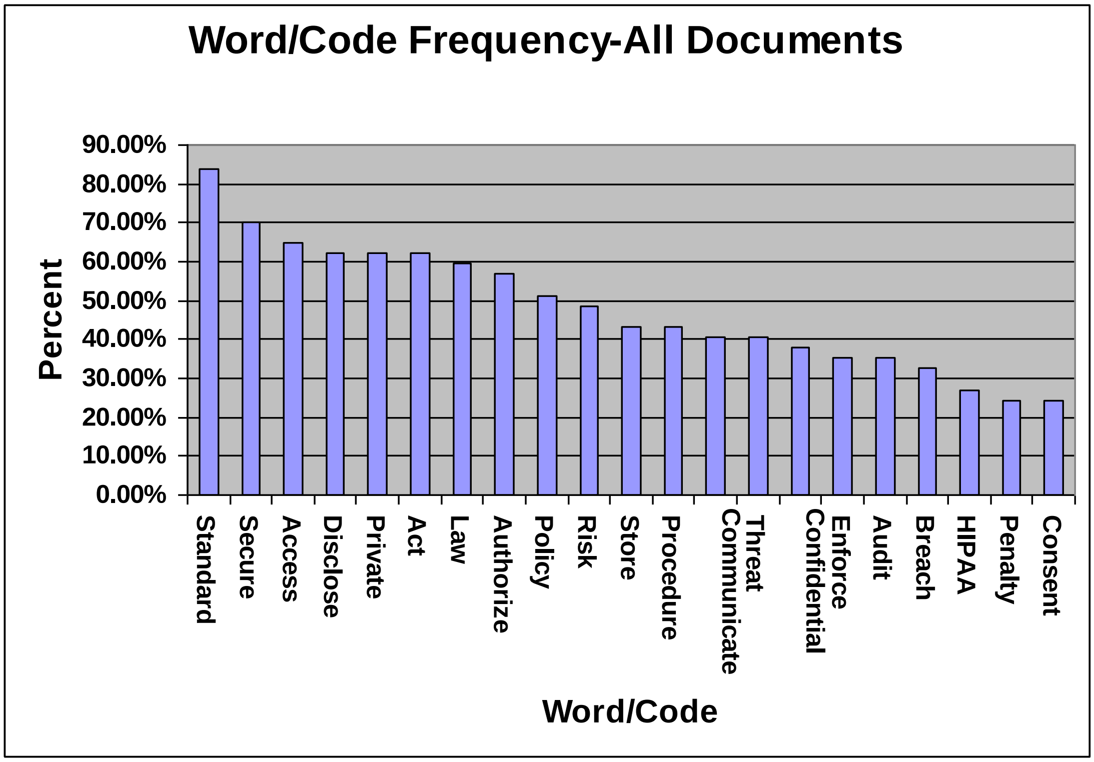
Analysis

The Atlas.ti cross-case frequency analysis was automatically calculated by the application and word/code presence in each document validated by two independent raters. Prior to the enactment of HIPAA, 1996, eleven documents were examined that addressed either standards or legislation. These years were 1890, 1901, 1918, 1966, 1971, 1974, 1987, and 1994. The earlier years, 1890 and 1918, reflect the mention of patient confidentiality and breach of that confidence as well as the establishment of standards-making organizations, but only mention a total of 8 of the selected word/codes. There were only two years prior to the enactment, 1987 and 1994, that mentioned more than 10 of the 21 code/words, and only 1994, when they were mentioned in more than one document. The average amount of word/codes per documents, prior to 1996, was 3.62. Out of a total of 231 possible word/codes, there were 66 used (28.57%). From of 1996 on, the year HIPAA enactment, there were 26 documents that mentioned data security measures, in 1996, 1997, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008. All but one of these years, 1997, mentioned more than 10 of the word/codes in the documents, and 7 of the years, 1996, 2001, 2002, 2003, 2005, 2006, and 2007, had more than one document in the year. The majority of the legislation listed for 2007 and 2008 is still pending. The average amount of word/codes per document, post-HIPAA was 14.52. Out of a possible 546 word/codes, there were 204 used (37.36%), a slight increase.

The overall frequency of the word/codes within a document was not used as a measurement because it could have been a result of the document length, and not have been indicative of its relevance. Instead, relevance was determined by the number of separate documents in which each word/code was found. The word/code in the total list of documents that was most frequently found in multiple documents was “standard”, appearing in 83.78% of the documents (31). The word/code “secure”, and its derivatives, in (70.27) of the documents (37). The remaining word/codes, in order of their frequency, are “access”(64.86%) “disclose”, “private”, and “Act” (62.16%), “law” (59.46%), “authorize” (56.76%), and “policy”(51.35%), “risk”(48.65), “store” and “procedure” (43.24%), “communicate” and “threat”(40.54%), “confidential”(37.84%), “enforce” and “audit” (35.14%), breach”(32.43) “HIPAA”(27.03%), “penalty” and “consent” (24.32%). Other word/codes were initially chosen for frequency in the documents, but not included in the final calculations because they appeared in less than ten documents. Ten of the 21 word/codes were found in more than half of the total documents. (See Table 1)

Table 1

Frequency in All Documents (37)		
Standard	31	83.78%
Secure	26	70.27%
Access	24	64.86%
Disclose	23	62.16%
Private	23	62.16%
Act	23	62.16%
Law	22	59.46%
Authorize	21	56.76%
Policy	19	51.35%
Risk	18	48.65%
Store	16	43.24%
Procedure	16	43.24%
Communicate	15	40.54%
Threat	15	40.54%
Confidential	14	37.84%
Enforce	13	35.14%
Audit	13	35.14%
Breach	12	32.43%
HIPAA	10	27.03%
Penalty	9	24.32%
Consent	9	24.32%
Interoperable		
Integrity		
Attack		
Firewall		
Authenticate		
Trail		
Signature		
Consortia		
Password		
Biometric		
Alert		
Other Laws <4		
Encrypt		
Decrypt		



There was a change noted in ranks when the documents were subdivided into those prior to 1996 and those after 1995. Although the word/code "standard" remained the greatest in frequency in both subgroups, it was found in 72.73% of the documents prior to 1996 and in 88.46% afterward, an increase of 15.73%. The related code/words "Act" was ranked 4th, in 45.45%, prior to 1996 and 3rd, in 69.23% afterward, an increase of 23.78%. "Law", 4th in 45.45%, and 4th in 65.38% an increase of 19.93%. The word/code "private" ranked 2nd in 63.64%, prior to 1996, but ranked 5th, in 61.54% after HIPAA was enacted, a decrease of 2.1%. The word/code "secure", often linked with the word "private", was ranked 5th, in 36.36%, prior to 1996 and 2nd, in 84.62% afterward, an increase of 48.26%. The word/code “confidential”, also related to the previous two, was ranked 8th, in 27.27% prior to 1996, and 9th afterward, but in 42.31%, an increase of 15.04%. The word/codes “enforcement” and “penalty” are related, as the enforcement of legislation usually imposes a penalty on those who do not comply with it. “Enforce” was ranked in 7th, in 18.18% prior to 1996, and ranked 9th, in 42.31% afterward, an increase of 24.13%, while “penalty”, not found in any of the chosen documents prior to 1996, was ranked 10th and found in 34.62% of the documents afterward. The word/codes ‘breach”, “threat”, “audit’ and ‘risk” are related. Threat usually implies there is a risk, or chance, of unauthorized access to confidential healthcare data and an audit is a method to determine if this has occurred. Of these, “breach” was ranked highest, at 9th, in 9.09% prior to 1996 and 9th, also in 42.31% of the documents afterward, an increase of 33.22%.”Threat” was next in rank for both categories; ranked 7th, in 18.18% prior to 1996, and ranked 7th, but in 50% of the documents afterward, a 31.82% increase. “Audit” was ranked next, at 7th, in 18.18% prior to 1996 and ranked 9th, in 42.31% afterward, a 24.13% increase. “Risk” was ranked 6th and in 27.27% prior to 1996, and ranked 5h, but in 61.54% afterward, an increase of 34.27%. The word/codes “policy” and “procedure” are related, each describing by what documented methods data security is to be accomplished. “Policy” is ranked 5th, in 36.36% prior to 1996 and ranked 6th, in 57.69% afterward, an increase in 21.33%. “Procedure” is ranked 6th, in 27.27 % prior to 1996 and ranked 7th, but in 50% of the documents afterward, an increase of 22.73%. The word/codes “consent”, “disclose” and “access” and “authorization” are related because in order to disclose protected healthcare data, one must receive consent or authorization for access. “Consent” was ranked 7th, in 18.18% of the documents prior to 1996, and ranked 11th, in 26.92% afterward, an increase of 8.74%. “Disclose” was ranked 3rd , in 54.55% of the documents prior to 1996, and 4th, in 65.38% afterward, an increase of 10.83%. “Access” was also ranked 3rd, in 54.55% prior to 1996 and also 3rd , in 69.23% afterward, an increase of 14.68%. “Authorization” was ranked 5th, in 36.36% prior to 1996, and ranked 4th, in 65.38% of the documents afterward, an increase of 29.02% The word/code “store”, referring to security measures needed when personal healthcare data is in storage, is ranked 4th , in 45.45% of the documents prior to 1996, and ranked 9th, in 42.31% afterward, a decrease of 3.14%. The word/code HIPAA was included even though it did not define a specific data security term, but because, in terms of frequency, it was found in more than ten documents. “HIPAA” was ranked 9th, in 9.09% of the documents, even before it was enacted, and ranked 10th, in 34.62% of the documents, after its enactment, an increase of 25.53%. The word/code “security”, as previously stated, had the greatest increase after HIPAA enactment, and often is used in conjunction with “privacy”. Privacy and confidentiality are sometimes used synonymously.

The amount of total documents found discussing data security prior to 1996 was 11, compared to the 26 found after HIPAA enactment. (See Table 4)

The frequency of all of the 21 word/codes increased after HIPAA enactment, the greatest, at 48.26%, for the word/code “secure” and its derivatives. “Penalty”(34.62%), “risk”(34.27%), “breach”(33.22%), “authorize”(29.02%), and “threat”(31.82%), all increased greater than 30%, “Act”(23.78%), "HIPAA”(25.53%), “enforce”(24.13%), “audit”(24.13%), “procedure”(22.73%) and “policy”(21.33%), increased greater than 20%. “Law” (19.93%) “communicate”(18.88%), “standard”(15.73%), “confidential”(15.04%) while “access”(14.68%), and “disclose”(10.83%), increased between 10% and 20%. “Consent”(8.74%), had the least increase, between 0% and 10%, while “private” (-2.1%) and “store”(-3.14%) were the only word/codes to decrease.

Table 2- Frequency Pre-HIPAA

Word/Code	Pre-Rank	Docs (11)	%
Standard	1	8	72.73%
Private	2	7	63.64%
Disclose	3	6	54.55%
Access	3	6	54.55%
Law	4	5	45.45%
Act	4	5	45.45%
Store	4	5	45.45%
Secure	5	4	36.36%
Authorize	5	4	36.36%
Policy	5	4	36.36%
Risk	6	3	27.27%
Procedure	6	3	27.27%
Communicate	6	3	27.27%
Threat	7	2	18.18%
Enforce	7	2	18.18%
Audit	7	2	18.18%
Consent	7	2	18.18%
Confidential	8	1	27.27%
HIPAA	9	1	9.09%
Breach	9	1	9.09%
Penalty	10	0	0.00%

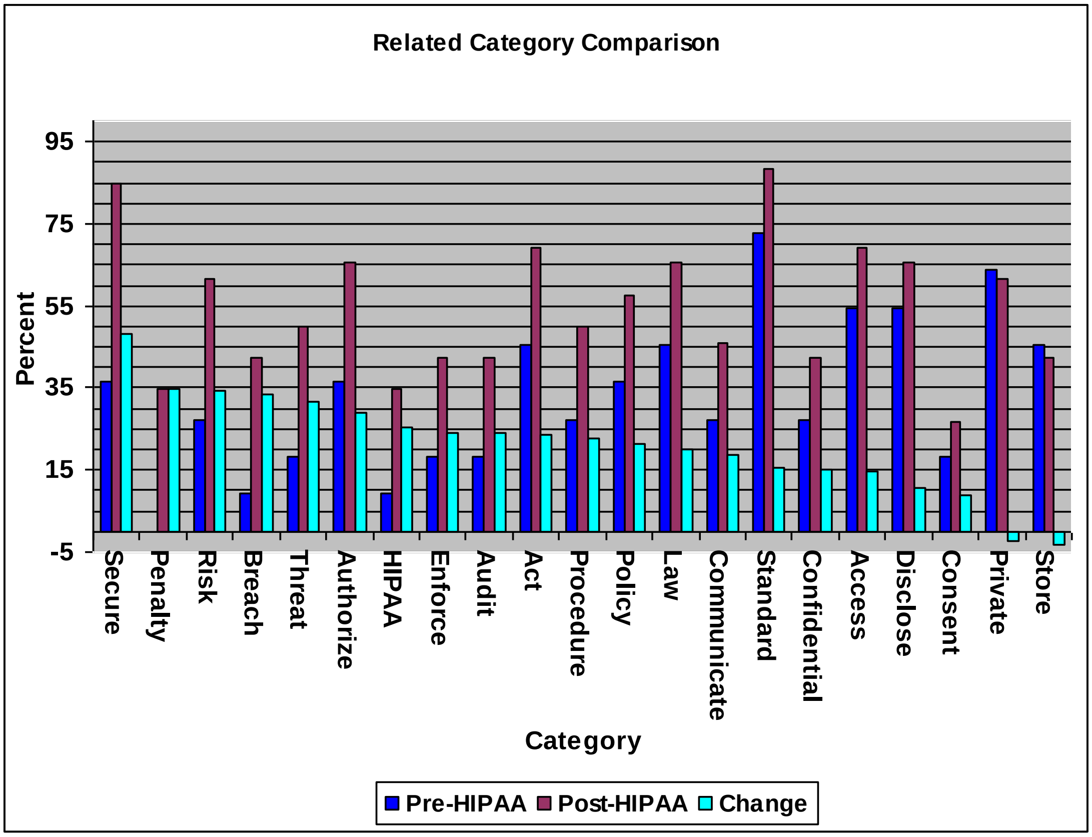
Table 3 – Frequency Post-HIPAA

Word/Code	Post- Rank	Docs (26)	%
Standard	1	23	88.46%
Secure	2	22	84.62%
Act	3	18	69.23%
Access	3	18	69.23%
Authorize	4	17	65.38%
Disclose	4	17	65.38%
Law	4	17	65.38%
Private	5	16	61.54%
Risk	5	16	61.54%
Policy	6	15	57.69%
Procedure	7	13	50.00%
Threat	7	13	50.00%
Communicate	8	12	46.15%
Store	9	11	42.31%
Enforce	9	11	42.31%
Audit	9	11	42.31%
Breach	9	11	42.31%
Confidential	9	11	42.31%
Penalty	10	9	34.62%
HIPAA	10	9	34.62%
Consent	11	7	26.92%

Table 4 - Percentage of Change in Word/Codes in Documents

Word/Code	Pre HIPAA	Post HIPAA	Change
Secure	36.36	84.62	48.26
Penalty	0	34.62	34.62
Risk	27.27	61.54	34.27
Breach	9.09	42.31	33.22
Threat	18.18	50	31.82
Authorize	36.36	65.38	29.02
HIPAA	9.09	34.62	25.53
Enforce	18.18	42.31	24.13
Audit	18.18	42.31	24.13
Act	45.45	69.23	23.78
Procedure	27.27	50	22.73
Policy	36.36	57.69	21.33
Law	45.45	65.38	19.93
Communicate	27.27	46.15	18.88
Standard	72.73	88.46	15.73
Confidential	27.27	42.31	15.04
Access	54.55	69.23	14.68
Disclose	54.55	65.38	10.83
Consent	18.18	26.92	8.74
Private	63.64	61.54	-2.1
Store	45.45	42.31	-3.14

Table 5



Related Category Comparison
Percent
95
75
55
35
15
-5
Secure
Penalty
Risk
Breach
Threat
Authorize
HIPAA
Enforce
Audit
Act
Procedure
Policy
Law
Communicate
Standard
Confidential
Access
Disclose
Consent
Private
Store
Category
Pre-HIPAA
Post-HIPAA
Change

Conclusion

The expectation of the study was that the exponential increase in technology, including multiple formats and devices that access and transmit electronic healthcare data since 1996, would necessitate an increase in the numbers of data security measures needed for protection. There was also the expectation that there would be an increase in the many terms and their frequency in documents that relate to data security, and that they would be found, in greater numbers, in more than one standard or piece of legislation. This cross case analysis of related legislation and standards and word/code frequencies has borne out at least part this expectation. The number of documents and the frequency of data security word/codes in them have increased an average of 19.5% since HIPAA enactment.

The word/codes were divided into the related categories of legislation (Act, standard, law, HIPAA), access to information(access, consent, authorize, disclose), breach of the security system, (breach, audit, threat, risk), enforcement of legislation, (enforce, penalty) the sharing of data (communication) the security of the data, (store, secure, private, confidentiality), written ways to establish and/or maintain security (policy and procedure), and the increases averaged in each subgroup.

The average of each group of related categories was calculated based on the percentage of pre-HIPAA and post-HIPAA documents in which they are included. The related category that has the highest percentage in pre-HIPAA is the one related to legislation; “Act”, “law”, “standard” and “HIPAA” at 43.18%. Those word/codes related to security; “store”, “secure”, “private” and “confidential” in an average of 43.18% of these documents. The word/codes related to access; “access”, “consent”, “authorize” and “disclose” are present in 40.91%. “Policy” and “procedure”, relating to documents providing details for data security, are in 31.82% of all documents, while the word/code “communicate”, relating to data transmission is in 27.27%.

In contrast, if the average of the related categories is calculated based on the post-HIPAA documents, the largest percentage of increase is in the group also related to legislation at 64.42%. Next highest is the group related to access at 56.73% The group related to policy and procedures (methods) is next at 55.77%, followed by breach (48.97%, communication (46.15%, enforcement(38.47% and security(14.52%) (See Tables 6-9)

The related categories with the highest percentage both pre and post-HIPAA documents are those of laws, access and security. However, the categories which showed the highest percentage increase from pre-HIPAA documents to post-HIPAA documents are those related to breach and enforcement; “breach”, “audit”, “threat”, “risk”, “enforce” and “penalty”.(See Tables 10-12). The more relevant of the two, is the amount of change between pre and post-HIPAA documents because it denotes the change over the years and, perhaps, the focus of the future.

Table 6- Post-HIPAA Related Categories

Act	69.23
Standard	88.46
HIPAA	34.62
Law	65.38
LAWS	**64.4225**
Access	65.38
Consent	26.92
Authorize	69.23
Disclose	65.38
ACCESS	**56.7275**
Breach	42.31
Audit	42.31
Threat	50
Risk	57.69
BREACH	**48.0775**
Enforce	42.31
Penalty	34.62
ENFORCEMENT	**38.465**
Store	42.31
Secure	84.62
Private	61.54
Confidential	42.31
SECURITY	**57.695**
Communicate	46.15
COMMUNICATION	**46.15**
Policy	61.54
Procedure	50
METHODS	**55.77**

Table 7 Post-HIPAA

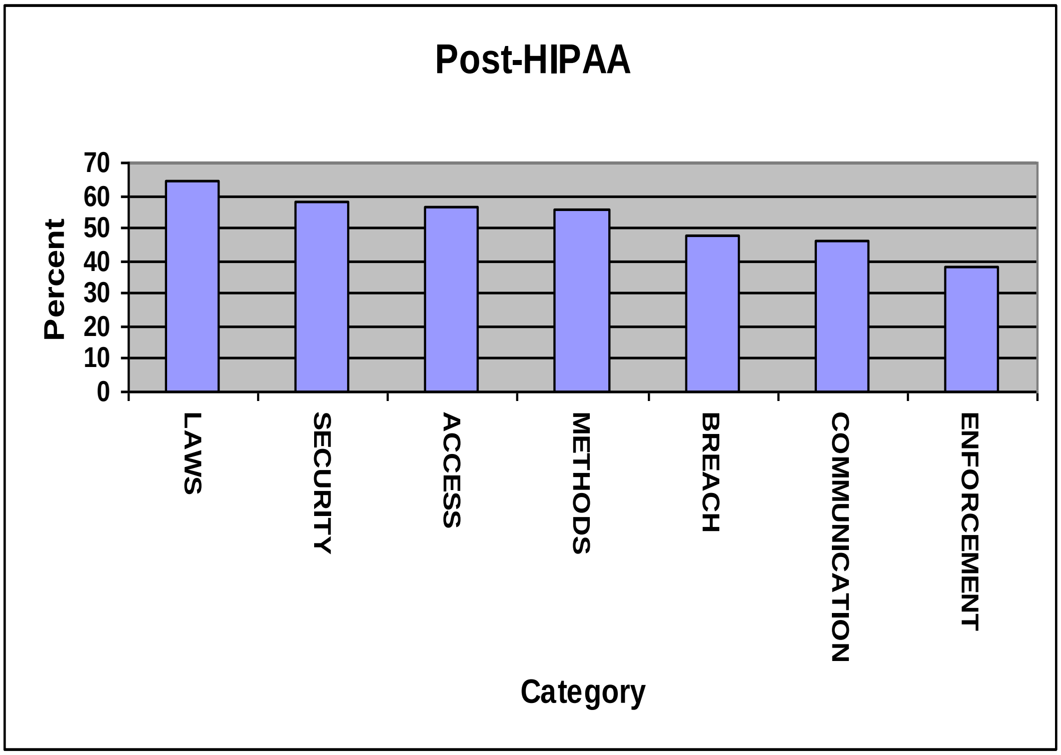


Table 8 – Pre-HIPAA Related Categories

Pre-HIPAA	
Law	**45.45**
HIPAA	**9.09**
Act	**45.45**
Standard	**72.73**
LAWS	**43.18**
Access	**54.55**
Consent	**18.18**
authorize	**36.36**
Disclose	**54.55**
ACCESS	**40.91**
Breach	**9.09**
Audit	**18.18**
Threat	**18.18**
Risk	**27.27**
BREACH	**18.18**
Enforce	**18.18**
Penalty	**0.00**
ENFORCEMENT	**9.09**
Store	**45.45**
Secure	**36.36**
Private	**63.64**
Confidential	**27.27**
SECURITY	**43.18**
COMMUNICATION	**27.27**
Policy	**36.36**
Procedure	**27.27**
METHODS	**31.82**

Table 9 – Pre-HIPAA

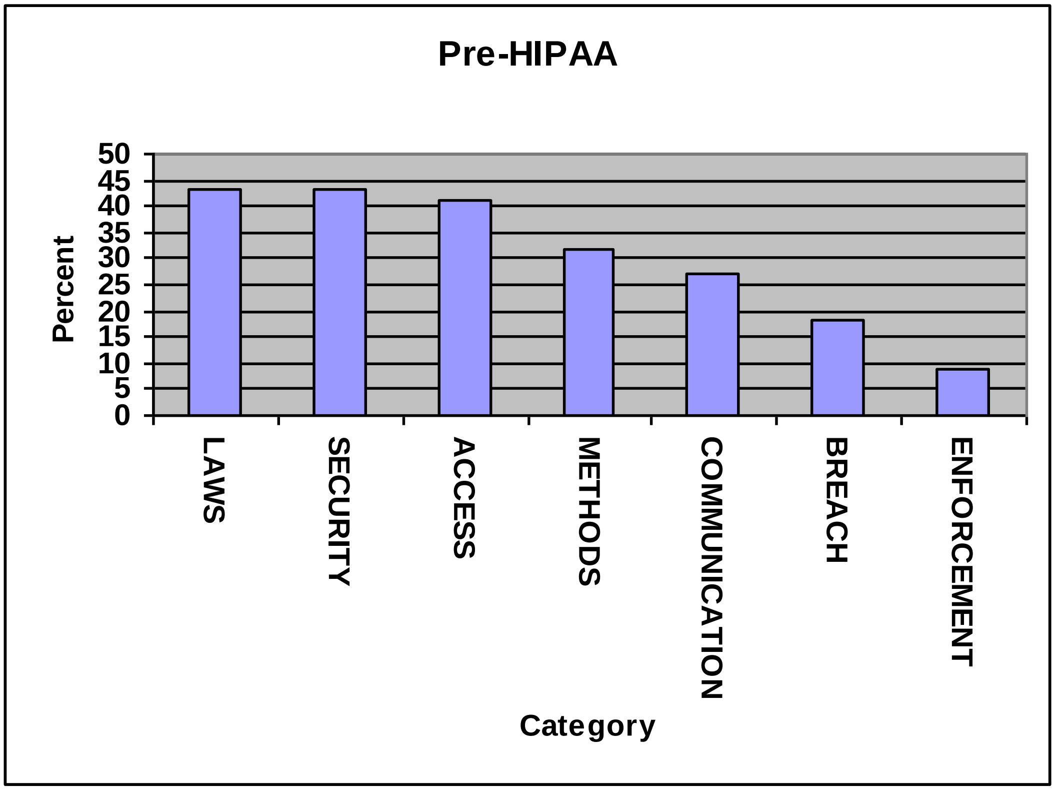


Table 10 – Comparison of Related Categories

Pre-HIPAA

Legislation	43.18%
Security	43.18%
Access	40.09%
Methods	31.82%
Communicate	27.27%
Breach	18.18%
Enforcement	9.09%

Post-HIPAA

Legislation	64.42%
Security	57.70%
Access	56.73%
Methods	55.77%
Breach	48.08%
Communicate	46.15%
Enforcement	38.47%

Table 11 – Related Average Comparison

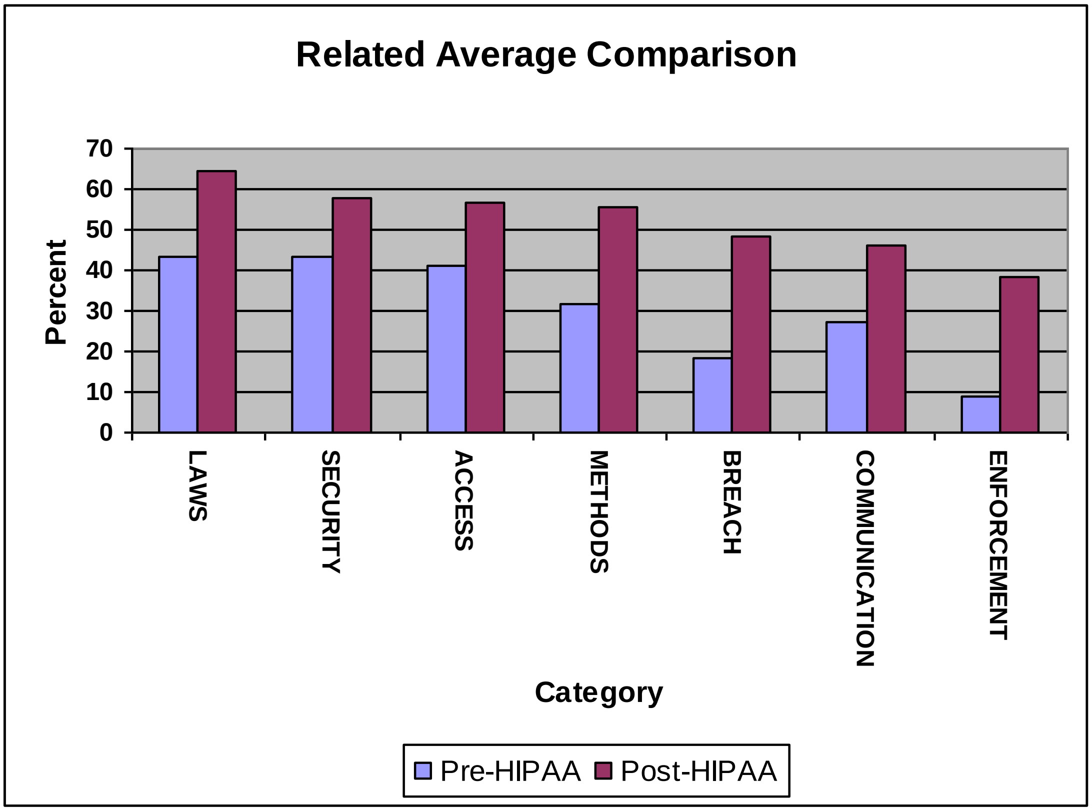
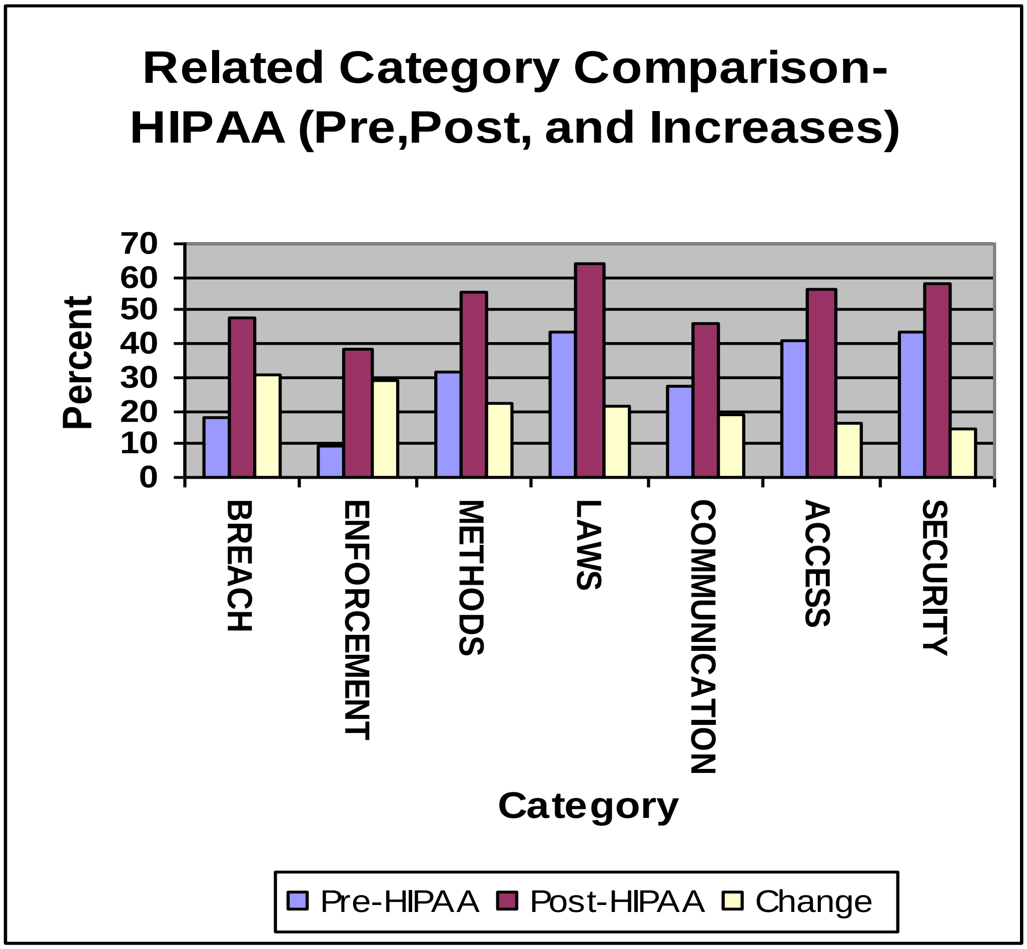


Table 12 Related Categories by Increase Percentage

Related Categories by Increase	
Law	19.93
Standard	15.73
Act	23.78
HIPAA	25.53
LAWS	**21.24**
Access	14.68
Consent	8.74
Disclose	10.83
Authorize	29.02
ACCESS	**15.82**
Breach	33.22
Threat	31.82
Audit	24.13
Risk	34.27
Breach	**30.86**
Enforce	24.13
Penalty	34.62
ENFORCEMENT	**29.38**
Confidential	15.04
Private	-2.1
Secure	48.26
Store	-3.14
SECURITY	**14.52**
COMMUNICATION	**18.88**
Policy	21.33
Procedure	22.73
METHODS	**22.03**



Related Category Comparison-HIPAA (Pre,Post, and Increases)

Category	Pre	Post	Change
BREACH	40.91	48.08	30.86
ENFORCEMENT	31.82	38.47	29.38
METHODS	9.09	55.77	22.03
LAWS	43.18	64.42	21.25
COMMUNICATION	27.27	46.15	18.88
ACCESS	43.18	56.73	15.82
SECURITY	18.18	57.7	14.16

Results

The results from this cross-case analysis show, based on the selection of word/codes, that most of the emphasis since the HIPAA enactment, if comparing the related categories based on the percentage of increase from pre to post-HIPAA documents, is toward preventing breaches of information systems collecting, carrying, or storing protected healthcare information, and the enforcement of penalties in case of breach or non-compliance with legislation. There is not as much emphasis on specific measures or ways to achieve data security. The category related to legislation is first in the calculation of both pre and post-HIPAA documents, but in the middle of the seven categories if calculating related groups based on increases. Even though some of the pieces of legislation chosen for review have not be enacted into law, and the new standardization methods have not been made mandatory, the trend toward standardization of content format continues, as shown by the organizations creating vendor standards, such as CCHIT, and those creating interoperability standards, such as HITSP. The governmental mandate toward the conversion to electronic patient health records in 2014 will drive more global increases in the sharing of information. There is already some global standardization related to sharing of healthcare data with the use of HL7 messaging and SNOMED CT clinical terminology. The effort toward continued standardization and interoperability may include international legislation to provide secure access, collection, storage, and transmission of healthcare data.

Future Studies

Using the analyses of these pieces of legislation as a basis, it would be interesting to see exactly what security measures or standards are contained in pending or future legislation, and if the focus is still on the prevention and identification of breaches in information systems. The number of breaches and the type of information illegally disclosed could help to direct methods of protection to certain areas of the systems that share information. It would also be interesting to monitor the enforcement of legislation and convictions or penalties meted out as a result of non-compliance.

After the enactment of HIPAA, many of the data security measures were removed from the more global pieces of legislation to more specific information technology (IT) standards. Analyzing these IT-specific standards relating to data security might be a more comprehensive study for the future.

Data security legislation or standards that include all entities and data content would need to be put in place to regulate collection, usage, communication and storage in every device, medium and format. HIPAA laid the foundation, even with the narrow focus of "covered entities". The security predicament arises when the government is given the power to collect and use personal data. Esther Dyson, in Reflections on Privacy 2.0, in *Scientific American*, September 2008, believes that this governmental power should be limited. This balance between the right to security as privacy, and the right to access personal information, will continue to be an issue.

Jodi Daniel, J.D., M.P.H. Director of the Office of Policy and Research from the Office of the National Coordinator for Health Information Technology (U.S. Department of Health and Human Services) believes there will need to be a combined policy approach for control of healthcare data between the consumer and data users, in addition to combined approach for security. The United States defines protections by the entity holding the data, while the European Union defines protection in terms of the type of data held.

In her opinion, the Federal Government has several options to address this issue: providing accreditation and/or certification for healthcare applications, providing incentives or disincentives for compliance, publishing legislation, imposing regulations and adopt policies in programs. Future programs could then either revisit prior polices or consider new issues arising. Future studies might include monitoring these five areas to determine if there is a trend. Because the issue of data security breaches seems to be of increasing importance, a study monitoring future breaches; their location, type, frequency and/or direct or indirect resulting damage, would be interesting.

Appendix A – Microsoft Database-L(legislation) St(standard)

DocName	Date	Type	Content	Notes
Common Law of Confidentiality	1890	L	A legal system derived from the broad and comprehensive principles encompassed within the unwritten laws of England and applied in most English-speaking countries, including the United States (except the state of Louisiana).	When there is no authoritative statement of the law, judges have the authority and duty to make law by creating precedent-The tort of breach of confidence, is a common law tort that protects private information that is conveyed in confidence.
National Institute of Standards and Technology (NIST)	1901	St	to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.	
American National Standards Institute (ANSI)	1918	St	The American National Standards Institute (ANSI) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 90 years	
Freedom of Information Act and Amendments	1966	L	and guaranteed the public the right of access to information held by the federal government	Privacy Act of 1974 enhances the FOIA by permitting individuals access to records about themselves, which are held by federal agencies
American Society for Testing and	1971	St	int'l standards related to the architecture, content, storage, security, confidentiality,	

Materials (ASTM) - ASTM E31			functionality, and communication of information used within healthcare and healthcare decision making	
Privacy Act of 1974	1974	L	code of fair information practices- regulate the collection, maintenance, use, dissemination of personal information by federal executive branch agencies.	balance need to maintain information rights of individuals t protected against unwarranted invasions of their privacy-
Computer Security Act of 1987	1987	L	assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems	for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems
Federal Information Processing Standard 140-2 (FIPS)	1994	L	coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government	
Federal Education Records Protection Act-FERPA	1994	L	This law creates a minimum standard for the protection of records which may be increased by either state or local law or regulations. The FERPA, FOIA and Privacy Acts do not differentiate between the medium of storage or the method of transmission	
World Wide Web Consortium	1994	St	international consortium where member organizations, a full-time staff, and the public work	

(W3C)			together to develop Web standards.	
Logical Observation Identifiers Names and Codes-LOINC	1994	St	facilitate the exchange and pooling of clinical results for clinical care, outcomes management, and research by providing a set of universal codes and names to identify laboratory and other clinical observations.	Regenstrief Institute-LOINC codes are universal identifiers for laboratory and other clinical observations that solve this problem
Health Insurance Portability and Accountability Act- HIPAA	1996	L	electronic transmission standards for claims data-regulating privacy of electronic medical records and the security of medical data storage and transmission.-standards for unique health identifiers	at a time when provider organizations demand the cost savings and convenience of patient record automation, HIPAA demands multiple levels of responsibility and accountability for those electronic records.
Standards of Good Practice for Information Security	1996	St	detailed documentation of best practice for information security	used as the default governing document for information security behavior by many major organizations, by itself or in conjunction with other standards such as ISO/IEC 27002 or COBIT.
Health Level 7 (HL7)	1997	St	defining application messages, but are based on formal models	
Graham-Leach-Bliley Act - 1999	1999	L	the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third	

			parties, other than agents of the institution	
HIPAA Privacy Rule	2000	St	provide patients with access to their medical records and more control over how their personal health information is used and disclosed.	mandated in HIPAA
US Patriot Act	2001	L	the expanded use of National Security Letters, which allows the FBI to search telephone, email and financial records without a court order; and the expanded access of law enforcement agencies to business records, including library and financial records.	
HIMSS Interoperability Standards	2001	St	provide a business analysis and management perspective on interoperability standards. Each issue examines one or more key standards initiatives in terms of impact on healthcare information technology (HCIT) and healthcare in general.	As HCIT increasingly becomes the focus of policy makers' intent on improving patient safety, clinical outcomes and cost effectiveness, interoperability becomes a critical factor.
Sarbanes -Oxley Act	2002	L	section 404 requires that businesses have methods to ensure protection of vital information in the enterprise infrastructure. This requires and internal control report.	doesn't spell out what security requirements are needed, security is viewed as one of the primary facets of compliance.
Homeland Security Act	2002	L	sweeping anti-terrorism law giving federal law enforcement agencies broad powers to look over citizens and thwart potential attacks on the homeland.	

Federal Information Security Management Act (FISMA)	2002	L	provide information security for the information and information systems –including those provided or managed by another agency, contractor, or other source.	Title III of the E-Government Act,- risk based policy for cost effective security
E-Government Act of 2002	2002	L	Establishes in the Office of Management and Budget (OMB) an Office of Electronic Government	provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
Medicare Modernization Act - 2003	2003	L	Section 1860D-4(e)(2) also imposes limitations on the disclosure of personal health information as it relates to this program.	information shall only be disclosed if the disclosure is permitted under Federal regulations concerning the privacy of individually identifiable health information promulgated under section 264(c) of HIPAA.
FDA Title 21CFR-Part 11	2003	L	regulation of electronic records and signatures-FDA will enforce limiting system access to authorized individuals, establishment and adherence to written policies	hold individuals accountable for written signatures-enforcement discretion for audit trails
HIPAA Final Security Rule	2003	L	adopts standards for the security of electronic protected health information to be implemented covered entities	

HIMSS Medical Device Workgroup	2004	St	integration and interconnection of disparate medical (and information) technology devices and systems where medical data exchanged.-Identify both the security issues-best practices available-vulnerabilities	Evaluate the issues of security threats -Coordinate with similar groups and committees
Certification Commission for Healthcare Information Technology - CCHIT	2004	St	provide strategic guidance on the development of PHR certification and the maturity of the market.	certification requirements are based on widely accepted industry standards
Patient Safety and Quality Improvement Act of 2005 (PSQIA)	2005	L	voluntary reporting system to enhance the data available to assess and resolve patient safety and health care quality issues.-improve patient safety and reduce the incidence of events that adversely affect patient safety.	OCR has been delegated the authority to enforce the confidentiality protections of the PSQIA.
Healthcare Information Technology Standards Panel - HITSP	2005	St	assist with NHIN-harmonize and recommend the technical standards necessary to assure the interoperability of electronic health records.	harmonize & recommend technical standards, (Interoperability Standards -IS) for electronic data. Focuses on privacy & security between entities, not within them
International Organization for Standardization (ISO) 27000 series	2005	St	guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.	security policy; communications & operations management, access control; information security incident management;
Title IX of Public Law 109-	2006	L	establish a program to provide security for dept. information	establish and maintain a

461 of Veteran's Benefits			and information systems- ‘‘Department of Veterans Affairs Information Security Enhancement Act of 2006’’.	comprehensive department-wide information security program- provide for the development & maintenance of cost-effective security controls to protect Dept. information, in any media or format,
Payment Card Industry Data Security Standard	2006	St	requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.	
Independent Health Record Trust Act	2007	L-pending	Creates Privacy Protection Agreement between IHRT and participant	creates independent record trusts certified & regulated by FTC-compile, maintain & regulate access to EHRs for voluntary participants
Health Information Privacy and Security Act	2007	L-pending	Creates office of Health Information in HHS to protect privacy of personal health information	power to set stds. and & penalize entities
Wired for Healthcare Quality Act	2007	L-pending	Creates non-profit Nat'l Health Information Technology and Privacy Corp to ensure that its technologies sustain, don't erode privacy related to use, collection and disclosure of personal info	establishes AHIC to create & maintain national interoperability stds., voluntary for private entities except those contracting with Feds
Health Information Technology Act of 2007	2007	L-pending	award grants to eligible health care entities to offset costs related to clinical health care informatics systems -improve quality in health care and patient	Requires the Secretary to provide for the development and adoption of national data and

			safety	communication health information technology standards
PRO(TECH)T Act	2008	L-pending	provide incentives to doctors, hospitals, insurers, and the government to use electronic formats for health information, hopefully reducing medical errors and costs	provisions include safeguards, penalties, and notification requirements when a breach takes place.

Appendix B – Word Cruncher Sample

Words	**P1**	**P2**	**P3**	**P4**	**P5**	**P9**	**P11**	**P14**	**P15**	**P18**	**P19**	**P21**	**P23**	**P24**	**P25**	**P26**	**P27**	**P29**	**P30**	**P31**	**P36**	**P37**	**P38**	**P 9**	**P40**	**P41**	**P43**	**P46**	**P47**	**P48**	**P49**
ACCESS	0	1	0	0	0	3	0	0	0	3	17	0	0	1	67	5	1	0	0	0	0	25	1	14	7	208	20	17	0	57	2
ACCESS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	19	0	0	0	0	0
ACCESS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0
ACCESS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ACCESS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ACCESS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
ACCESS’’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0
ACCESSED	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	5	0	0	0	5	0
ACCESSES	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	0	3	0
ACCESSIBILITY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	3	0	0	0	2	0	0	0
ACCESSIBLE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	1	0	3	0	3	0	1	0
ACCESSING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0
ACCESS—THE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Access																															
ACCOUNTABILITY	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	0	1	0	3	2	9	2	0	0	0	0
ACCOUNTABILITY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
ACCOUNTABILITY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0
ACCOUNTABLE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Accountability																															
ACT	0	0	0	0	0	42	0	0	4	4	0	0	2	34	0	14	16	3	1	11	0	71	0	1	8	61	8	24	3	10	41
ACT’’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
ACT’’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
ACT’S	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ACTS	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	5	1	0	0	0	0	1	0	0	0	3	1	0	0	0	0
ACTS—SECTION	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Act																															
AHIC	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AHRQ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
ALARM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
ALARMS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Alarm																															

Appendix C – Initial Word Selection

Words	Freq	Docs
Access	598	49
Accountability	27	11
Act	463	35
AHIC	5	1
AHRQ	4	2
Alarm	13	5
Alert	13	7
ACCOUNTABILITY	1	1
ANSI	20	4
Attack	50	8
Audit	119	27
Authenticate	181	16
Authorize/Authority	393	73
Biometric	6	5
Breach	63	12
CCHIT	7	3
Communicate	92	37
Confidential	102	28
Consent	39	16
Consortium	16	6
Decrypt	11	6
Disclose	323	59
Encrypt	111	14
Enforce	96	30
FERPA	27	3
FIPS	63	2
Firewall	18	2
FISMA	6	1
FOIA	3	1
HIPAA	106	17
HITSP	20	2
Identify	265	73
Identity	31	8
Incident	74	16
Integrity	90	14
Interoperable	103	13
Intrusion	11	4
Law/Legal/Legislative	898	55
LOINC	25	2
ONCHIT	4	2
Password	47	9
Penalty	60	16
Policy	501	36
Private	512	36
Procedure	353	25
PSQIA	5	1
REAUTHORIZED	12	2
Risk	253	28
SARBANES	1	1
SDO	14	5
Secure	1797	60
SENSITIVE	1	1
Signature	56	12
SNIP	3	2
SNOMED	2	1
SOX	2	1
SSO	3	1
Standard	1198	60
Store	108	31
Theft/threat	41	24
TOKEN’	5	1
Trail	25	8
TRANSMISSION	2	1
UNAUTHORIZED	73	10
Unique	32	9
USERNAMES	1	1
Valid	3	2
WEDI	4	1

Appendix D - Frequency Word List

Word/Code	Docs	Percent
Standard	31	83.78
Secure	28	75.68
Law	27	72.97
Disclose	26	70.27
Private	26	70.27
Access	25	67.57
Act	25	67.57
Authorize	22	59.46
Policy	21	56.76
Risk	21	56.76
Communicate	21	56.76
Breach	21	56.76
Procedure	20	54.05
Threat	19	51.35
Confidential	17	51.35
Store	18	48.65
Audit	17	45.95
Enforce	16	43.24
HIPAA	13	35.14
Penalty	11	29.73
Consent	11	29.73
Not Used		
Integrity	8	21.62
Alert	7	18.92
Interoperable	6	16.22
Trail	6	16.22
Authenticate	5	13.51
Password	5	13.51
Attack	4	10.81
Biometric	4	10.81
Signature	4	10.81
Consortia	3	8.11
Decrypt	3	8.11
Encrypt	3	8.11
Firewall	1	2.70

Appendix E - Word/Code Frequency Distribution by Document-Sample

Date	Standard	Secure	Disclose	Private	Law	Act	Auth.	Access	Policy	Store	Risk	Proced.	Comm.	Confiden	Threat	Enforce	HIPAA	Audit	Penalty	Consent	Breach	**Total**
1890	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**7**
1901	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
1918	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**
1966	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**9**
1971	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**6**
1974	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**9**
1987	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**14**
1994	0	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	**7**
1994	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0	0	**16**
1994	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	**3**
1994	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**
1994	**3**	**1**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**0**	**1**	**1**	**2**	**0**	**1**	**0**	**18**
1996	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	0	0	1	0	0	**15**
1996	1	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0	1	**7**
1996	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**2**	**1**	**1**	**1**	**2**	**1**	**0**	**1**	**1**	**0**	**1**	**18**
1997	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**5**
1999	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**16**
2000	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**20**
2001	1	1	1	0	1	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	0	**13**
2001	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	0	1	1	0	1	0	**14**
2001	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**1**	**1**	**2**	**0**	**2**	**0**	**2**	**1**	**1**	**1**	**1**	**1**	**0**	**18**
2002	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	**4**
2002	1	1	0	0	1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	1	**10**
2002	0	1	1	0	1	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	**7**
2002	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	**18**
2002	**2**	**4**	**2**	**1**	**4**	**4**	**2**	**2**	**3**	**0**	**2**	**3**	**1**	**1**	**1**	**2**	**0**	**1**	**1**	**1**	**2**	**19**
2003	1	1	0	0	1	1	1	1	1	0	1	1	1	0	0	1	0	1	0	0	0	**12**
2003	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**21**
2003	1	1	1	1	0	1	0	0	0	1	1	0	0	1	1	0	1	0	0	0	0	**10**
2003	**3**	**3**	**2**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**21**
2004	1	1	1	1	1	0	1	1	0	1	1	0	0	0	1	0	1	0	0	0	0	**11**
2004	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**
2004	**2**	**2**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**11**
2005	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	0	**18**
2005	1	0	1	1	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	**8**
2005	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	0	0	1	0	0	1	**15**
2005	**3**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**3**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**21**
2006	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	0	0	1	0	0	1	**15**
2006	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	**19**

Appendix F - Word/Code Frequency by Document Date

Date	Standard	Secure	Disclose	Private	Law	Act	Auth.	Access	Policy	Store	Risk	Proced.	Comm.	Confid.	Threat	Enforce	HIPAA	Audit	Penalty	Consent	Breach	**Total**	**Average**
1890	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**7**	
1901	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	
1918	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	
1966	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**9**	
1971	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	
1974	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**9**	
1987	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**14**	
1994	**3**	**1**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**0**	**1**	**1**	**2**	**0**	**1**	**0**	**18**	**Total 66**
Total	**8**	**4**	**6**	**7**	**5**	**5**	**4**	**6**	**4**	**5**	**3**	**3**	**3**	**3**	**2**	**2**	**1**	**2**	**0**	**2**	**1**	**76**	**Avg-3.619**
%	**72.73**	**36.36**	**54.55**	**63.64**	**45.45**	**45.45**	**36.36**	**54.55**	**36.36**	**45.45**	**27.27**	**27.27**	**27.27**	**27.27**	**18.18**	**18.18**	**9.09**	**18.18**	**0.00**	**18.18**	**9.09**		
Docs	**11**																						
1996	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**2**	**1**	**1**	**1**	**2**	**1**	**0**	**1**	**1**	**0**	**1**	**18**	
1997	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**5**	
1999	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**16**	
2000	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**20**	
2001	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**1**	**1**	**2**	**0**	**2**	**0**	**2**	**1**	**1**	**1**	**1**	**1**	**0**	**18**	
2002	**2**	**4**	**2**	**1**	**4**	**4**	**2**	**2**	**3**	**0**	**2**	**3**	**1**	**1**	**1**	**2**	**0**	**1**	**1**	**1**	**2**	**19**	
2003	**3**	**3**	**2**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**21**	
2004	**2**	**2**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**11**	
2005	**3**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**3**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**21**	
2006	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**0**	**2**	**1**	**0**	**2**	**19**	
2007	**4**	**2**	**2**	**3**	**0**	**2**	**3**	**3**	**2**	**2**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**2**	**12**	
2008	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**10**	**Total 204**
Total	**23**	**22**	**17**	**16**	**17**	**18**	**17**	**18**	**15**	**11**	**16**	**13**	**12**	**11**	**13**	**11**	**9**	**11**	**9**	**7**	**11**	**305**	**Avg-14.52**
%	**88.46**	**84.62**	**65.38**	**61.54**	**65.38**	**69.23**	**65.38**	**69.23**	**57.69**	**42.31**	**61.54**	**50.00**	**46.15**	**42.31**	**50.00**	**42.31**	**34.62**	**42.31**	**34.62**	**26.92**	**42.31**		
#Doc	**26**																						

References

1. Halamka, John D. MD, Mandl, Kenneth D. MD, MPH and. Tang, Paul C MD Early Experiences with Personal Health Records, *J Am Med Inform Assoc*. 2008;15:1-7.

2. Griffith R. Understanding confidentiality and disclosure of patient information. *British Journal of Community Nursing*. 12(11):530-4, 2007 Nov.

3. Belsis MA. Dwivedi AN. Gritzalis S. Bali RK. Raouf N.G. Naguib. Providing secure mAccess to medical information. *International Journal of Electronic Healthcare*. 3(1):51-71, 2007.

4. Rhodes H. Breaking down privacy and security barriers to HIE. *Journal of Ahima*. 78(10):68-9, 2007 Nov-Dec.

5. Adler MP. HIPAA security redux. A re-evaluation process and recommended areas to review. *Journal of Ahima*. 78(10):38-42, 2007 Nov-Dec.

6. Alsobrook SC. HIPAA--where are we now?. *Journal of the Tennessee Dental Association.* 87(4):31-3, 2007.

7. Susilo W. Win KT. Securing electronic health records with broadcast encryption schemes. *International Journal of Electronic Healthcare*. 2(2):175-84, 2006.

8. Dalley A. Lynch K. Feltham P. Fulcher J. David Bomba. The use of smart tokens to permit the secure, remote access of electronic health records. *International Journal of Electronic Healthcare.* 2(1):1-11, 2006.

9. Grey M. Inside job. When it comes to patient information, the importance of maintaining proper data security can never be overestimated. *Healthcare Informatics*. 24(10):50-4, 56, 2007 Oct.

10. Matthews A. Trust systems for regional healthcare., *Healthcare Quarterly*. 10(4):146-8, 2007.

11. Gritzalis S. Belsis P. Katsikas SK. Interconnecting autonomous medical domains. Security, interoperability, and semantic-driven perspectives for electronic health records. *IEEE Engineering in Medicine & Biology Magazine*. 26(5):23-8, 2007 Sep-Oct.
12. Raths D. RHIOs go to Congress. As bills move forward in Washington, so too does healthcare IT along with all its privacy baggage. *Healthcare Informatics*. 24(9):44-5, 2007 Sep.

13. Spitzer M. Brinkmann L. Ueckert F. Clearinghouse: a teleradiology platform emphasizing security of data and communication. *Medinfo.* 12(Pt 1):508-12, 2007.

14. Croll PR. Henricksen M. Caelli B. Liu V. Utilizing SE Linux to mandate ultra-secure access control of medical records. *Medinfo*. 12(Pt 1):498-502, 2007.

15. Zafar A. Dixon BE. Pulling back the covers: technical lessons of a real-world health information exchange. *Medinfo*. 12(Pt 1):488-92, 2007.

16. Malin B. Airoldi E. Confidentiality preserving audits of electronic medical record access. *Medinfo*. 12(Pt 1):320-4, 2007.

17. Scaglione BJ. Digital security technology simplified. *Journal of Healthcare Protection Management.* 23(2):51-60, 2007.

18. Maune J. Wezelis K. Building continuity. As hospitals look at ways to secure critical patient data, the question remains: how costly will it be?, *Healthcare Informatics.* 24(8):75-6, 2007 Aug.

19. Libenson E. The threat from within. Implementing secure access controls helps organizations protect sensitive patient information from insider threat. *Healthcare Informatics.* 24(7):54, Jul. 2007

20. Halpert A. Davis N. Lemery C. Hjort B. AIHMA Privacy and Security Practice Council. Safeguards for remote access. *Journal of Ahima.* 78(7):68-70, 2007 Jul-Aug.

21. Department of Veterans Affairs. Data breaches. Interim final rule. *Federal Register.* 72(120):34395-401, 2007 Jun 22.

22. Connor K. Privacy architecture and e-consent. What the future holds. *Journal of Ahima.* 78(6):64-5, 70, 2007 Jun.

23. Rode D. Refocusing on confidentiality and security. *Journal of Ahima*. 78(6):18, 20, 2007 Jun.

24. Flucke J. Prying eyes: strategies to ensure the confidentiality of your digital records. *Dental Assistant.* 76(3):10, 12-3, 2007 May-Jun.

25. Adam Wright, PhD and Dean F. Sittig, PhD., Encryption Characteristics of Two USB-based Personal Health Record Devices, *Journal of the American Medical Informatics Assoc.* 2007;14:397-399.

26. Fesko H. McGuigan P. Prevention of HIPAA security breaches. *Health Care Law Monthly.* :3-9, 2007 May.

27. Goedert J. I.T. threats: obvious, unknown or hyped? *Health Data Management*. 15(5):54, 56, 58 passim, 2007 May.

28. Martin L. Keys of encryption. *Health Management Technology*. 28(5):18, 20, 2007 May.

29. Amatayakul M. The value of HIM in and security privacy compliance., *Journal of Ahima.* 78(5):44-6; quiz 49-50, 2007 May.

30. Kim DK. Yoo SK. Park JJ. Kim SH., PDA–Phone-Based Instant Transmission of Radiological Images over a CDMA Network by Combining the PACS Screen with a Bluetooth-Interfaced Local Wireless Link *Journal of Digital Imaging,* Volume 20, Number 2 / June, 2007, pp 131-139

31. Mohammed Y. Sax U. Viezens F. Rienhoff O. Shortcomings of current grid middlewares regarding privacy in HealthGrids. *Studies in Health Technology & Informatics.* 126:322-9, 2007.

32. Holub P. Hladka E. Prochazka M. Liska M., Secure and pervasive collaborative platform for medical applications. *Studies in Health Technology & Informatics*. 126:229-38, 2007.

33. Herveg J. Does HealthGrid present specific risks with regard to data protection?. *Studies in Health Technology & Informatics*. 126:219-28, 2007.

34. Wernick AS. Connectivity, privacy, and liability. What medical professionals must consider. *Journal of Ahima.* 78(4):64-5, 2007 Apr

35. Zhou Z. Data security assurance in CAD-PACS integration. *Computerized Medical Imaging & Graphics.* 31(4-5):353-60, 2007 Jun-Jul.

36. Elliott K. Securing the network. Network access control solutions can be an important tool in the fight against intrusion. *Healthcare Informatics.* 24(3):55, 2007 Mar.

37. Albright B. Guarding the perimeter. New security risks and HIPAA compliance continue to challenge IT professionals. *Healthcare Informatics.* 24(3):42-4, 2007 Mar.

38. Brown EV. Safeguarding and monitoring Data transmission. A Honolulu-based healthcare enterprise safeguards against confidential data leaks. *Health Management Technology*. 28(3):32-3, 2007 Mar.

39. Wozak F. Schabetsberger T. Ammmenwerth E. End-to-end security in telemedical networks--a practical guideline. *International Journal of Medical Informatics.* 76(5-6):484-90, 2007 May-Jun.

40. Kluge EH. Secure e-Health: managing risks to patient health data. *International Journal of Medical Informatics*. 76(5-6):402-6, 2007 May-Jun.

41. Lovis C. Spahni S. Cassoni N. Geissbuhler A. Comprehensive management of the access to the electronic patient record: towards trans-institutional networks. *International Journal of Medical Informatics*. 76(5-6):466-70, 2007 May-Jun.

42. Sucurovic S. Implementing security in a distributed web-based EHCR. *International Journal of Medical Informatics*. 76(5-6):491-6, 2007 May-Jun.

43. Blobel B. Comparing approaches for advanced e-health security infrastructures. *International Journal of Medical Informatics*. 76(5-6):454-9, 2007 May-Jun.

44. Anderson JG. Social, ethical and legal barriers to e-health. *International Journal of Medical Informatics.* 76(5-6):480-3, 2007 May-Jun.

45. Sloane T. D.C. (not) confidential. Unless congress steps in, HHS is content to let health data privacy wither. *Modern Healthcare.* 37(10):24, 2007 Mar 5.

46. Krishna R. Kelleher K. Stahlberg E. Patient confidentiality in the research use of clinical medical databases. *American Journal of Public Health*. 97(4):654-8, 2007 Apr.

47. Scott M. Privacy & security. Worried about stolen laptops? Help is here. *Hospitals & Health Networks.* 81(2):24-5, 2007 Feb.

48. Burritt B. Security solutions. An ounce of preventative care yields enormous returns for Kettering Medical Center. *Healthcare Informatics.* 24(2):72, 74, 2007 Feb.

49. Collmann J. Cooper T. Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security. *Journal of the American Medical Informatics Association*. 14(2):239-43, 2007 Mar-Apr.

50. Beech M. Confidentiality in health care: conflicting legal and ethical issues. *Nursing Standard.* 21(21):42-6, 2007 Jan 31-Feb 6.

51. Haugh R. HIPAA. Averting a big oops. Hos*pitals & Health Network*s. 81(1):16, 18, 2007 Jan.

52. Demster B. Ensuring privacy and security in home health. *Journal of Ahima.* 78(1):62-3, 2007 Jan.

53. Alvarez G. Li S. Hernandez L. Analysis of security problems in a medical image encryption system. *Computers in Biology & Medicine*. 37(3):424-7, 2007 Mar.

54. Kraemer S. Carayon P. Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics.* 38(2):143-54, 2007 Mar.

55. Paquette M. An ounce of prevention for the healthcare IT network. *Health Management Technology*. 27(12):18, 20-1, 2006 Dec.

56. Malin B. Re-identification of familial database records. AMIA ... Annual Symposium Proceedings/AMIA Symposium. 524-8, 2006.

57. Goedert J. Keeping up with HIPAA compliance. *Health* Data Management. 14(12):36, 38, 40 passim, 2006 Dec.

58. Halamka J. Juels A. Stubblefield A. Westhues J. The security implications of VeriChip cloning. *Journal of the American Medical Informatics Association*. 13(6):601-7, 2006 Nov-Dec.

59. Nordberg R. EHR in the perspective of security, integrity and ethics. *Studies in Health Technology & Informatics.* 121:291-8, 2006.

60. Conn J. A real steal. Patients, providers face big liabilities as medical identity theft continues to rise, and in many cases it's an inside job. *Modern Healthcare*. 36(40):26-8, 2006 Oct 9.

61. Haugh R. Technology. IT gets HIPAA. *Hospitals & Health Networks*. 80(9):14-5, 2006 Sep.

62. Conn J. HIPAA, 10 years after. *Modern Healthcare*. 36(31):26-8, 2006 Aug 7.

63. Conn J. Embedded trouble. Link in software inherited through acquisition left patient data vulnerable. *Modern Healthcare.* 36(32):28, 30, 2006 Aug 14.

64. Hilty DM. Yellowlees PM. Cobb HC. Neufeld JD. Bourgeois JA. Use of secure e-mail and telephone: psychiatric consultations to accelerate rural health service delivery. *Telemedicine Journal & E-Health.* 12(4):490-5, 2006 Aug.

65. Giakoumaki A. Pavlopoulos S. Koutsouris D. Secure and efficient health data management through multiple watermarking on medical images. *Medical & Biological Engineering & Computing.* 44(8):619-31, 2006 Aug.

66. Davies C. Collins R. Balancing potential risks and benefits of using confidential data. *British Medical Journal.* 333(7563):349-51, 2006 Aug 12.

67. Souhami R. Governance of research that uses identifiable personal data. *British Medical Journal..* 333(7563):315-6, 2006 Aug 12.

68. Conn J. Personal and (maybe) confidential. Questions over privacy, formats and definitions remain, but personal health records are on the way. *Modern Healthcare.* 36(27):28-31, 2006 Jul 3-10.

69. Rhodes HB. Privacy and security challenges in HIEs. *Journal of Ahima*. 77(7):70-1, 74, 2006 Jul-Aug.

70. Demster B. A resource for privacy and security programs. *Journal of Ahima*. 77(7):68-9, 74, 2006 Jul-Aug.

71. Singleton P. Wadsworth M. Consent for the use of personal medical data in research.] *British Medical Journal.* 333(7561):255-8, 2006 Jul 29.

72. Kalra D. Gertz R. Singleton P. Inskip HM. Confidentiality of personal health information used for research. *British Medical Journal*. 333(7560):196-8, 2006 Jul 22.

73. Blobel B. Nordberg R. Davis JM. Pharow P. Modelling privilege management and access control. *International Journal of Medical Informatics*. 75(8):597-623, 2006 Aug.

74. Lubell J. VA theft included medical data. Groups concerned information could be used to discriminate against vets. *Modern Healthcare*. 36(22):12, 2006 May 29.

75. FIGO Committee for the Ethical Aspects of Human Reproduction and Women's Health. Confidentiality, privacy and security of patients' health care information. *International Journal of Gynaecology & Obstetrics*. 93(2):184-6, 2006 May.

76. Choi YB. Capitan KE. Krause JS. Streeper MM. Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *Journal of Medical Systems*. 30(1):57-64, 2006 Feb.

77. Quinnild J. Fusile J. Smith C. Why information security belongs on the CFO's agenda. *Healthcare Financial Management.* 60(2):56-9, 2006 Feb.

78. Nam-Ju Lee RN, MSN, Justin Starre, MD, PhD, Suzanne Bakken, RN, DNSc, School of Nursing, Department of Biomedical Informatics, Department of Radiology, Columbia University, New York, NY USA A Systematic Review of User Interface Issues Related to PDA-based Decision Support Systems in Health Care. AMIA Symposium :1021, 2005

79. Chong D. Better remote access, secure endpoints. An upgrade for an outdated remote access solution extends the network while bolstering endpoint control. [Journal Article] *Health Management Technology*. 28(10):38-9, 2007 Oct.

80. Blobel B. Advanced and secure architectural EHR approaches. *International*

Journal of Medical Informatics. 75(3-4):185-90, 2006 Mar-Apr.

81. Rudolph BA. Shah GH. Love D. Small numbers, disclosure risk, security, and reliability issues in Web-based data query systems. *Journal of Public Health Management & Practice.* 12(2):176-83, 2006 Mar-Apr.

82. Srinivasan A. Keeping online personal records private: security and privacy considerations for Web-based PHR systems. *Journal of Ahima*. 77(1):62-3, 68, 2006 Jan.

83. Austin S. E-mail: so fast, so convenient, so ... risky?, *Nursing.* 36(2):76, 2006 Feb.

84. Noore A. Singh R. Vatsa M. Houck MM. Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International*. 169(2-3):188-94, 2007 Jul 4.

Giakoumaki A. Pavlopoulos S. Koutsouris D. Secure and efficient health data management through multiple watermarking on medical images. *Medical & Biological Engineering & Computing.* 44(8):619-31, 2006 Aug.

85. Bones Erland, Hasvold Per, Henriksen Eva, Strandenoes Thomas, Risk Analysis of Information Security in a mobile instant messaging and presence system for health care. *International Journal of Medical Informatics* 76 (2007) 677–687

86. Schattner P. Pleteshner C. Bhend H. Brouns J. Guidelines for computer security in general practice. *Informatics in Primary Care*. 15(2):73-82, 2007.

87. EHNAC-Electronic Healthcare Network Accreditation Commission, Healthcare Network Accreditation Program Criteria-HNAP, Version 9.4, January 1, 2008

88. Meray N. Reitsma JB. Ravelli AC. Bonsel GJ. Probabilistic record linkage is a valid and transparent tool to combine databases without a patient identification number. *Journal of Clinical Epidemiology*. 60(9):883-91, 2007 Sep.

89. Daunt M. Using healthcare data: Security protection is needed when using USB sticks.[comment]. *British Medical Journal.*. 335(7611):112, 2007 Jul 21.

90. Conn, Joseph, Upgrading to Health 2.0, *Modern Healthcare,* 01607480, 12/10/2007, Vol. 37, Issue 49

91. Conn J. GAO rebukes HHS on milestones. Agency says privacy, security must be addressed timely. *Modern Healthcare*. 37(26):46, 2007 Jun 25.
Amatayakul M. Are you ready for HIPAA now? *Healthcare Financial Management* 112-114 May 2007.

92. Ruest Nelson; Ruest Danielle, Building a World of Trust— The Case for

Outsourcing PKI, Accessed 03/21/2008 from White Paper 13 December 2007

93. *Safeguarding Private Medical Data* (2008). Accessed March 26,2008, New York Times Web site:Http://www.nytimes.com/2008/03/ Published: March 26, 200826/opinion/26wed2.html?ex=1207195200&en=5a30e67290d97792&ei=5070 &emc=eta1

94. Pashel, George, Understanding standards development, *Behavioral Healthcare,* March 2008

95. Hirsch, Reece, EMRs, Data Mining and HIPAA (2008) from Healthcare Informatics Blog, Web site: http://www.healthcare-informatics.com/ME2/dirmod.asp?sid=349DF6BB879446A1886B65F332AC487F &nm=&type=Blog&mod=View+Topic&mid=67D6564029914AD3B204AD35D8 F5F780&tier=7&id=0132A4630BDD4E58B61EBAD98A6384CD- Accessed 04/30/2008

96. Luella Nash LeVee- Access is Power (May 12, 2008) Accessed May 29th, 2008 from Military Medical Technology, Web site: http://www.military-medical-technology.com/article.cfm?DocID=695

97. Cohn, Simon MD, (June 22, 2006) *MPH Letter to the Secretary; Recommendations regarding Privacy and Confidentiality* Accessed May 28, 2008 Web site:http://ncvhs.hhs.gov/060622lt.htm - 61KB - 30 Jun 2006

98. Isreal, Rob, Building an Endpoint Security Arsenal, *Health Management Technology* Jul2007, Vol. 28 Issue 7, p12-36, 4p

99. Surveying the RHIO Landscape - Practice Brief, *Journal of Ahima,* Jan 2006 77/1, pg 64A

100. *Office of the National Coordinator: Mission*(2006) Accessed 08/31/2008) from Health Information Technology Web site: http://www.hhs.gov/healthit/onc/mission/

101. Blobel Bernd, Comparing Approaches for advanced e-health security infrastructures. *International Journal of Medical Informatics* 76 2007 454-459

102. *Cell phone as medical tool* (2008). Accessed June 09, 2008, from Boston Globe June 2, 2008 Web site: http://www.statesman.com/business/content/business/stories/technology/06/02/0602cellphonemedicine.html

103. Bosveld, Jane, Science on the Edge, *Discover* June 2008, pg 62

104. Chou David C., Chou Amy Y, Healthcare information portal: a web technology for

the healthcare community, *Technology in Society* 24 2002 pp317-330

105. Burritt Bob, *Security Solutions* (February 2007). Accessed 6/24/2007 from Healthcare Informatics, Web site: http://www.healthcare-informatics.com/ME2/dirmod.asp?sid=&nm=&type=Publication&m

106. *The U.S. Patriot Act*(2006). Accessed 07/01/2008 from The White House, Web site: http://www.whitehouse.gov/infocus/patriotact/

107. *The U.S.Patriot Act*(2006). Accessed 07/01/2008 from Wikipedia, Web site: http://en.wikipedia.org/wiki/USA_PATRIOT

108. *The Sarbanes – Oxley Act*(2002). Accessed 07/01/2008 from Guide to the Sarbanes-Oxley Act, Web site:http://www.soxlaw.com/

109. *ISO IEC 17799 2005* (2005). Accessed 07/02/2008 from Praxiom Research Group, Ltd Web site: http://praxiom.com/iso-17799-2005.htm

110. *Interoperability Specifications*(2005). Accessed 7/10/2008 from HITSP Web site:http://www.hitsp.org/government.aspx

111. *CEN EN13606*(2007). Accessed 07/14/2008 from CEN Standards Web site: http://www.openehr.org/standards/cen.html

112. *HL7 Standard*(1997) Accessed 07/14/2008 from openEHR Web site: http://www.openehr.org/standards/hl7.html

113. *ANSI ASCX12*(1979). Accessed 07/14/2008 from Wikipedia, Web site :http://en.wikipedia.org/wiki/ANSI_ASC_X12

114. *Payment Card Industry Standard* (2006). Accessed 08/05/2008 from PCI Security Standards Council Web site: http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

115. Krohn, Richard. HIPAA Compliance: A Technology Perspective, *JHIN* Vol. 16, No.2 2002 pp 14-15

116. Covitch, Jennifer. Managing Web Access Through Delegated Administration, *JHIN* Vol 16 No. 2 2002 pp 8-9

117. Bauer, Jeffrey C PhD. HIPAA: A Paradigm Shift in the Politics of Healthcare, *JHIN* Vol 18 No. 2 2004 pp 5-6

118. Brantley, Alton MD PhD. HIPAA: Reviewing the Game Films, *JHIN* Vol. 18 No. 2 2004 pp 7-9

119. Ao Mei , Walker Rosemary DDS MBA MS. CIO's Views of HIPAA Security Rule Implementation – An Application of Q Methodology, *JHIN* Vol. 19 No. 2 2005. pp 73-80

120. Klein Sharon Esq, Jones John W. Clinical Decision Support Programs Can Be Risky Business, *JHIN* Vol. 21 No. 2 2007 pp 15-17

121. Wilson Marilyn. Mobilizing the Right Resources to Achieve HIPAA Compliance, *JHIN* Vol. 16 No. 2 2002 pp 5-7

122. Amatayakul, Margaret. Security Project Plan, *JHIN* Vol. 16 No. 2 2002 pp 12-13

123. Carter Patricia I JD. Applying Your Corporate Compliance Skills to the HIPAA Security Standard. *JHIN* Vol. 14 No. 4 2005 pp 13-27

124. Aitkins Rita. Risk Management Methodology for HIPAA Security Standard. *JHIN* Vol. 14 No. 4 pp 29-40

125. *Privacy Act of 1974*(1974). Accessed 08/11/2008 from United States Department of Justice, Web site: http://www.usdoj.gov/oip/04_7_1.html

126. *Report to Secretary of the U.S. Department of Health and Human Services on Uniform Data Standards for Patient Medical Record Information as Required by the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996*(1996). Accessed 08/11/2008 from http://www. www.hipaadvisory.com/regs/ncvhsexecsum.htm

127. *CCHIT* (2008). Accessed 08/12/2008 from Certification Commission for Healthcare Information Technology, Web site: http://www.cchit.org/about/news/releases/2008/Personal-Health-Records-PHR-Patient-Privacy-Focus-Task-Force.asp

128. *Right to Information Act 2005*(2005) Accessed 08/12/2008 from Wikipedia, Web site: http://en.wikipedia.org/wiki/RTI_Act

129. *Freedom of Information Legislation*(1966) Accessed 08/12/2008 from Wikipedia Web site:http://en.wikipedia.org/wiki/Freedom_of_information_legislation

130. Jacobs, Ian, *World Wide Web Consortium*(2004) Accessed 08/13/2008 from About the World Wide Web Consortium, Web site: http://www.w3.org/Consortium/

131. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981).Accessed 08/14/08 from Council of Europe, Web site: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

132. *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing*

Off-the-Shelf (OTS) Software (2005) Accessed 08/21/08 from Center for Devices and Radiological Health, Web site: http://www.fda.gov/cdrh/comp/guidance/1553.html

133. Shelby, Anne, *Pending Privacy and Data Security Legislation in the 110th Congress*(2007). Accessed 08/22/2008 from Privacy and Security Law Blog. Web site:http://www.privsecblog.com/archives/federal-legislation-pending-privacy-and-data-security-legislation-in-the-110th-congress.html

134. Centers for Medicare and Medicaid Services, Accessed 08/22/2008 Web site:http://www.cms.hhs.gov/

135. The Joint Commission, Accessed 08/22/2008 Web site: http://www.jointcommission.org/

136. Hall, Mark A. Hoffman, Sharona, *Hastings Center Report*; Jan2008, Vol. 38 Issue 1, p7-8, 2p

137. Steward, Melissa Electronic Medical Records, Privacy, Confidentiality, Liability, *Journal of Legal Medicine,* 2005, 26:491-506

138. Beech. Maureen, Confidentiality in health care; conflicting legal and ethical issues, *Nursing Standard* January 2007 Vol. 21(21) pp 42-46

139. Hall Mark A, The HIPAA Headache *The Hastings Report* Jan/Feb 2008 pg 7

140. Hoffman, Sharona, Letter to the Editor *The Hastings Report* Jan/Feb 2008 p 8

141. Hagland, Mark The Gap: HIPAA and Secure IT, *Health Management Technology* May 1998, Vol. 19 (6) p24

142. Cantor Julie D MA, JD Privacy Protections for Cybercharts: An Update on the Law, *JAMA* April 2001 , 285:1767

143. Hussong Sharon, Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights, *American Journal of Law and Medicine* 2000, 26, 453-474

144. Hodge James G Jr. JD, LLM, Gostin Lawrence O. JD, Jacobson Peter D JD, MPH, Legal Issues Concerning Electronic Health Information, Privacy, Quality, and Liability, *JAMA* 1999, Vol. 282 (15) 1466-1471

145. Masys Daniel, MD, Baker Dixie PhD, Butros Amy MLS, Cowles Kevin, Giving Patients Access to Their Medical Records via the Internet, *Journal of the American Informatics Association* April 2002 Vol. 9(2) pp 181-191

146. Rosenbaum Sara, JD, Burke Taylor, JD LLM, Benevelli John Candidate JD, MPH, Borzi Phyllis M Ed, JD, Repasch Lee, MA, Legal Issues in Health Information : Implications for Public Health Practice and Policy, *Public Health Reports* May-June 2005, Vol. 120 pp350-352

147. Gostin Lawrence O. JD, LLD(Hon) Hodge James G. Jr. JD, LLM, Valdiserri, Ronald O. MD MPH, Informational Privacy and the Public's Health: The Model State Public Health Privacy Act, *American Journal of Public Health*, September 2001, Vol. 91 (9) pp 1388-1392

148. Magnusson Roger S.., The Changing Legal and Conceptual Shape of Health Care Privacy*, Journal of Law, Medicine, Ethics*, Winter 2004, pp 680-691

149. Donawa Maria, Change in FDA Stance on Part 11 Requirements, *Medical Device Technology,* April 2003, pp 24-26

150. *Freedom of Information Act 1966* (1966) Accessed 08/27/2008 from Historical Documents Web site: http://www.historicaldocuments.com/FreedomofInformationAct.htm

151. *Title IX of Public Law 109-461*(Dec 22, 2006). Accessed 08/27/08 from Web site: http://www.va.gov/ogc/docs/PL109-461.pdf

152. *Patient Safety and Quality Improvement Act of 2005 (PSQIA)* (2005). Accessed 08/30/2008 from United States Department of Health and Human Services Web site:http://www.hhs.gov/ocr/psqia/

153. *Health Information Technology Act of 2007* (2007) Accessed 08/20/2008 from Govtrack.us, Web site:http://www.govtrack.us/congress/bill.xpd?bill=s110-1408

154. Marshall Glenn, Moehrke John, Security, Privacy and Infrastructure. HITSP Webinar Series, August 21, 2008

155. *News and Updates,*(2008). Accessed Sept.21,2008 from Centers for Law and the Public's Health Web site: http://www.publichealthlaw.net/Projects/WHO%20PAHO.php

156. Comprehensive Privacy and Security: Critical for Health Information Technology Center for Democracy and Technology Version 1.0 May 2008

157. *2007: A Year of Record Data Breaches* (2008). Accessed September 2008 from Baseline Magazine, Web site: http://www.baselinemag.com/c/a/Security/2007-A-Year-of-Record-Data-Breaches/

158. *Security Rule and Privacy Rule Distinctions* Accessed 09/21/08 from Interhack, Web site:

http://web.interhack.com/publications/hipaasec_analysis.php?bcsi_scan_24E4C0F8750746C8=IW3dyLBQKl3bajvVLNtrjSEAAADTSjRj&bcsi_scan_filename=hipaasec_analysis.php.

159. *By Legal Requirement* (2007). Accessed 08/31/2008 from the National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/PubsByLR.html

160. Miller, Chuck, *National health-record privacy law in Congress.*(June 26 2008) Accessed 09/03/2008 from ESET Web site: http://www.scmagazineus.com/National-health-record-privacy-law-in-Congress/PrintArticle/111818/

161. *Medicare Modernization Act*(2003). Accessed 09/19/08 from U.S. Treasury Web site: http://www.ustreas.gov/offices/public-affairs/hsa/pdf/pl108-173.pdf

162. *MEDecision CEO Endorses Federal Family Health Information Technology Act of 2006* (March 16, 2006) Accessed 09/23/08 from Business Wire Web site: http://findarticles.com/p/articles/mi_m0EIN/is_2006_March_16/ai_n26797792

163. *H.R. 3800: Promoting Health Information Technology Act* (2007). Accessed 09/02/2008 from Govtrack.us Web site: http://www.govtrack.us/congress/bill.xpd?bill=h110-3800&tab=summary

164. Herold, Rebecca, *Insider Threat Examples & 7th HIPAA Criminal Conviction*(2008) Accessed 09/02/08 from Realtime Community IT Compliance Web site: http://www.realtime-itcompliance.com/laws_regulations/2008/08/insider_threat_examples_7th_hi.htm

165. *Health Insurance Reform: Security Standards*, (Thursday, February 20, 2003) Accessed 08/27/08 from The Federal Register/ Vol. 68, No. 34 Web site: http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf

166. The Future of Privacy, *Scientific American*, September 2008, pp 46-72

167. Daniel, Jodi JD,MPH, *Health IT Privacy and Security: Protecting Health Information Nationwide* (11/19/2008) Accessed 11/21/2008 from HIMSS Virtual Conference Web site: http://www.himssvirtual.org/Nov09presentations/

Jacqueline H. Phillips, R.N. **CURRICULUM VITAE**

CAREER RELATED EXPERIENCE

June 2005 – present
Clinical Research Coordinator/Informaticist
St. Vincent Hospital, Indianapolis, Indiana
Indiana Neuroscience Institute
Conduct and develop clinical research/Develop and maintain databases for data collection and analysis.

June 2004 – present
Sr. Information Services Consultant
St, Vincent Hospice, Indianapolis, Indiana
Maintain clinician computers/Create and maintain clinical forms.

September 2001 – present
Database Consultant
Indiana Task Force One, Indianapolis, Indiana
Maintain database/Develop forms

January 2000 – 2001 , 2004 - present
Staff Nurse
St. Vincent Hospice, Indianapolis, Indiana
Adult and pediatric patient care

September 1996 – 2006
Website Design/Database Management
Vi Walker Silver, Indianapolis, Indiana
Website design and maintenance/Database design and maintenance

April 1987 – 2007
Firefighter/Paramedic
Pike Township Fire Department, Indianapolis, Indiana
Firefighting and emergency medical care

January 1983 – 2000
Staff Nurse
St. Vincent Hospital, Indianapolis, Indiana
Coronary Care and Emergency Department

May 1980 – 1985
Staff Nurse
Hendricks Community Hospital, Danville, Indiana
Operating Room

7733 WEST 96TH STREET, ZIONSVILLE, IN 46077 ~ 317-873-2210 ~ JACID@AOL.COM

EDUCATION

Clinical Research Certificate
Indiana University/Purdue University, Indianapolis, Indiana
Completion: 2006

Associate of Science in Fire Technology
Ivy Tech Community College, Indianapolis, Indiana
Graduation: April 1992 (4.0 GPA)

Associate of Science in Nursing
Indiana University, Indianapolis, Indiana
Graduation: May 1980 (3.6 GPA)

Bachelor of Fine Arts
Ohio Wesleyan University, Delaware, Ohio
Graduation: June 1967 (3.1 GPA)

PROFESSIONAL SKILLS

29 years nursing experience
15 years experience with personal computers
12 years experience Microsoft Access
McKesson Horizon Home Care, Front Page,
Power Point, Microsoft Office