An Overview of Laws and Standards for Health Information Security and Privacy

Francis Akowuah[1], Xiaohong Yuan[1], Jinsheng Xu[1], Hong Wang[2]
[1]Department of Computer Science, North Carolina A&T State University, Greensboro, North Carolina, USA
[2]Department of Management, North Carolina A&T State University, Greensboro, North Carolina, USA

Abstract
In the complex technological world that healthcare organizations and their business associates operate, there exist security threats and attacks which render individually identifiable health information vulnerable. Laws exist to ensure that healthcare providers take practical measures to address the security and privacy needs of health information. There are also standards that assist healthcare entities to meet the security and privacy requirements of health information. This paper provides a chronological overview of U.S. laws and standards related to health information security and privacy, such as HIPAA, Sarbanes-Oxley Act, HITECH, COBIT, ISO/IEC 27002 2005, and CSF.

Keywords
Health information systems, security and privacy, laws, standards

1. Introduction

With the adoption of health information systems, healthcare organizations and their business associates operate in a complex, interconnected, technological world. Individual identifiable health information thus become vulnerable to an entire new set of security threats and attacks such as malicious code, denial of service, and many others. When these threats and attacks are successful, individual privacy becomes woefully invaded. Moreover, it brings about economic loss and reputation damage to healthcare organizations [1].

Fortunately, the United States government has taken keen interest in healthcare provisioning and has enacted laws and regulations over the years to curb the security and privacy problems faced by healthcare organizations. These laws require healthcare entities to take measures to address the security and privacy needs of health information. Notable among these laws are Health Insurance and Portability Act (HIPAA), Sarbanes-Oxley Act, and Health Information Technology for Economic and Clinical Health (HITECH). Standards such as Control Objectives for Information and Related Technology(COBIT), ISO 27002 2005 and Common Security Framework (CSF) also exist to assist these entities to meet the security requirements of the law.

In this paper, we give a chronological overview of the United States laws and standards for health information security and privacy. We consider federal laws such the HIPAA, Sarbanes-Oxley Act, and HITECH. The requirements of these laws and their implications on healthcare providers are discussed. Furthermore, recommendations and best-practices of COBIT, ISO/IEC 27002 2005, and CSF are overviewed. Laws that were enacted before 1996 to protect individual health information are also briefly discussed. Though other laws and standards exist that relate to information systems, only those related to health information security and privacy are discussed in this paper.

The remainder of the paper is structured as follows. Section 2 provides information about pre-HIPAA laws. Sections 3 to 5 overview HIPAA, Sarbanes-Oxley and HITECH respectively. Sections 6, 7 and 8 discuss COBIT, ISO/IEC 27002 2005 and CSF standards. Section 9 concludes the paper.

2. Federal Laws Prior To HIPAA

Before HIPPA came into enforcement there had not been a far-reaching federal regulation that ensured or catered for private health information. The Freedom of Information Act passed in 1966 provided the American public the right to acquire information from federal agencies with some exceptions. Among the nine exceptions were access to personnel and medical information, since a disclosure of such information obviously was an invasion of privacy [2]. This exception was however not strong enough to protect patient records and other health information.

As a result, the Privacy Act of 1974 was enacted specifically to protect patient confidentiality. However, only federally operated health care facilities had to comply with this act. It was an important legislation because it explicitly stated that patients had the right to access and amend their medical records. Medical facilities were required under this act to document all disclosures of patients' health information [2].

3. Health Insurance Portability And Accountability Act Of 1996 (HIPAA)

HIPAA was signed into law on August 21, 1996. The objectives were to make health care delivery more efficient

and to increase the number of Americans with health insurance coverage. Three main provisions were made to achieve the objectives. They are portability, tax and administrative simplification provisions. This paper focuses on the administrative simplification provision.

The Department of Health and Human Services (HHS), as instructed by the administrative simplification provision, issued a number of regulations concerning electronic transmission of health information, which was expanding rapidly in the early 1990s. Although the ultimate aim of the provisions was to standardize the use of electronic health information, Congress realized that advances in electronic technology could compromise the privacy of health information. Consequently, nationwide security standards and safeguards were developed for the use of electronic health care information (referred to as the Security Rule). In addition, privacy standards were created for protected health information (referred to as the Privacy Rule) [3]. In what follows, the HIPAA Privacy Rule and Security Rule are described.

3.1 HIPAA Privacy Rule

Standards for Privacy of Individually Identifiable Health Information or the Privacy Rule was first published on December 28, 2000 by the United States Department of Health and Human Services. The rule however became effective in April 2003 [4]. It promulgates detailed regulations concerning the types of uses and disclosures of individually identifiable health information that are permitted by the covered entities [3].

The Privacy Rule defines *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral as Protected Health Information (PHI). "Individually identifiable health information" refers to information, including demographic data that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Employment data kept by covered entities in their capacity as employer are not considered as PHI [5]. Typical examples of PHI are medical records, billing records, enrollment, payment, claims adjudication, etc. [6].

While allowing the flow of health information to enhance high quality health care and protect public health and well-being, the Privacy Rule ensures that individuals' health information is properly protected. In other words, while it provides protection of the privacy of the patient's health information, it also allows important uses. In order to allow the flow of information, covered entities are permitted (not required) to disclose and use health information without individual's authorization for the following purposes:

- Treatment, payment and healthcare operations
- Public interest and benefit activities
- Limited data set for research, public health

The Privacy Rule also permits informal permission to be obtained from the individual, usually, in situations when he/she is incapacitated. The individual has the opportunity to agree, acquiesce or object. Moreover, individuals can request access to and an accounting of uses and disclosures of health information from covered entities [5]. Patients have the right to access their information and to request for how the information has been disclosed.

3.2 HIPAA Security Rule

The Health Insurance Reform: Security Standards or the Security Rule was published in the federal register on February 20, 2003 but compliance began on April 21, 2006. [4]. It establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. Once again, covered entity refers to organizations that are subject to the rule. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information [5].

Administrative safeguards are policies and procedures that depict how the covered entity complies with HIPAA. These include written privacy policies and the designation of a Privacy Officer. Physical safeguards control physical access to protected health information to avoid unauthorized access to protected data. Technical safeguards control access to computer systems and protect PHI transmitted over open networks from being intercepted [4].

The emphasis must be laid here that while HIPAA Privacy Rule protects the privacy of PHI, HIPAA Security Rule protects only information that a covered entity creates, receives, maintains or transmits in *electronic form*. Hence it does not apply to PHI transmitted orally or in writing. Electronic transmission includes media such as the Internet, extranets, private networks, leased lines, and dial-up lines. It does not include paper faxes, voice mail, telephone calls, or videoconferencing [6].

4. Sarbanes-Oxley Act of 2002 (SOX)

The name of the act was coined from Senator Paul Sarbanes and Representative Michael Oxley who drafted the act in 2002. The intent is "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes". Section 302 spells new standards for corporate accountability and penalties for acts of wrong-doing. It holds Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) accountable for the accuracy and completeness of financial statements. According to Section

404 of the act, publicly-traded organizations are supposed to implement internal controls and procedures to communicate, store and protect financial data. These controls must be protected from internal and external threats and unauthorized access, including those that occur through online systems and networks [7]. Organizations must assess the effectiveness of these controls and report to Security and Exchange Committee (SEC).

With regard to healthcare organizations, financial information includes patient direct payments for healthcare, health insurance and other health plan payments. As defined in HIPAA, individually identifiable health information refers to information, including demographic data that relates to "…the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual" [5]. It must be noted that the Sarbanes-Oxley Act does not explicitly discuss health information security in the text of the act. However, most modern accounting systems are computer-based and are often incorporated in health information systems. Accurate financial reporting depends on reliable and secure computing environments. Review or assessment of internal controls is not complete without mentioning information assurance or security. As such, information assurance professionals and other Information Technology (IT) professionals need to understand Sarbanes-Oxley Act to develop strategies to assist their organizations to comply with SOX [8] . SOX requirements indirectly compel management to consider information security controls on systems across the organization in order to comply.

Moreover, the act created the Public Company Accounting Oversight Board (PCAOB) to assist in the implementation and oversight of Sarbanes-Oxley Act. The board guides and oversees auditors as they assess a company's compliance with SOX. PCAOB created Proposed Auditing Standard to provide detailed guidance in the assessment process. In a release, PCAOB stated this:

> *Determining which controls should be tested, including controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include: …Controls, including information technology general controls, on which other controls are dependent* [9].

In essence, this statement asserts that information technology (IT) general controls form the foundation for many other types of financial reporting controls and therefore, must be assessed for SOX.

The requirements are quite hard to implement. In the first place, security best practices are not well defined in the act. Also, some organizations have budget constraints to enable them to implement the needed security technologies. This also goes in line with obtaining the right security expertise. Hence difficulties in deploying and managing required technology come as a result [7].

5. Health Information Technology for Economic and Clinical Health (HITECH)

On February 17, 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), was signed into law. The aim was to promote the adoption and meaningful use of electronic health record (EHR) technology. Privacy and security concerns associated with the electronic transmission of health information are addressed by Section D of the act [10]. HITECH responded to the increased public awareness and debate over the regulations made by the HIPAA Privacy and Security Rules. HIPAA Security and Privacy provisions and penalties, under HITECH, are applied directly to business associates of covered entities. Hitherto, the provisions and penalties were applied to business associates through contractual provisions with covered entities. Business associates are required to restrict the use and disclosure of protected health information. In default, like covered entities, they shall be subjected directly to the civil and criminal penalties for violating HIPAA regulations [11].

HITECH Act imposes more stringent regulatory requirements than the Security and Privacy Rules of HIPAA. It also increases the severity of penalties for a violation of HIPAA and provides funding and incentives for hospitals and physicians for the adoption of health information technology. The breach notification process was also expanded as new conditions and penalties for noncompliance were also stipulated. For instance, in times of breach, covered entities shall notify victims within sixty days after the discovery of the breach. In the case where covered entity does not have contact information of victims, breach must be posted on their website or make media notifications (local). If more than 500 people are affected by the breach, state media and government notifications are required [10, 11].

In relation to the adoption of Electronic Health Record (EHR) systems, where almost all protected health information (PHI) are digital, patients become more vulnerable to scams and other threats. HITECH thus establishes protocols and certifications for health information products. The protocol refers to the process of notifying breaches. Certification program is handled by the National Institute of Standards and Technology. EHR systems are also required to use some form of encryption technology to render PHI "unusable, unreadable, or indecipherable" to unauthorized individuals. Practitioners must destroy all unencrypted PHI after use [10].

Other new requirements of HITECH include [10,11]:

- Covered entities must honor an individual's request that information be withheld from health plan providers if care is paid for in cash.
- Covered entities must be capable of providing a 3-year audit trail of patient health information disclosures upon request.
- Covered entities may not receive payment for communicating with patients for marketing purposes without the specific authorization of the patient (including fundraising, solicitations, etc.).
- Employees of covered entities or other individuals who knowingly access, use, or disclose PHI for improper purposes will be subject to criminal penalties.
- Civil penalties for violations under HIPAA are increased, depending on the conduct.

6. Control Objectives For Information And Related Technology (COBIT)

COBIT is a framework created by Information Systems Audit and Control Association (ISACA) for IT management and IT Governance. The first version was released in 1995 with the latest version being COBIT 5. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. With COBIT, organizations are able to develop policy and good practice for IT control throughout organizations. It stresses on regulatory compliance, assists organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. Globally, COBIT is used by those with primary responsibilities for business processes and technology, those who depend on technology for relevant and reliable information and control of information technology [12].

ISACA strives to underscore the importance of technology in business processes and the need for management to appreciate it. ISACA also asserts that, in determining the appropriate technology to use and how to control its use, management needs to understand the risks and constraints in order to make good business decisions.

COBIT has four domains which include Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate. Thirty-four (34) IT processes are categorized under these four domains. COBIT covers security in addition to all the other risks that can occur with the use of IT. Although one out of the 34 processes is specifically devoted to security, control objectives that address security are scattered throughout the various processes in each domain [13]. COBIT requires deep expert knowledge to implement each application because of its generic nature. Although the guideline of security management is also published, its content is abstract [14].

The process devoted to security is called Ensure Systems Security which is defined under Deliver and Support domain. Ensure Systems Security provides security guidance on the following [13]:

- Manage Security Measures
- Identification, Authentication and Access
- Security of Online Access to Data
- User Account Management
- Management Review of User Accounts
- User Control of User Accounts
- Security Surveillance

IT professionals designing health information systems can follow the guidance provided in COBIT to ensure security.

7. ISO/IEC 27002 2005

Previously known as ISO/IEC 17799:2000, ISO/IEC 27002 2005 is a standard that can be applied to general information security management. In other words, it demonstrates what can be done to protect an organization's information assets. When ISO/IEC 17799:2000 was officially published on June 15, 2005, it was known as ISO IEC 17799 2005. On July 1, 2007, the name was formally changed to ISO IEC 27002 2005. However, much of its content is the same with some sections added [15].

As stated in the official title page ISO 27002 is a "code of practice for information Security Management". Any organization seeking to adopt a comprehensive information security management program or improve its existing information security practices can use the standard. Although ISO/IEC recommends a complete consideration of the practices, organizations do not have to implement every recommended security practice stated therein. The important thing is to know what works best for the unique information security risks and requirements. The ISO standard asserts that information can be protected using a wide variety of controls. Such controls include hardware and software functions, procedures, policies, processes and organizational structures. Organizations including healthcare organizations, must develop, implement, monitor, evaluate and improve these types of security controls [15].

8. Common Security Framework (CSF)

Released in March 2009, CSF was established by The Health Information Trust Alliance (HITRUST) in collaboration with healthcare, technology and information security leaders. Organizations that create, access, store or exchange personal health and financial information can use

Table 1 Laws and Standards for health Information Security and Privacy

Law/Standard	Subject	Date	References	Description
The Freedom of Information Act	Acquiring information from federal agencies	1966	[2]	Provides the American public the right to acquire information from federal agencies with some exceptions, which includes health information.
The Privacy Act of 1974	Patient confidentiality	1974	[2]	Required federal operated health facilities to protect the confidentiality of patients' medical records.
HIPAA	Health care security and privacy	August 21, 1996	[5]	To protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
Sarbanes-Oxley Act	Financial reporting	2002	[7]	Improves the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes
HITECH	Health information system	February 17, 2009	[11] [10]	To promote the adoption and meaningful use of health information technology.
COBIT	Risk management	1995	[12]	Framework for IT management and governance
ISO 27002	Information security management	July 1, 2007	[15]	Code of practice for information Security Management
CSF	Health information security	March 2009	[17]	Provides the needed structure, detail and clarity that pertains to information security that is tailored to the healthcare industry.

CSF which is the first IT security framework developed specifically for healthcare information [16]. Organizations benefit in terms of the needed structure, detail, and clarity that pertains to information security that is tailored to the healthcare industry. With the help of prescriptive set of controls and supporting requirements, organizations are able to meet the objectives of the framework. CSF leverages and cross-references existing standards and regulations helping to avoid the introduction of redundancy and ambiguity into the industry. By normalizing the security requirements of healthcare organizations including federal, state and other standards, CSF helps organizations to easily understand their compliance status across a wide range of authoritative sources and standards [17].

CSF is organized into two components:
Information Security Control Specifications Manual: It is best-practice-based specification that provides prescriptive implementation guidance. It entails recommended security governance practices and security control practices to ensure the effective and efficient management of information security.
Standards and regulations mapping: A reconciliation of the framework to common and different aspects of generally adopted standards and regulations. The CSF includes 42 control objectives and 135 control specifications based on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 standards [17]

CSF can only be accessed by subscribing to HITRUST Central, the managed online community for healthcare information security professionals. Standard subscriptions at no charge are available to individuals from qualifying organizations as defined by HITRUST. The online, interactive version of the CSF, authoritative sources and the CSF Assurance Kit is available only through a paid subscription [17].

9. Conclusion

A number of laws and standards exist to ensure the security and privacy of health information. This paper provides an overview of U.S. laws such as HIPAA, Sarbanes-Oxley Act and HITECH, as well as standards such as COBIT, ISO/IEC 27002 2005 and CSF. These laws and standards can be summarized in Table 1.

Although standards such as COBIT and ISO 27002 2005 are generic in nature, healthcare organizations can implement them to achieve security and privacy of health information as required by federal laws such as HIPAA and HITECH. However, healthcare providers, health plans, business associates and all other covered entities shall only reap the benefits if these standards are implemented properly. Drastic steps must also be taken to comply with all the rules and regulations required by laws. Security is everyone's business, as such, all parties in an organization should be

involved in playing their roles in securing health information.

Acknowledgements

This work is partially supported by NSF under grant HRD-1137516, and by Department of Education under grant P120A090049. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation and Department of Education

References

[1] Ruoyu Wu, Gail-Joon Ahn, and Hongxin Hu, "Towards HIPAA-Compliant Healthcare Systems," in *Proceedings. of* the *2nd ACM SIGHIT International Health Informatics Symposium*, Miami, 2012, pp. 593-602.

[2] Karen A. Wager, Frances W. Lee, and John P. Glaser, *Health Care Information Systems: A Practical Approach for Health Care Management*, 2nd ed., John Wiley & Sons, Inc., 2009.

[3] Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin (Eds.). Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, National Academies Press, 2009, Washington DC, US.

[4] Alan R. Heminger and John Chessman, "A Study of U.S. Battlefield Medical Treatment/Evacuation. Compliance with HIPAA Requirements," in *Proceedings of the 42nd Hawaii International Conference on System Sciences*, Hawaii, 2009.

[5] Office of Civic Rights. (2003, May) Department of Human & Health Sciences. Accessed on April 2012, Availabe at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[6] Charles A. Shoniregun, Kudakwashe Dube, and Fredrick Mtenzi, *Electronic Healthcare Information Security*. New York: Springer Science+Business Media, LLC, 2010.

[7] SOX-Online. (2006) SOX Online. [Online]. HYPERLINK "http://www.sox-online.com" http://www.sox-online.com

[8] Greg Stutts. (2004, May) SANS Institute InfoSec Reading Room. [Online]. HYPERLINK "http://www.cs.jhu.edu/~rubin/courses/sp06/Reading/soxForInfoSec.pdf" http://www.cs.jhu.edu/~rubin/courses/sp06/Reading/soxForInfoSec.pdf

[9] PCAOB. (2004) Public Company Accounting Oversight Board. [Online]. HYPERLINK "http://pcaobus.org/Rules/Rulemaking/Docket008/2004-03-09_Release_2004-001-all.pdf" http://pcaobus.org/Rules/Rulemaking/Docket008/2004-03-09_Release_2004-001-all.pdf

[10] Eric M. Johnson and Nicholas Willey, "Will HITECH Heal Patient Data Hemorrhages?," in *IEEE, System Sciences (HICSS), 2011 44th Hawaii International Conference*, Kauai,Hawaii, 2011, pp. 1-10.

[11] Linn Foster Freedman. (2009, February) The Health Information Technology for Economic and Clinical Health Act (HITECH Act): implications for the adoption of health information technology, HIPAA, and privacy and security issues. [Online]. HYPERLINK "http://www.nixonpeabody.com/publications_detail3.asp?ID=2621" http://www.nixonpeabody.com/publications_detail3.asp?ID=2621

[12] ISACA. (2011) Information Systems Audit and Control Association. [Online]. HYPERLINK "http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx" http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[13] Carol Woodbury. (2004) SkyView Partner. [Online]. HYPERLINK "http://www.skyviewpartners.com/pdf/COBIT_Security.pdf" http://www.skyviewpartners.com/pdf/COBIT_Security.pdf

[14] Shoichi Morimoto, "Application of COBIT to Security Management in Information Systems Development," in *Proceedings of the Fourth International Conference on Frontier of Computer Science and Technology*, Shanghai , 2009, pp. 625-630.

[15] PRGL. (2011, December) Praxiom Research Group Limited. [Online]. HYPERLINK "http://www.praxiom.com/iso-17799-intro.htm" http://www.praxiom.com/iso-17799-intro.htm

[16] Solutionary. (2012, March) Solutionary. [Online]. HYPERLINK "http://www.solutionary.com/index/compliance/security-frameworks.php" http://www.solutionary.com/index/compliance/security-frameworks.php

[17] HITRUST. (2012, March) Health Information Trust Alliance. [Online]. HYPERLINK "http://www.hitrustalliance.net/csf/" http://www.hitrustalliance.net/csf/