December 2003

A New Security Framework for HIPAA-Compliant Health Information Systems

Bengisu Tulu
Claremont Graduate University

Samir Chatterjee
Claremont Graduate University

A New Security Framework for HIPAA-Compliant Health Information Systems

Bengisu Tulu
Network Convergence Laboratory
Claremont Graduate University
bengisu.tulu@cgu.edu

Samir Chatterjee
Network Convergence Laboratory
Claremont Graduate University
samir.chatterjee@cgu.edu

Abstract

Security in health care information systems is among the highest priority research topics. Introduction of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) increased the pressure on health care organizations for implementing security. Two existing frameworks, which affect the proposed security standards, are introduced. It is important to understand the development of standards and how they can be useful, in order to successfully implement them. In this paper, we propose a techno-managerial framework that can aid planners of security systems as deployed within health care environment. Having a security framework will enable organizations to implement security standards more easily and quickly. As a result, we–the patients–will start seeing an increasing number of new health care services supported by the information technologies.

Keywords: Security framework, HIPAA, health information systems

Introduction

It has become impossible to practice modern medicine without seeking the help of information technologies and communication networks. Today's health care professionals spend a significant portion of their time managing information – for example obtaining and recording information about patients, consulting colleagues, planning diagnostic procedures, devising strategies for patient care, interpreting results of laboratory and radiological studies or conducting case based or population-based research. Only computers can manage the vast amount of information generated during clinical encounters and other health care transactions. One of the biggest challenges involves balancing two competing values – free access to information and protection of patients' privacy and confidentiality. Information should be readily available to health care professionals so as to provide the best possible care. Yet, making this information readily available creates opportunities for access by unwelcome individuals. Such undesired access could be by curious clinicians or even more worrisome to people who may wish to harm the patient physically, emotionally or financially (Shortliffe and Perrault, 2001).

Recent research (Brender, et al., 2000) was conducted to identify what is needed to implement information society in health care and the related research topics that should be given higher priority to achieve the desired evolution. The results indicated that security is among the highest priority research topics according to international experts involved in this research. It was indicated in this study that the problem regarding security in health care information systems is not the technology itself but the practices. How to implement the existing security technologies within the health care boundaries is a question that still needs to be answered.

In this paper, we develop a techno-managerial framework that can aid planners of security systems as deployed within health care environment. In Section 2, we first briefly discuss the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and then present a general security model for health care systems. In Section 3, we further develop both technical as well as non-technical security issues as pertaining to HIPAA compliance. Section 4 discusses two existing frameworks for security in health care information systems. In Section 5, we present our techno-managerial framework and finally conclude this paper by discussing its applicability.

HIPAA and the General Security Model

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996. HIPAA requires that the Secretary of Health and Human Services (HHS) adopt standards for the electronic transmission of specific administrative transactions. Table 1 shows some of the requirements for HIPAA.

Table 1. Sample Requirements for HIPAA (1996)

1.	The Secretary must adopt standards for transactions and data elements for such transactions, to enable health information to be exchanged electronically that are appropriate for financial and administrative transactions consistent with the goals of improving the operation of the health care system and reducing costs including: a. Health Claims or equivalent encounter information b. Health Claims attachments c. Enrollment and Disenrollment in a Health Plan d. Eligibility for a Health Plan e. Health Care payment and Remittance Advice f. First Report of Injury g. Health Claim Status h. Referral Certification and Authorization i. Coordination of Benefits
2.	The Secretary shall adopt standards providing for a unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system
3.	The Secretary shall adopt standards for code sets for appropriate data elements for financial and administrative transactions.
4.	The Secretary shall adopt security standards that …specify procedures for the electronic transmission and authentication of signatures.

Before we take a look at the general security model, it is important to further explore the foundations of health privacy and confidentiality. These two terms are not synonymous. Privacy generally applies to people, including their desire not to be a victim of eavesdropping, whereas confidentiality is best applied to information. We imply privacy when someone spots us in a place where we do not want to be seen while confidentiality is broken when someone can look into our medical record in some location (Shortliffe and Perrault, 2001).

The General Security Model (Figure 1) proposes that the security of information systems has to be analyzed under two main topics, which are application security and communication security [3, 6]. Application security assures that the application under use cannot be interrupted or damaged by intruders. Application security threats can be grouped under two fundamental categories, people attacking software and software attacking software like virus programs (**http://www.cloakware.com/pdfs/FSAwardpressrelease-1Oct2002.pdf**, 2002). Communication security deals with assuring a secure communication between principals (Blobel, 2000), which may be a user and an application, two applications, etc. It ensures that while data is being transferred between various parties, it cannot be intruded upon or sniffed by other parties. Some of the threats related to communication security are loss of privacy, loss of data integrity, and identity spoofing. Since communication security is concerned about interactions and has serious threats, it must always be included (Blobel, 2000). The General Security Model has been used to identify the security needs of the health care environment in a generic way. In fact, if we take a closer look at the HIPAA security rules we will see the reflections of general security model in technical rules.

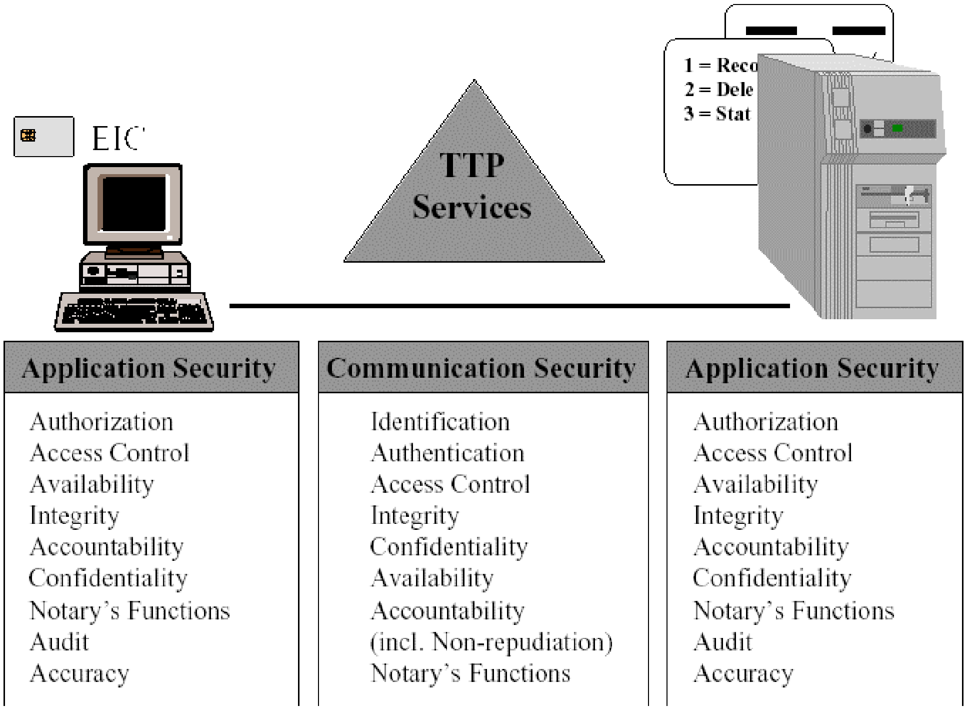

Figure 1. General Security Model (Brender, et al., 2000)

HIPAA Security Model

HIPAA mandates rules to maintain the privacy of protected health information, to establish security requirements to protect that information, and to develop standard identifiers. Based on the HIPAA security rules (HIPAA.org, 2003), if a system or the communication between two systems was implemented using technology(s) meeting standards in a general security framework (Identification and Authentication; Authorization and Access Control; Accountability; Integrity and Availability; Security of Communication; and Security Administration.) then that system would be essentially secure. However, there is no single standards development organization (SDO) that is addressing all aspects of health care information security and confidentiality. As a result, HIPAA defines the security standard 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 standard does not reference or advocate specific technology in order to allow the security standard to be stable, yet it is flexible enough to take advantage of state-of-the-art technology. HIPAA security standards can be summarized under four main topics:

1. **Administrative procedures to guard data integrity, confidentiality, and availability:** Defines the mandatory documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

2. **Physical safeguards to guard data integrity, confidentiality, and availability:** Defines the mandatory practices to protect physical computer systems and related buildings and equipment from fire and other natural hazards, as well as from intrusion.

3. **Technical security services to guard data integrity, confidentiality, and availability:** Defines the processes that are put in place to protect information and to control individual access to information.

4. **Technical security mechanisms:** Defines the processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.

Technical Aspects

It is clear that the information security needs are not restricted to the technical aspects of the health care environment only. These four main categories identify the information security needs of a health care environment by taking various aspects of it into account. In this section, the technical rules will be explained in detail. Figure 2 and Figure 3 provide the details for these two rules, 3 and 4.

Figure 2, Technical Security Services, is the security rule 3 in HIPAA, which was defined by Blobel (Blobel, 2000) after modifying the CORBA Specifications. The general security model provides the main thinking for these two rules. Rule 3 deals with the application security. However, as mentioned above, communication security has to be included all the time since we are talking about applications that were developed to interact with other principals. Figure 3, Technical Security Mechanisms, deals with the communication security itself, which is described in the general security model. In the general security model, data and entity authentication should also be considered under application security. One reason for this modification is that entity authentication cannot be separated from authorization. The applications should have control over the entity authentication in order to make better authorization decisions. This does not imply that all applications should have authentication capability. Rather they should be able to identify the authentication mechanisms that an entity can use in their environment and be able to assess the authentication information, which can be provided by the entity itself or by a separate authentication application.

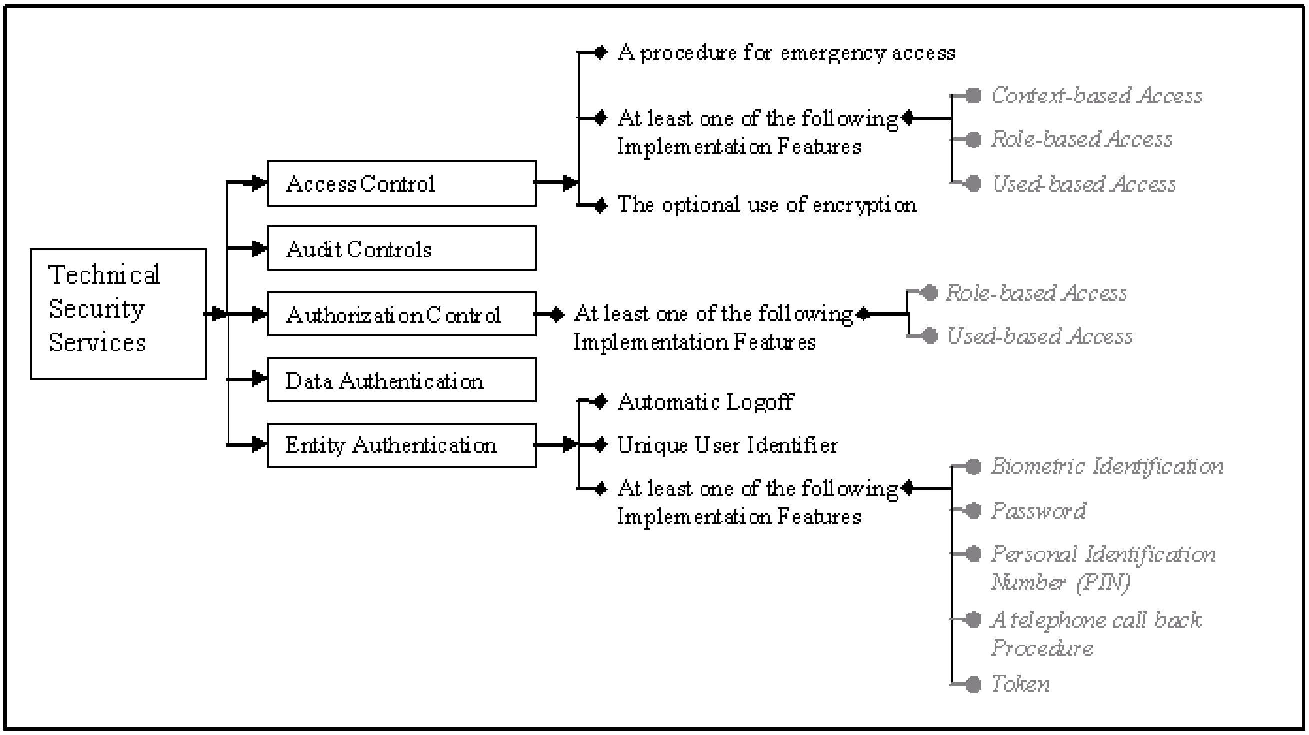
Technical Security Services
Access Control
Audit Controls
Authorization Control
Data Authentication
Entity Authentication
A procedure for emergency access
At least one of the following Implementation Features
The optional use of encryption
Context-based Access
Role-based Access
Used-based Access
At least one of the following Implementation Features
Role-based Access
Used-based Access
Automatic Logoff
Unique User Identifier
At least one of the following Implementation Features
Biometric Identification
Password
Personal Identification Number (PIN)
A telephone call back Procedure
Token

Figure 2. HIPAA Proposed Security Rule 3

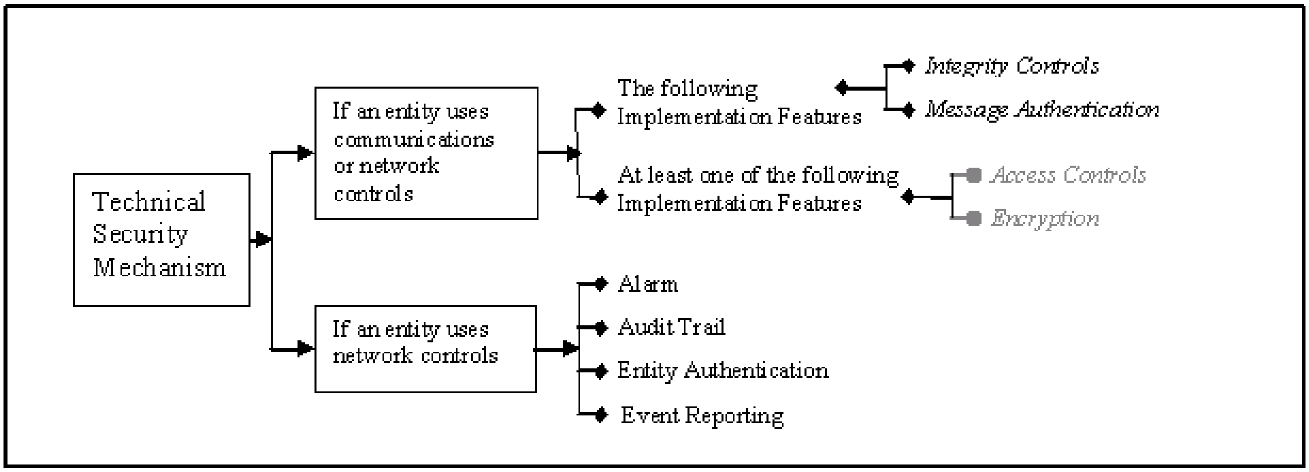
Technical Security Mechanism
If an entity uses communications or network controls
If an entity uses network controls
The following Implementation Features
Integrity Controls
Message Authentication
At least one of the following Implementation Features
Access Controls
Encryption
Alarm
Audit Trail
Entity Authentication
Event Reporting

Figure 3. HIPAA Proposed Security Rule 4

Non-technical Aspects of HIPAA Security

> "Regarding security with special aspects of the health care domain, ethical, legal, social, organizational, and technological issues must be handled." (Blobel, 2000)

Complexity of the health care environment, as summarized by Blobel above, makes it more complex to develop a security framework that covers all these issues. However, non-technical aspects also require a careful consideration in order to have a strong security implementation in the health care environment. HIPAA reserved the first two rules of the security section to non-technical issues that concern about administrative procedures and physical safe guards.

In order to achieve "trustable" security levels, a comprehensive information security policy is necessary (Janczewski and Shi, 2002). These policies should be defined based on the organization's philosophy and the environment to which it belong. Standards like HIPAA provide guidelines for defining the policy rules in health care organizations. Security policies will vary based on the organization structure, culture and much other organization specific attributes. However, an organization should at least cover the following security baselines in its security policy:

1. A statement of organizational philosophy and goals regarding privacy and security; (Janczewski and Shi, 2002) which concerns the management of information security and its organization.
2. A classification of information assets by type; (Janczewski and Shi, 2002) which concerns the control of the asset management, the definition of the ownership of health information assets, and standards for health information classification.
3. Standards for administering, controlling and monitoring information use by type; (Blobel, 2000) which concerns the personnel security, their training about the information security, and awareness of security policies, as well as the physical and environmental security.
4. Standards for information system design, implementation and operation; (Janczewski and Shi, 2002) which concerns the computer and network management, and system development and maintenance.
5. A definition of procedures for detecting and handling abuses; (Janczewski and Shi, 2002) which concerns the system access controls, user classification, authorization and authentication.
6. Standards for legal and ethical issues; (Blobel and Roger-France, 2001) which concerns the ethical and legal rules that apply in health care environments.

The first five items that were listed by Janczewski and Shi cover almost all the issues regarding the security. An additional item on their list should be the legal and ethical standards, which were covered by Blobel et al. (Blobel and Roger-France, 2001) security framework.

Survey of Security Frameworks for Health Care Organizations

Based on these technical and non-technical aspects of security, different frameworks were developed by researchers. Blobel et al. (Blobel and Roger-France, 2001) has developed a framework that purely addresses the technical aspects and it shown in Figure 4.

Blobel et al. reported that security services and related mechanisms could be managed by following a series of actions. They provided a list of seven actions and based on these guidelines they came up with nine use case scenarios to develop their framework. The list of actions is provided below (Blobel and Roger-France, 2001):

1. Identification of the domain;
2. Definition of the security objects;
3. Specification of the use cases and the set of security services needed;
4. Specification of the architecture, which implements the general security model (explained above);
5. Realization of a detailed threat and risk analysis and specification of security requirements considering the use case specifications;
6. Selection and specification of security mechanisms for providing security services;
7. Consideration of IT-related security mechanisms and implementation of the security environment needed using appropriate algorithms.

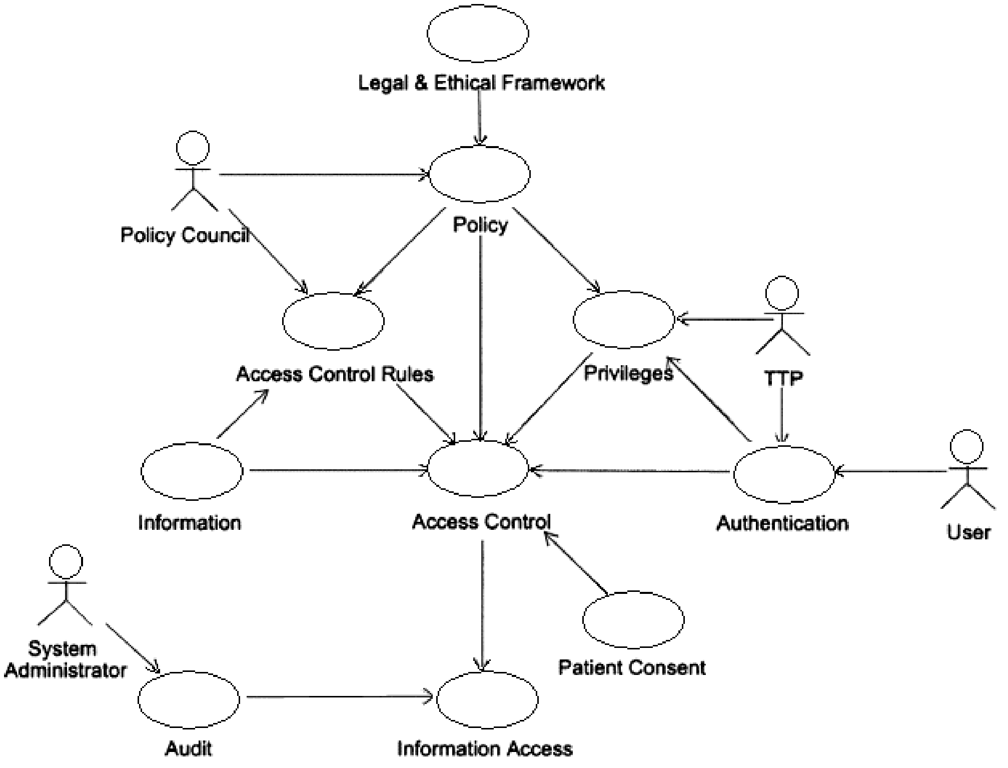

Figure 4. Security Framework by Blobel (Blobel and Roger-France, 2001)

A different framework that addresses more of the organization aspects has been developed by Janzewski and Shi (Blobel and Roger-France, 2001). They reported in their study that a security framework should include an overall baseline assessment and risk analysis, specific policy development, measure implementation, and monitoring and reporting action. It also added that a framework should enable the personnel involved in developing policies and procedures to understand the ultimate goal of their efforts, as well as how these efforts complement parallel efforts elsewhere within the organization. The security baselines, listed in the previous section, were used to introduce this framework.

The coverage of these two frameworks is not exactly the same. The Blobel et al. framework is covering in detail the technical aspects of the security compared to Janzewski and Shi framework. On the other hand, the latter framework covers in detail the managerial and organizational aspects of the environment.

A Hybrid Framework for Security

The two frameworks described above were selected since they affect the security standards that are being proposed. It is important to understand the development of standards and how they can be useful, in order to successfully implement them. Although these frameworks mentioned are very comprehensive, a combined version of these two frameworks will provide better results. HIPAA forces us to realize that it is very important to cover both technical and managerial aspects in detail to have successful security implementations. We present such a hybrid security framework in Figure 5. This framework is a simple eight-stage framework that should help the management team to decide how to make their organization HIPAA compliant. Each of these stages is described in detail below.

Stage 1: Infrastructure Evaluation

The infrastructure evaluation stage serves as the foundation where the ensuing seven stages will draw upon. Analyzing the existing components and current status of the infrastructure will provide management a clear vision and understanding of the security issues that the organization is challenged with. The analysis component of the assessment is intended to provide a diagnostic regarding the current state of the infrastructure. The result of the diagnostics will provide a list of areas that requires implementation of new security mechanisms and/or a list of secured areas that needs to be improved. For each item in the list, there should be opportunities and challenges listed as well. The diagnostics list is the first step for managers to identify the most suitable security mechanism for their organization. Some critical components of the infrastructure that should be considered are provided in Table 2.

Table 2. Some Critical Components of the Infrastructure

System	Hardware Software Applications
Structure	Work Processes (Medical and Administrative) Organizational Structure Roles and Responsibilities Geographic Spread
Policy	Security Policy of the enterprise and its impacts on business strategy Upper management support policy Government Policy on security
Strategy	Core competencies
Environment	Competitors Regulations

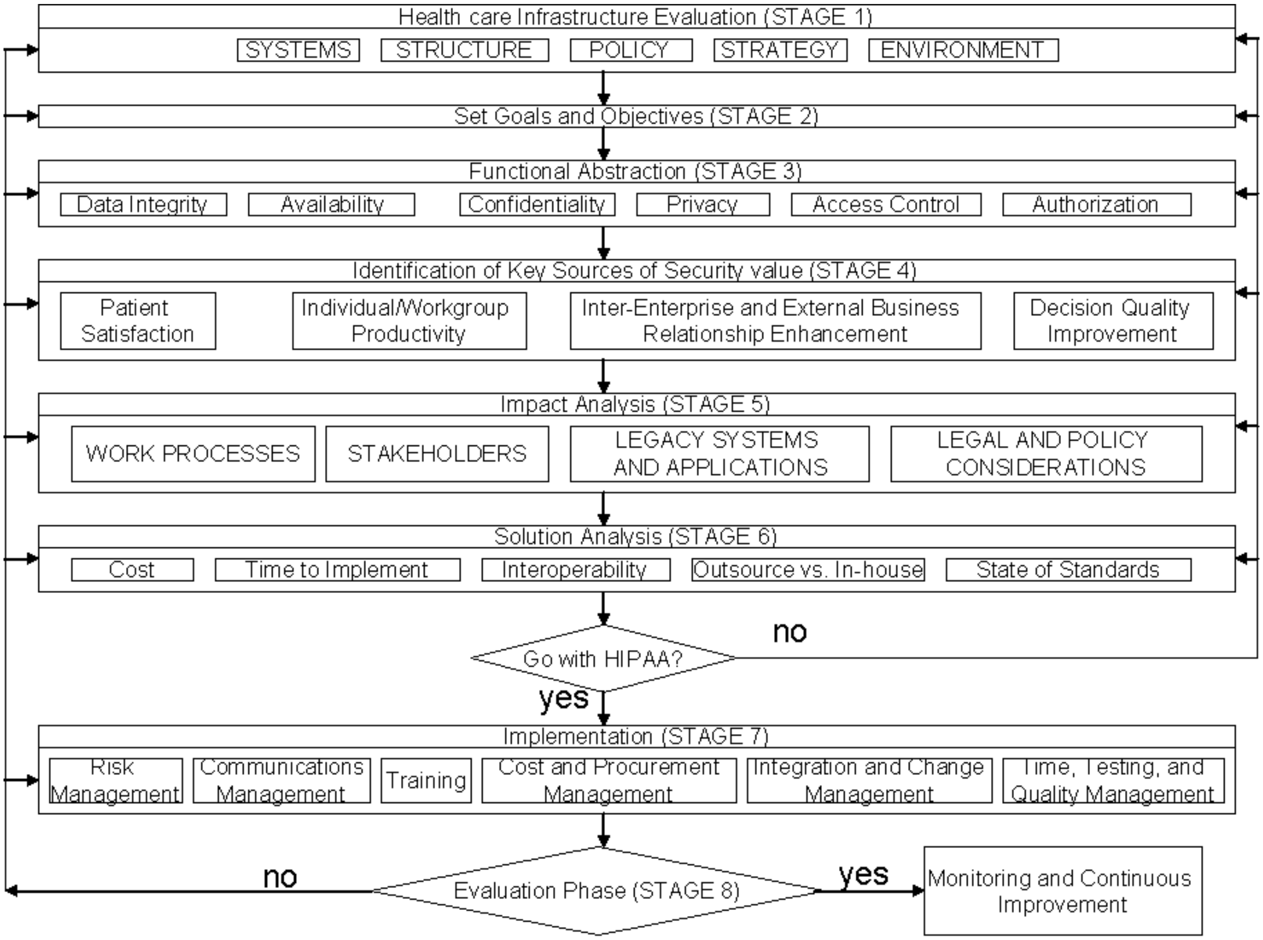
Health care Infrastructure Evaluation (STAGE 1)
SYSTEMS
STRUCTURE
POLICY
STRATEGY
ENVIRONMENT
Set Goals and Objectives (STAGE 2)
Functional Abstraction (STAGE 3)
Data Integrity
Availability
Confidentiality
Privacy
Access Control
Authorization
Identification of Key Sources of Security value (STAGE 4)
Patient Satisfaction
Individual/Workgroup Productivity
Inter-Enterprise and External Business Relationship Enhancement
Decision Quality Improvement
Impact Analysis (STAGE 5)
WORK PROCESSES
STAKEHOLDERS
LEGACY SYSTEMS AND APPLICATIONS
LEGAL AND POLICY CONSIDERATIONS
Solution Analysis (STAGE 6)
Cost
Time to Implement
Interoperability
Outsource vs. In-house
State of Standards
Go with HIPAA?
no
yes
Implementation (STAGE 7)
Risk Management
Communications Management
Training
Cost and Procurement Management
Integration and Change Management
Time, Testing, and Quality Management
no
Evaluation Phase (STAGE 8)
yes
Monitoring and Continuous Improvement

Figure 5. A New Security Framework Addressing Technical and Organizational Issues

Stage 2: Set Goals and Objectives

After understanding the infrastructure of the organization in detail, it is important for the organization to restate its organizational vision, mission, and goals. These statements will help the organization to define what return is expected from implementing security mechanisms. Even though HIPAA rules are mandatory, managers should identify the possible effects of necessary changes on the organization.

Stage 3: Functional Abstraction

Information System reliability requirement is a critical domain where functional abstraction from processes, procedures, interfaces and people, among others, are derived to attain a high-level verification of how effective or germane a specific security system can be used optimize an enterprise's reliability requirement. In Stage 3, we recommend an appraisal of how each of these requirements (Data Integrity, Availability, Confidentiality, Privacy, Access Control, Authorization, and Authentication) rate in importance and substance in the operations of the enterprise.

Stage 4: Identification of Key Sources of Security Value

A needs assessment provides an opportunity to consult with a variety of people in the organization as well as the patients. The information collected, ideas generated, and the conversations that take place when people discuss their work lives lend enthusiasm to the process. Functional requirements are subsequently developed from the needs assessment effort. The data collected - whether obtained through interviews, observations, focus groups, performance data, questionnaires or tests - can clarify issues and provide a focus on the following key sources of security value: Patient Satisfaction, Individual/Workgroup productivity, Inter-Enterprise and External Business Relationship Enhancement, Decision Quality improvement.

There are several steps to consider when developing a plan to conduct a needs assessment. These steps include: (1) Selecting the method for gathering information, (2) Selecting the sources of information, (3) Assigning responsibilities for activities of the needs assessment, (4) Conducting the information gathering, (5) Analyzing and reporting the information. The lesson learned from past IT projects is that a technology needs assessment is more effective when the analysis is based on the enterprise's strategic goals and analysis of the current state of infrastructure resources.

Stage 5: Impact Analysis

It is important to identify the impact of implementing HIPAA in order to predict the possible outcomes of the project. The impact can be analyzed under four main topics: Work Processes, Stakeholders, Legacy Systems and Applications, Legal and Policy Considerations. After identifying the impact of implementing HIPAA on the business processes one can determine the processes requiring enhanced security how strategic these are for the organization. This also helps to prioritize the applications and determine the sequence of migration. The success of implementation is directly related with the stakeholders of the organization. Therefore, it is important to identifying decision criteria for internal and external users, and to assess the requirement for technical support and administration.

Stage 6: Solutions Analysis

Once the justification of the implementation is made, requirements are identified, and the impacts are predicted, the organizations should consider the alternative solutions for implementing HIPAA. An assessment of the alternatives that can fulfill the requirements of the organization is the next step. This assessment should be based on cost, time to implement, interoperability, acquisition type (outsource vs. in-house), and state of standards.

At the end of this stage, the organization should be able to make a decision in order to implement HIPAA. If there are still doubts about the implementation then the stages where doubts can be cleared (Stage 1,2,3,4,5) should be reconsidered.

Stage 7: Implementation

Project implementation begins with identifying initiatives or activities needed to carry out the best solution. The broad categories for delineating the HIPAA implementation plan are: Risk Management; Communications Management; Cost and Procurement Management; Integration and Change Management; Time, Testing, and Quality Management; and Training. Each of these should be carefully planned in order to achieve success.

Stage 8: Evaluation

An assessment exercise can be performed during or after implementation to identify the success of the project. Different techniques, individually or in combination, can be used to evaluate the implementation. Measuring results against goals, standards, and stated objectives will help managers to evaluate the performance of the project.

Conclusions

It is clear that health care organizations have a tremendous challenge ahead as they become HIPAA compliant and at the same time plan strategies to deploy security within their organizations. While the technical issues are clearly needed, the intricate relationship between various stakeholders in the health care arena makes it even more necessary to incorporate the organizational and managerial issues into a framework. Our proposed framework is aimed at that.

Another important issue in implementing security is gaining knowledge about the existing technologies that can provide necessary tools to satisfy the requirements of security standards. A guideline should be developed for the existing security technologies and should be expanded as new ones are added. This guideline can be provided as an addition to the global security framework. Such a guideline should not only include all the existing technologies that can provide the technical and managerial services required, but should also mention the weaknesses and strengths of each technology.

Having a security framework will enable organizations to implement security standards more easily and quickly. It also ensures that the implementers and planners are aware of all the important information regarding the security needs and technologies, which they need to consider. As the number of health care organizations that implement security framework and standards increase, we - the patients - will start seeing an increasing number of new health care services supported by the information technologies.

References

Blobel, B. "Advanced tool kits for EPR security," *International Journal of Medical Informatics* (60), 2000, pp. 169-175.

Blobel, B., and Roger-France, F. "A systematic approach for analysis and design of secure health information systems," *International Journal of Medical Informatics* (62), 2001, pp. 51-78.

Brender, J., Nohr, C., and McNair, P. "Research needs and priorities in health informatics," *International Journal of Medical Informatics* (58-59), 2000, pp. 257-289.

HIPAA.org "HIPAA Security Rules," (2003:May 30), 2003, **http://www.cloakware.com/pdfs/FSAwardpressrelease-1Oct2002.pdf**, loakware Wins Frost & Sullivan Award for Technology Innovation," (2003:May 30), 2002,

Janczewski, L., and Shi, F.X. "Development of Information Security Baselines for Health care Information Systems in New Zealand," *Computers & Security* (21:2), 2002, pp. 172-192.

Shortliffe, E.H., and Perrault, L.E. *Medical Informatics: Computer Applications in Health Care and Biomedicine*, Springer-Verlag, New York, 2001.