

**Security Issues in Healthcare Information Communication:
A Comprehensive Review of the Health Care Portability and Accountability Act
(HIPAA 1996)**

by

Mike Zaccaro
School of Business Administration
University of North Carolina at Pembroke
michael.zaccaro@uncp.edu

and

Ramin Cooper Maysami^{*}
School of Business Administration
University of North Carolina at Pembroke
One University Drive, P.O. Box 1510
Pembroke, NC 28374
USA
Tel: 910-987-2311
Fax: 910-235-0204
e-mail: ramin.Mysami@uncp.edu

submitted to:

Preliminary Version: Please do not quote or reproduce

* Corresponding Author.

Security Issues in Healthcare Information Communication: A Comprehensive Review of the Health Care Portability and Accountability Act

I. Introduction

The Department of Health and Human Services (HHS), Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, Insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected.

The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information.

Health Insurance Reform: Security Standards
Office of the Secretary
Department of Health and Human Services
United States of American

Internet technology has enabled health professionals to obtain and share increased amounts of health care information in order to track and monitor diseases, contend Chew, et. al. (2004), whose survey of the medical literature shows that “increasingly, physicians use on-line databases to search for the latest information on clinical protocols in different medical specialties and patient management and to consult with specialists and seek continuing medical education.” Additionally, “the Internet has allowed physicians throughout the world to collaborate, communicate, and interact.” Chew, et. al (2004) continue, “The Internet is of increased importance in the practice of family medicine as a consequence of the efficiency of communications, the accessibility of on-line evidence-based medicine reviews, and the need to assist patients in selecting reliable Internet resources.”¹

¹ Chew, F. W. G. Grant, and R. Tote “Doctors On-line: Using Diffusion of Innovations Theory to Understand Internet Use” Medical Informatics Vol. 36, No. 9: 645-650. Available at <http://www.stfm.org/fmhub/fm2004/October/Fiona645.pdf>

According to an American Medical Association (AMA) survey recounted by the Electronic Information Report, “70% of doctors used the Web compared to just 20% a year earlier, with 25% stating they used e-mail to communicate with their patients. According to the same report, “online Continuing Medical Education (CME) has also experienced a major boost. Medscape reported 45,500 hours of CME usage on its Web site in the first quarter of 2001, a 20% increase from the previous quarter and a 136% increase from the first quarter of 2000.”²

This, of course is in line with the inevitable penetration of our daily lives by the power of the Internet. eHealth may soon be a term readily found in any dictionary! Rapid development of this type inevitably begets directive and guidelines, and the regulators of the US healthcare industry have been quick to act. “To improve the efficiency and effectiveness of the health care system, the US Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which included a series of ‘administrative simplification’ provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions.”³

The immediate action of the HSS after the enactment of HIPAA was to implement a number of provisions to address the regulatory issues relating to privacy, electronic transactions code sets, national identifier requirements for employers, providers, and health plans, and of course, security rules. The Privacy Rule set April 14, 2003 as the deadline for compliance with privacy requirements that govern the use and disclosure of protected health information (PHI) except for small health plans, which had an April 14, 2004 deadline).⁴ The Electronic

² “Government Pushes Healthcare Industry to Adopt Internet”, *Electronic Information Report*, 10760490, 05/25/2001, Vol. 22, Issue 19

³ Guidance on Compliance with HIPAA Transactions and Code Sets (After the October 16, 2003 implementation deadline). Available at <http://hipaa.dhs.ca.gov/pdf/CMSSguidance-final.pdf>.

⁴ (Protected health information, or “PHI”, is defined at 45 CFR § 160.103, which can be found on the OCR website (<http://hhs.gov/ocr/hipaa>).

Transactions and Code Sets Rule, in turn, required all covered entities to be in compliance with the electronic transactions and code sets standard formats as of October 16, 2003.

The National identifier requirements for employers, providers, and health plans selected the Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), as the identifier for employers. Covered entities were to use this identifier effective July 30, 2004, except for small health plans, which have until August 1, 2005. The National Provider Identifier (NPI) was adopted as the standard unique health identifier for health care providers. The Final Rule became effective May 23, 2005. Providers may apply for NPIs on or after that date. The NPI compliance date for all covered entities, except small health plans, is May 23, 2007; the compliance date for small health plans is May 23, 2008. The health plan identifier rule is expected in the coming years.

And Finally, the Security Rule required all covered entities to be in compliance no later than April 20, 2005, except small health plans, which, must comply no later than April 20, 2006. The provisions of the Security Rule apply to electronic protected health information (EPHI).

The law, then, is clear: October 16, 2003 was the deadline for covered entities to comply with HIPAA's electronic transaction and code sets provisions. After that date, covered entities, including health plans, may not conduct noncompliant transactions.

Just before the October 2003 HHS has received a number of inquiries expressing concern over the health care industry's state of readiness. In response, the Department believed it was particularly important to outline its approach to enforcement of HIPAA's electronic transactions and code sets provisions.”⁵

⁵ Guidance on Compliance with HIPAA Transactions and Code Sets (After the October 16, 2003 implementation deadline). Available at <http://hipaa.dhs.ca.gov/pdf/CMSguidance-final.pdf>.

The remainder of the current report is organized as follows: Section II introduces HIPAA and its several aims and scopes—security of healthcare information being one of them. Section III confirms the need for security of information in the healthcare industry, and describes security goals and objectives. Section IV reproduces HIPAA Administrative Simplification related to Security and Electronic Signatures as proposed by the Center for Medicare and Medicaid Services of the United States’ Department of Health and Human Services. Next, Security Standards are covered in depth in Section V and Electronic Signature Standards in Section VI. Section VII introduces the reader to the National Institute of Standards and Technology’s “Introductory Resource Guide for Implementing the HIPAA Security Rule. And finally, section VIII discusses HIPAA-related issues such as lack of compliance and provides example of helpful suggestions offered in the literature⁶

II. Back to the Basics: What is HIPAA?

The Center for Medicare and Medicaid services (CMS) responsible for implementing various unrelated provisions of the act acknowledges that HIPAA may mean different things to different people.⁷

Blue Cross Blue Shields of North Carolina, for example, defines the Health Insurance Portability and Accountability Act (HIPAA) as “a federal health benefits law passed in 1996, effective July 1, 1997, which among other things, restricts pre-existing condition exclusion periods to ensure portability of health-care coverage between plans, group and individual;

⁶ The authors would like to thank Ms. Joan Hash for granting us the permission to use the material in the Resource Guide.

⁷ <http://www.cms.hhs.gov/hipaa/>

requires guaranteed issue and renewal of insurance coverage; and prohibits plans from charging individuals higher premiums, co-payments, and/or deductibles based on health status.”⁸

AnswerStat.com, on the other hand, defines HIPAA: as the Act, “which among other things addresses the privacy of health information and has wide-ranging ramifications to the medical community in general and medical call centers specifically.”⁹.

According to Administrative Services of Kansas, Inc (ASK), “HIPAA is a Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment or relationships. It also gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.”¹⁰

TriWest Healthcare Alliance believes HIPAA was introduced “to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance; and for ‘other purposes’.”¹¹

SearchCIO.com emphasizes that there are two sections to the Act. “HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section, which deals with the standardization of

⁸ <http://www.bcbsnc.com/apps/glossary/all.do?index=H>

⁹ <http://www.answerstat.com/articles/glossary.html#h>

¹⁰ <http://www.ask-edi.com/glossary.htm#wordH>

¹¹ https://www.triwest.com/triwest/default.html?triwest/unauth/content/provider/handbook/provider/pro_glossary_of_terms.html

healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to this Act. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.” Additionally, “HIPAA seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data. The Act mandates: standardized formats for all patient health, administrative, and financial data; unique identifiers (ID numbers) for each healthcare entity, including individuals, employers, health plans and health care providers; and security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.¹²

The Center for Medicare and Medicaid Services, finally, identifies its own business activities with regard to HIPAA as (1) Health Insurance Reform explained in Title I of the HIPAA Act of 1996, and HIPAA Title II--Administrative Simplification. Health Insurance Reform protects health insurance coverage for workers and their families when they change or lose their jobs. It governs the rules regarding pre-existing conditions and portability of health insurance coverage.¹³ The Administrative Simplification provisions require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. “Adopting these standards will improve the efficiency and effectiveness of the nation’s health care system by encouraging the widespread use of electronic data interchange in health care.”¹⁴ Figure 1 depicts all components of HIPAA with an exaggerated focus on “security” provisions of the statute, the focal point of the current study.

{Insert [Figure 1](#) Here}

¹² http://searchcio.techtarget.com/sDefinition/0,,sid19_gci862786,00.html

¹³ <http://www.cms.hhs.gov/hipaa/hipaa1/default.asp>

¹⁴ <http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>

III. Why Security?

The Department Of Health and Human Services and Center for Medicare and Medicaid Services emphasize that prior to HIPAA, there were no generally accepted set of security standards or general requirements for protecting health information in the health care industry.¹⁵ At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of computers to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

For example, in order to provide more efficient access to critical health information, covered entities have begun to use web-based applications and other “portals” that gives physicians, nurses, medical staff as well as administrative employees more access to electronic health information. Providers are also using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are now providing access to claims and care management, as well as a member of self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies creates an increase in potential security risks.

According to the CMS, “As the country moves towards its goal of a National Health Information Infrastructure (NHII), and greater use of electronic health records, protecting the confidentiality, integrity, and availability of EPHI becomes even more critical. The security standards in HIPAA were developed for two primary purposes. First, and foremost, the

¹⁵ See Security 101 for Covered Entities, available at http://www.cms.hhs.gov/hipaa/hipaa2/education/Security%20101_Cleared.pdf

implementation of appropriate security safeguards protects certain electronic health care information that may be at risk. Second, protecting an individual's health information, while permitting the appropriate access and use of that information, ultimately promotes the use of electronic health information in the industry – an important goal of HIPAA.”¹⁶

Brenner (2005) of SearchSecurity.com believes that HIPAA's security requirements affect companies that store and transmit protected health information electronically. This includes healthcare providers, insurers and clearinghouses. Enterprises that serve clients in the healthcare industry, laboratories, collection agencies and lawyers, for example, must also implement protections to secure the information, Brenner (2005) contends. “There's no cookie-cutter approach for everyone. The standards don't specify any particular technology to adopt. They outline what must be done, not how to do it,” emphasizes Brenner (2005). He continues, “Organizations trying to figure out how to apply the standards must take into account their size, complexity, capabilities, compliance costs and the potential risks to their electronically protected health information.”

Security Rule Goals and Objectives

Pursuant to “Security standards: General rules” section of the HIPAA Security Rule¹⁷, each covered entity must (1) ensure the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) that it creates, receives, maintains, or transmits, (2) protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI, and (3) protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

¹⁶ http://www.hipaadvisory.com/Action/Security/CMS_Series/Security101.pdf

¹⁷ See 45 C.F.R. § 164.306(a).

“Generally speaking, HIPAA security requires that: (a) Administrative safeguards be in place to manage the selection and execution of security measures; (b) Physical safeguards be in place to protect electronic systems and related buildings and equipment from environmental hazards and unauthorized intrusion; (c) Technical safeguards be in place, including an automated processes to protect data and control access to it; (d) Risk assessments are conducted and that security policies and procedures are documented, and (e) Organizations have a device to screen traffic from the Internet such as a firewall,” Brenner (2005) asserts.¹⁸

IV. Overview of HPPA Administrative Simplifications

This section reproduces the HIPAA Administrative Simplification related to Security as proposed by the Center for Medicare and Medicaid Services, of the United States’ Department of Health and Human Services. “The final rule, published in the Federal Register on February 20, 2003, specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information.” It may be viewed at <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>.

A. Background¹⁹

In order to administer their programs, the Department of Health and Human Services, other Federal agencies, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (such as patients, insured, providers, and health care plans) that the confidentiality and privacy of health care information they

¹⁸ Brenner, B, “HIPAA security rules broken down,” *SearchSecurity.com*, 15 March 2005, available at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1067095,00.html

¹⁹ Please see CMS’s “The Health Insurance Portability and Accountability Act of 1996—Administrative Simplification > Regulations > Security > Proposed Rule” (Last Modified on Friday, September 17, 2004) at <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec01.asp>

electronically collect, maintain, use, or transmit is secure. Security of health information is especially important when health information can be directly linked to an individual. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

In addition to the need to ensure electronic health care information is secure and confidential, there is a potential need to associate signature capability with information being electronically stored or transmitted. Today, there are numerous forms of electronic signatures, ranging from biometric devices to digital signature. To satisfy the legal and time-tested characteristics of a written signature, however, an electronic signature must do the following:

- Identify the signatory individual;
- Assure the integrity of a document's content, and
- Provide for non-repudiation, that is, strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid. Currently, the only technically mature electronic signature meeting the above criteria is the digital signature. There is no national standard for security or electronic signatures. Of necessity, each health care provider, health care plan, and health care entity has defined its own security requirements.

B. Legislation²⁰

The Congress included provisions to address the need for security and electronic signature standards and other administrative simplification issues in the Health Insurance Portability and Accountability Act of 1996, which was enacted on August 21, 1996. Through subtitle F of title II of that law, the Congress added to title XI of the Social Security Act a new part C, entitled “*Administrative Simplification.*” (Public Law 104-191) The purpose of part C is to improve the Medicare and Medicaid programs, in particular, and the efficiency and

²⁰ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec01.asp>

effectiveness of the health care system, in general, by encouraging the development of a health information system through the establishment of standards and requirements to facilitate the electronic maintenance and transmission of certain health information.

Part C of title XI of the Act consists of sections 1171 through 1179. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and certain health care providers concerning electronic transmission of health information.

- Section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.
- Section 1172 of the Act makes any standard adopted under part C applicable to (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form (in connection with the transactions referred to in section 1173(a)(1) of the Act).

The security standard to be adopted under Part C is not restricted to the transactions referred to in section 1173(a)(1) of the Act, but is applicable to any health information pertaining to an individual that is electronically maintained or transmitted.

This section also contains the following requirements concerning standard setting:

- The Secretary may adopt a standard developed, adopted, or modified by a standard setting organization (that is, an organization accredited by the American National Standards Institute (ANSI));
 - The Secretary may also adopt a standard other than one established by a standard setting organization, if the different standard will reduce costs for health care providers and health plans, the different standard is promulgated through negotiated rulemaking procedures, and the Secretary consults with each of the above-named groups.
 - If no standard has been adopted by any standard setting organization, the Secretary must rely on the recommendations of the National Committee on Vital and Health Statistics (NCVHS) and consult with each of the above-named groups
- Paragraph (a) of section 1173 of the Act requires that the Secretary adopt standards for financial and administrative transactions, and data elements for those transactions, to enable health information to be exchanged electronically.

Standards are required for the following transactions: health claims, health encounter information, health claims attachments, health plan enrollments and disenrollments, health plan eligibility, health care payment and remittance advice, health plan premium payments, first report of injury, health claim status, and referral certification and authorization.

- Paragraph (b) of section 1173 of the Act requires the Secretary to adopt standards for unique health identifiers for all individuals, employers, health plans, and health care providers and requires further that the adopted standards specify for what purposes unique health identifiers may be used.
- Paragraphs (c) through (f) of section 1173 of the Act require the Secretary to establish standards for code sets for each data element for each health care transaction listed above, security standards for health care information systems, standards for electronic signatures (established together with the Secretary of Commerce), and standards for the transmission of data elements needed for the coordination of benefits and sequential processing of claims.
- Generally, after a standard is established, it cannot be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard.

Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary must also ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

- Section 1175 of the Act prohibits health plans from refusing to process or delaying the processing of a transaction that is presented in standard format.
- Section 1176 of the Act establishes a civil monetary penalty for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than \$100 per person per violation and not more than \$25,000 per person for violations of a single standard for a calendar year. The procedural provisions in section 1128A of the Act, “Civil Monetary Penalties,” are applicable.
- Section 1177 of the Act establishes penalties for a knowing misuse of unique health identifiers and individually identifiable health information: (1) A fine of not more than \$50,000 and/or imprisonment of not more than 1 year; (2) if misuse is “under false pretenses,” a fine of not more than \$100,000 and/or imprisonment of not more than 5 years; and (3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years.

- Under section 1178 of the Act, the provisions of part C of title XI of the Act, as well as any standards established under them, supersede any State law that is contrary to them. However, the Secretary may, for statutorily-specified reasons, waive this provision.
- Finally, section 1179 of the Act makes the above provisions inapplicable to financial institutions or anyone acting on behalf of a financial institution when “authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.”

C. Process for Developing National Standards²¹

The Secretary has formulated a five-part strategy for developing and implementing the standards mandated under part C of title XI of the Act:

1. To ensure necessary interagency coordination and required interaction with other Federal departments and the private sector, establish interdepartmental implementation teams to identify and assess potential standards for adoption.

The subject matter of the teams includes claims/encounters, identifiers, enrollment/eligibility, systems security and electronic signature, and medical coding classification.

Another team addresses cross-cutting issues and coordinates the subject matter of teams.

2. *Develop recommendations for standards to be adopted;*
3. Publish proposed rules in the Federal Register describing the standards;
4. Analyze public comments and publish the final rules in the Federal Register;
5. Distribute standards and coordinate preparation and distribution of implementation guides

The implementation teams charged with reviewing standards for designation as required national standards under the statute have defined, with significant input from the health care industry, a set of principles for guiding choices for the standards to be adopted by the Secretary. These

²¹ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec01.asp>

principles are based on direct specifications in HIPAA, the purpose of the law, and generally desirable principles.

To be designated as an HIPAA standard, each standard should:

- i. Improve the efficiency and effectiveness of the health care system by leading to cost reductions for or improvements in benefits from electronic health care transactions;
- ii. Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses;
- iii. Be consistent and uniform with the other HIPAA standards--their data element definitions and codes and their privacy and security requirements--and, secondarily, with other private and public sector health data standards;
- iv. Have low additional development and implementation costs relative to the benefits of using the standard;
- v. Be supported by an American National Standards Institute's (ANSI)-accredited standards developing organization or other private or public organization that will ensure continuity and efficient updating of the standard over time;
- vi. Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster;
- vii. Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, except when they are explicitly part of the standard;
- viii. Be precise and unambiguous, but as simple as possible;
- ix. Keep data collection and paperwork burdens on users as low as is feasible;
- x. Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology

V. Security Standards²²

According to the American National Standards Institute's Healthcare Informatics Standards Board (ANSI HISB), "comprehensive adoption of security standards in health care, not piecemeal implementation, should be advocated to provide security to data that is exchanged between health care entities. There is, of course, no recognized single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and technical mechanisms) that must be in place to preserve health information confidentiality and privacy as defined in the law. Therefore, a new, comprehensive standard should be designed to define the security requirements to be fulfilled, after thoroughly researching the existing guidelines and standards, and consulting extensively with the organizations that developed them. Some requirements are:

- The standard must be comprehensive

By definition, if a system or communications between two systems, were implemented with technology(s) meeting standards in a general system security framework (Identification and Authentication; Authorization and Access Control; Accountability; Integrity and Availability; Security of Communication; and Security Administration.) that system would be essentially secure.

- The standard must be technology-neutral.

The standard should not reference or advocate specific technology because security technology is changing quickly. Flexibility should be afforded providers/plans/clearinghouses to choose their own technical solutions. A standard that is dependent on a specific technology or technologies would not be flexible enough to use future advances.

- The standard must be scalable.

The standard must be able to be implemented by all the affected entities, from the smallest provider to the largest clearinghouse. A single approach would be neither economically feasible nor effective in safeguarding health data.

²² Please see CMS's "The Health Insurance Portability and Accountability Act of 1996—Administrative Simplification > Regulations > Security > Proposed Rule" (Last Modified on Friday, September 17, 2004) at <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec05.asp>

A. General Approach

The CMS defines security standards as a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure. The implementation features address specific aspects of the requirements. The standard need not reference or advocate specific technology. This would allow the security standard to be stable, yet flexible enough to take advantage of state-of-the-art technology. It is not required that the standard address the extent to which a particular entity should implement the specific features. Instead, the CMS would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.

The recommendations contained in the National Research Council's 1997 report "For The Record: Protecting Electronic Health Information" similarly concluded that appropriate security practices are highly dependent on individual circumstances, but goes on to suggest that: "It is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities, risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another." Inherent in this approach is a balance between the need to secure health data against risk and the economic cost of doing so. Health care entities must consider both aspects in devising their security solutions.

B. Specific Requirements

Doherty (2004) draw attentions to the fact that “HIPAA’s security rules aim to be comprehensive, address all aspects of security and scale for large and small entities, and cover three areas: administrative, physical and technical safeguards. Administrative policies and procedures are the most vital and affect the physical and technical safeguards. Admin safeguards include security-awareness training for staff, procedures for reporting and responding to security incidents and developing contingency plans for disaster recovery.”²³

Each health care entity engaged in electronic maintenance or transmission of health information should assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures. Most importantly, these measures must be documented and kept current. The security standard consists of the requirements that a health care entity must address in order to safeguard the integrity, confidentiality, and availability of its electronic data. It also describes the implementation features that must be present in order to satisfy each requirement.

The security requirements, for purposes of presentation only, have been divided into the following four categories:

1. Administrative procedures to guard data integrity, confidentiality, and availability - these are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data (Table 1)
2. Physical safeguards to guard data integrity, confidentiality, and availability - these relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities (Table 2)

²³ Doherty, S. “Dissecting the Security Rules,” Network Computing (6/10/2004), Vol 15, Issue 11, Page 2. Available at <http://www.nwc.com/showitem.jhtml?docid=1511buyers>

3. Technical security services to guard data integrity, confidentiality, and availability - these include the processes that are put in place to protect and to control and monitor information access (Table 3) and
4. Technical security mechanisms - these include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network (Table 4).

C. Tabular presentation of the security requirements and Implementation

1. Administrative Procedures²⁴

The administrative requirements and supporting implementation features in the Rule are presented in Table 1. “Each requirement is to be documented, and documentation is to be made available to those individuals responsible for implementing the procedures ought to be reviewed and updated periodically.”

{Insert [Table 1](#) Here}

2. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability²⁵

The requirements and implementation features for physical safeguards are presented in Table 2. “Each requirement is to be documented, and documentation is to be made available to those individuals responsible for implementing the procedures ought to be reviewed and updated periodically.”

{Insert [Table 2](#) Here}

²⁴ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec06.asp>

²⁵ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec07.asp>

3. Technical Security Services to Guard Data Integrity, Confidentiality, and Availability²⁶

The proposed requirements and implementation features for technical security services are reported in Table 3. “each of these services should be implemented and documented. The documentation would be made available to those individuals responsible for implementing the services and would be reviewed and updated periodically.”

{Insert [Table 3](#) Here}

4. Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network²⁷

The requirements and implementation features for technical security mechanisms are recounted in Table 4. “Each of these mechanisms would need to be documented. The documentation would be made available to those individuals responsible for implementing the mechanisms and would be reviewed and updated periodically.”

{Insert [Table 4](#) Here}

VI. Electronic Signature Standard²⁸

HIPAA directs the Secretary of the Department of Health and Human Services to coordinate with the Secretary of the Department of Commerce in adopting standards for the electronic transmission and authentication of signatures with respect to the transactions referred to in the law. This rule was developed in coordination with the Department of Commerce’s National Institute of Standards and Technology. We propose to adopt a cryptographically based digital signature as the standard.

²⁶ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec08.asp>

²⁷ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec09.asp>

²⁸ <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/sec10.asp>

Whenever a HIPAA specified transaction requires the use of an electronic signature, the standard must be used. It should be noted that an electronic signature is not required for any of the currently proposed standard transactions.

In the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data. Use of an electronic signature refers to the act of attaching a signature by electronic means. The electronic signature process involves authentication of the signer's identity, a signature process according to system design and software instructions, binding of the signature to the document and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature. Table 5 presents the electronic signature requirements.

{Insert [Table 5](#) Here}

Various technologies may fulfill one or more of the electronic signature requirements specified in Table 5. Authentication systems (passwords, biometrics, physical feature authentication, behavioral actions and token-based authentication) can be combined with cryptographic techniques to form an electronic signature. However, a complete electronic signature system may require more than one of the technologies mentioned above. If electronic signatures would be used, certain implementation features must be included, specifically, message integrity, non-repudiation and user authentication.

Currently there are no technically mature techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. Therefore, if electronic signatures are employed, we would require that digital signature technology be used. A digital signature is formed by

applying a mathematical function to the electronic document. This process yields a unique bit string, referred to as a message digest. The digest (only) is encrypted using the originator's private key and the resulting bit stream is appended to the electronic document.

The recipient of the transmitted document decrypts the message digest with the originator's public key, applies the same message hash function to the document, then compares the resulting digest with the transmitted version. If they are identical, then the recipient is assured that the message is unaltered and the identity of the signer is proven. Since only the signatory authority can hold the Private Key used to digitally sign the document, the critical feature of non-repudiation is enforced.

VII. An Introductory Resource Guide for Implementing the HIPAA Security Rule²⁹

All that was discussed above may seem overwhelming, and it really is, considering that covered organization are additionally responsible for compliance with HIPAA's Privacy- and the National Transaction Code Set Rules, in addition to the above-mentioned security provisions.

Help has arrived, thankfully, in the form of Special Publication 800-66—a set of guidelines issued by National Institute of Standards and Technology (NIST) for complying with the Health Insurance Portability and Accountability Act's Security Rule.³⁰ NIST is the agency responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets.

²⁹ The authors would like to thank Ms. Joan Hash for granting us the permission to use the material in the Resource Guide.

³⁰ Hash, J., Bowen, P., Johnson, A., Smith, C. D. and Steinberg, D. I., "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Special Publication 800-66)," *National Institute of Standards and Technology, Technology Administration, US Department of Commerce*. Available at <http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf>.

Special Publication 800-66 was developed by the Computer Security Division (CSD) of NIST's Information Technology Laboratory (ITL), pursuant to its mission regarding the development of guidance for IT security planning, implementation, management, and operation. Specifically, it is to (1) assist with implementation of the Security Rule, (2) provide a brief summary on each standard, (3) identify available NIST publications which can be used as resources, (4) and aid in understanding general security concepts (Help educate).

The stated purpose of the publication is “to help educate readers about the security standards included in the HIPAA Security Rule. The document is also designed to direct readers to helpful information in other NIST publications on security topics included in the HIPAA Security Rule. Readers can draw upon these publications for consideration in implementing the Security Rule,” during security program development life cycle.

The life cycle phases include planning of security controls and policies, implementation of security controls, assessment of the security of an IT system or program, and technical and IT infrastructure guidance. Figure 2 identifies NIST publications that may be most helpful to an organization seeking more information on security-related issues in various development stages shown below.

{Insert [Figure 2](#) Here}

Identified by Franklin (2005) as “a combination of painfully obvious and truly useful information,” SP 800-66 “provides excellent guidance, including, for instance, tables showing activity categories, their descriptions and a series of “getting started” questions. It also provides listings that differentiate mandatory provisions from recommended activities to help enterprises prioritize the process. The publication also offers examples of acceptable ways to meet HIPAA

requirements—“the kind of information for which consultants charge big bucks,” according to Franklin (2005).³¹

Two sample templates available in SP 800-66 are reproduced in this section as Tables 6 and 7. Table 6 presents key activities, description and sample questions to help organizations “assign security responsibilities.

{Insert [Table 6](#) Here}

Table 7 presents a sample template for the transmission security requirement.

{Insert [Table 7](#) Here}

VIII. Discussions and Conclusions

Phoenix Health Systems and Healthcare Information and Management Systems Society (HIMSS) conducted the “Winter 2005 U.S. Healthcare Industry HIPAA Compliance Survey” from January 4 to January 20, 2005 with a sample of 400 healthcare industry representatives consisting of 80% Providers (Hospitals with 400+ beds: 25%, Hospitals with 100-400 beds: 17%, Hospitals with less than 100 beds: 14%, Medium-sized physicians practices (11 to 29 physicians)/other providers: 7%, and Small physicians practices (10 or fewer physicians)/other providers: 17%) and 20 percent Payers (Covering fewer than 150,000 lives: 8%, Covering 150,000-500,000 lives: 4%, Covering 501,000-1,500,000 lives: 4%, and Covering more than 1,500,000 lives: 4%).³²

The respondents reported similar “roadblocks” to overall HIPAA Compliance. “Achieving successful integration of new systems, policies, and procedures across the

³¹ Franklin, C. “Federal Government Finally Issues HIPAA Compliance Rules,” *Network Computing*, April 2005. Available at <http://www.nwc.com/showArticle.jhtml?articleID=160911499#>.

³² The authors would like to thank the Phoenix Health Systems for granting us the permission to report the result of the survey.

enterprise” ranked as the primary impediment to HIPAA compliance for the second consecutive year. “Interpretation of HIPAA regulations” ranked second, “budget constraints” ranked third, and “time constraints” ranked fourth. Comments from respondents indicated that many feel CMS has not provided adequate guidance regarding interpretation and implementation of the Security regulations.

Specifically, the results of Phoenix Health Systems’ HIPAA Security Compliance survey revealed the following:

- Thirty percent (30%) of Payers (up from 13% in June 2004) and only 18% of Providers indicate that they were compliant with the HIPAA Security Regulations.
- The number of organizations that expected to be fully compliant by April 2005 had actually declined over the previous six months. Only 74% of Providers (down from 87%), and 80% of Payers (down from 91%), indicated they would be compliant on or before the deadline;
- Ninety-three percent (93%) of Providers and 98% of Payers had designated an individual as the organizational Security Officer; and
- Forty percent (40%) of Providers and 26% of Payers indicated that their organizations had experienced at least one data security breach in the past six months.

Many initial implementation obstacles were internal in nature, such as obtaining management support for HIPAA initiatives, or mounting campaigns to increase staff awareness of issues and requirements. Further along the road, the problems were more external, with collaborative difficulties arising among industry trading partners as each struggled with various components of the TCS requirements.

Providers and Payers differed only slightly in their assessment of which HIPAA Security standards were most difficult to implement. Providers list Audit Controls (55%), Risk Management/Risk Analysis (49%), Information System Activity Review (48%), and Data Backup Plan/Disaster Recovery Plan/Emergency Mode Operation Plan (39%) as the major

roadblocks to HIPAA compliancy, while payer listed Information System Activity Review (40%), Risk Management/Risk, Analysis (34%), Audit Controls (32%), and Data Backup Plan/Disaster Recovery Plan/Emergency Mode Operation Plan (29%).

Although overall Security compliance does not appear imminent – the average number of organizations that are currently compliant with the Security Regulations is only 24% – Winter 2005 survey results demonstrate that organizations are making progress in two important areas of Security compliance. Ninety-three percent (93%) of Providers and 98% of Payers have designated an individual as the Security Officer/Official. Thirty-two percent (32%) of Provider organizations have already conducted required HIPAA Security training – with an additional 60% expecting to finish prior to the deadline. Thirty-seven percent (37%) of Payer organizations have already conducted the required HIPAA Security training – with an additional 58% expecting to finish prior to the deadline.

Harman (2005) believes that “HIPAA and the final Privacy Rule have led to the application of sophisticated technologies for controlling access to personal health information.” These include the identification and authentication of individuals authorized to access information and the establishment of audit trails of those accessing and/or modifying information at the different levels of access (Institute for Health Care Research and Policy, 1999; U. S. DHHS, 2003)³³.

There are real incentives to be compliant, not the least of which is to avoid penalties, which can be severe, Harman (2005) points out. Tomes (2000) asserts that failure to conform to the HIPAA Privacy Rule could result in either civil or criminal penalties as high as \$250,000

³³ Institute for Health Care Research and Policy. Health Privacy Project. (1999). Exposed: A health privacy primer for consumers. Retrieved January 26, 2005 from www.healthprivacy.org/usr_doc/34775.pdf.

and/or prison terms of 10 years for those who sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.³⁴ If a patient suffers serious injury from the violation, the penalties could increase to 20 years imprisonment or life if the patient dies (U.S. DHHS and Department of Justice Health Care Fraud and Abuse Control Program, 2003; Office of Civil Rights, 2005; Prophet 1997)³⁵.

According Harman (2005), “Implementation of HIPAA is a process, not a defined outcome that is finished on a certain date in time. As with all complex legislation, there must be an ongoing process of education, implementation, and monitoring which requires an assessment of the interrelatedness of the system factors and identification of problems that must be fixed. It will take a few more years before we can substantiate that this legislation is part of our health care culture.” She continues, “the Privacy Rule affects both handwritten and electronic documentation, and its implementation is just the first stage in a process that will be unfolding for many years. The emerging electronic health medical record must, in fact, accommodate the rules and regulations related to HIPAA.”³⁶

In conclusion, it is worthwhile to note Kibbe (2005) proposed 10 steps to HIPAA security compliance:³⁷

1. Understand why computer security is important;
2. Make certain your colleagues and staff take security as seriously as you do;
3. Catalog all the information system components that interact with protected health information in your office;

³⁴ Tomes, J. (2000). HIPAA’s privacy and security regulations: Administrative complication, not simplification. *Health Law Digest* 28(1), 14.

³⁵ U.S. Department of Health and Human Services and Department of Justice Health Care Fraud and Abuse Control Program. (2003). *Annual report for 2002*. Retrieved April 20, 2005 from <http://www.usdoj.gov/dag/pubdoc/hcfacreport2002.htm>

³⁶ Harman, L., (May 31, 2005). “HIPAA: A Few Years Later,” *Online Journal of Issues in Nursing*. Vol.10 No.2 Available at: www.nursingworld.org/ojin/topic27/tpc27_2.htm

³⁷ Kibbe, D. C., “10 steps to HIPAA security compliance,” *Family Practice Management*; Apr2005, Vol. 12 Issue 4, p43, 7

4. Prepare for disaster before it occurs;
5. Make sure your network and communications safeguards are intact and robust;
6. Be certain that you have anti-virus software and keep it up to date;
7. Understand what encryption will do and when it is necessary;
8. Consider chains of trust and your business relationships;
9. Demand that your vendors fully understand the HIPAA security standards;
10. Start with a plan – and the end –in mind.

Table 1. Administrative Procedures to Guard Data Integrity, confidentiality, and Availability

Requirement:	Implementation:
Certification	Evaluate computer system(s) or network design(s) to certify that the appropriate security has been implemented.
Chain of trust partner agreement	If data are processed through a third party, the parties would be required to enter into a chain of trust partner agreement
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	Documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
Internal audit	In-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an entity.
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.

Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management.

Table 2. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability

Requirement:	Implementation:
Assigned security responsibility	Assigned to one person and to include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data
Media controls (all listed implementation features must be implemented).	<ul style="list-style-type: none"> Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	<ul style="list-style-type: none"> Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	Delineate the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a terminal unattended).
Secure work station location	Physical safeguards to eliminate or minimize the possibility of unauthorized access to information.
Security awareness training	Required for all employees, agents, and contractors

Table 3. Technical Security Services to Guard Data Integrity, Confidentiality and Availability

Requirements:	Implementation:
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	Audit control mechanisms to record and examine system activity.
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access.
Data Authentication	Corroboration that data in its possession has not been altered or destroyed in an unauthorized manner.
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

Table 4. Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network

REQUIREMENT:	IMPLEMENTATION:
Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication.	Access controls. Alarm. Audit trail. Encryption. Entity authentication.
In addition, one of the following implementation features must be implemented: Access controls, Encryption.	Event reporting. Integrity controls. Message authentication.
I using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	

Table 5. Electronic Signature Requirements and Implementation

Requirement:	Implementation:
Digital signature If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional.	Ability to add attributes. Continuity of signature capability. Countersignatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication

Table 6. Sample Templates: Assigned Security Responsibility

HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required.		
Key Activities	Description	Sample Questions
	<p>Introductory Reference:</p> <p><i>An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 3)</i></p>	
<p>1. Select a Security Official To Be Assigned Responsibility for HIPAA Security</p>	<ul style="list-style-type: none"> • Identify the individual who will ultimately be responsible for security. Select an individual who is able to assess effective security and to serve as the point of contact for Security policy, implementation, and monitoring. 	<ul style="list-style-type: none"> • Who in the organization— Oversees the development and communication of security policies and procedures? • Is responsible for conducting the risk assessment? • Handles the results of periodic security evaluations? • Directs IT security purchasing and investment? • Ensures that security concerns have been addressed in system implementation?
<p>2. Assign and Document the Individual’s Responsibility</p>	<ul style="list-style-type: none"> • Document the individual’s responsibilities in a job description • Communicate this assigned role to the entire organization. 	<ul style="list-style-type: none"> • Is there a complete job description that accurately reflects assigned security duties and responsibilities? • Have the staff members in the organization been notified as to whom to call in the event of a security problem?
<p>Supplemental NIST References</p>	<ul style="list-style-type: none"> • NIST SP 800-14 • NIST SP 800-26 • NIST SP 800-53 	

Example:

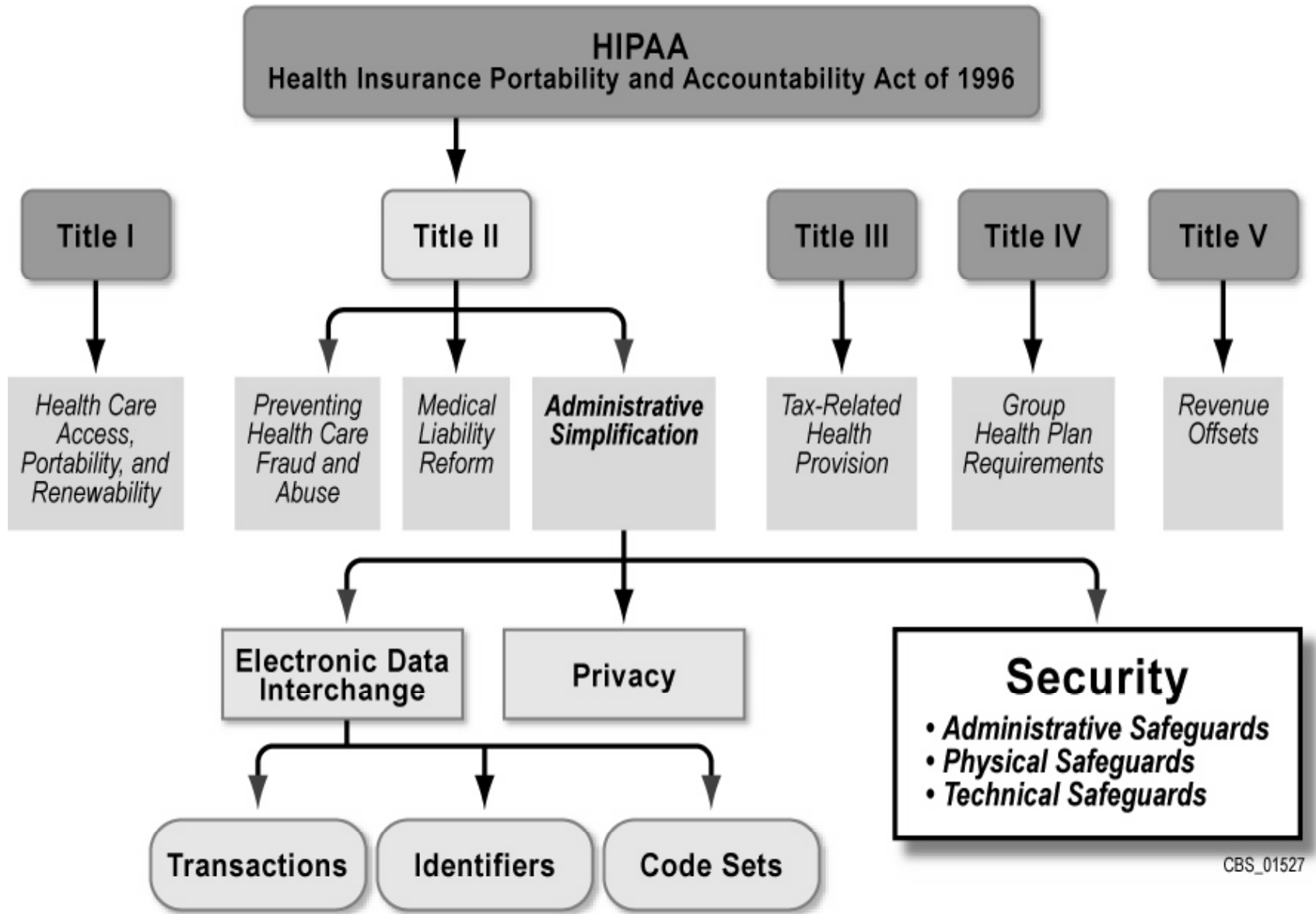
The head of a small (10 employees) health care service provider organization has been reviewing HIPAA standards and realizes that they must formally assign a person to be responsible for HIPAA implementation. Currently no one on staff has the expertise in security needed to do the job. They have two choices: (1) train an existing employee or (2) hire a new resource. From a cost perspective, they would prefer to train existing staff. They have three IT specialists on staff that currently support the small local area network (LAN) installed one year ago. They believe that, it would not be difficult to train a resource from this operation to coordinate HIPAA security implementation. They have also asked the training manager to identify recommended sources so that a comprehensive training strategy can be developed. The new function will also be discussed at the weekly staff meeting..

Table 7. Sample Templates: Transmission Security

HIPAA Standard:		
<i>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</i>		
Key Activities	Description	Sample Questions
	<p>Introductory Reference:</p> <p><i>An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 16 &19)</i></p>	
<p>1. Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information</p>	<ul style="list-style-type: none"> • Identify scenarios that may result in modification to the electronic protected health information (EPHI) by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors). 	<ul style="list-style-type: none"> • What measures exist to protect EPHI? • What measures are planned to protect EPHI? • Is there an auditing process in place? • Is there assurance that information is not altered during transmission? • Are there trained staff members to monitor transmissions?
<p>2. Develop a Transmission Security Policy</p>	<ul style="list-style-type: none"> • Establish a formal (written) set of requirements for transmitting electronic protected health information. 	<ul style="list-style-type: none"> • Have the requirements been discussed and agreed to by identified key personnel involved in transmitting electronic health information? • Has a written policy been developed and communicated to system users?
<p>3. Implement Procedures for Transmitting Electronic Health Information Using Hardware/Software if Needed</p>	<ul style="list-style-type: none"> • Identify methods of transmission that will be used to protect electronic health information • Identify tools and techniques that will be used to support the transmission security policy. 	<ul style="list-style-type: none"> • Is encryption needed to effectively protect the information? • Is encryption feasible and cost-effective in this environment? • Are staff members skilled in the use of encryption?
<p>Supplemental NIST References</p>	<ul style="list-style-type: none"> • NIST SP 800-14 	

	<ul style="list-style-type: none">• NIST SP 800-42• NIST SP 800-53• NIST SP 800-63• FIPS 140-2	
<p>Example:</p> <p>A health care provider has decided to use the Internet to transmit patient data to a support vendor for backup and contingency operations. The transmission of this data should be protected from disclosure. No one who is not authorized to read the file should be able to monitor the transmission and capture the information during its transmission. The health care provider has decided to design and implement a web application, which enforces the use of strong encryption methods to prevent unauthorized disclosure of the data during transmission.</p>		

Figure 1: Security Provisions of HIPAA



CBS_01527

Figure 2. NIST Publications to Address Various Stages of a Security Program's Life Cycle.

