Global Information Assurance Certification Paper

SANS GSEC Practical Assignment
Version 1.4b Option 2
Administrivia version 2.7
Pre-Approval Submission Date: December 29, 2003
Topic Approval Date: January 12, 2004
Practical Submission Date: February 29, 2004

Developing & Implementing an Information Security Policy and Standard Framework

By: Peni D. Smith

Abstract

In August of 1998, the Department of Health and Human Services published a proposed rule (to the Federal Register) proposing, "…standards for the security of individual health information and electronic signature use by health plans, health care clearinghouses, and health care providers" (Proposed Security Rule 43242). As a health care provider, and a covered entity under HIPAA, our Information Security team began reviewing the proposed security rule requirements and formulating a compliance program. It quickly became apparent that the proposed security rule requirements were reasonable security controls that should be implemented to support normal business operations. The issue, however, was that our current Information Security framework was outdated. Our Information Security standards had not been updated since 1995. As a result, our Information Security Program contained weaknesses brought about by new technology implementations (since 1995). In an attempt to advance the Company's Information Security Program, our team began defining security program requirements, including federal security requirements, and security controls needed to support business and technology drivers. Our mission – to create a solid Information Security policy and standard framework that would not only achieve compliance with federal security regulations, but also serve as an Information Security industry best practice. As stated in ISO 17799, "Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization" (ISO 17799 1).

This practical will discuss our team's tactical approach to developing and implementing an Information Security policy and standard framework. Key project processes highlighted will include gathering security requirements, designing an Information Security Governance process, and integrating with existing security communication and training initiatives. To help assist other Companies in building/enhancing their Information Security policy and standard framework, or other HIPAA covered entities in complying with security rule requirements, we will briefly discuss project challenges and resulting "lessons learned."

Part One: The Current Scenario

1.1: The Issue

After reviewing the proposed HIPAA Security rule requirements, it became apparent to our team that our existing Information Security policies and standards were not adequate to achieve full compliance. Advances in technology had brought about new vulnerabilities that were not addressed by our program. For example, wireless local area network technology was being deployed within our hospital facilities and corresponding Information Security standards and guidelines had not yet been drafted. Additionally, with increased use of the Internet to transmit patient information (e.g., to confirm eligibility of patients), we had not defined required security controls for open-network transmission.

The current scenario created vulnerabilities and risks to the Company. Once the HIPAA Security rule became final and a compliance date reached, there would be increased risks such as possible civil and criminal penalties for non-compliance. Additionally, if the lack of security controls permitted security breaches to the confidentiality, availability, and/or integrity of patient information, patient safety may be affected, or worse, lives could be lost.

1.2: Vulnerabilities/Risks

Our Company serves as an Information Systems (IS) service provider to our hospital facilities, as well as other healthcare providers (our "customers"). As a result, under the proposed security rule, we would be subject to specific security terms/requirements for any data processed on behalf of a third-party. The proposed rule stated, "If data are processed through a third party, the parties would be required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information" (Proposed Security Rule 43252). Therefore, the Company would be contractually obligated to modify IS applications and infrastructure to comply with the proposed security rule requirements. Failure to meet these contractual obligations could lead to additional liability, negative impact to public relations, and potential lost revenue (if customers were to change IS service providers). As an IS service provider, the Company needed effective, consistent Information Security policies and standards to help create a secure, private network. Without standardized Information Security policies and standards, the Company's network might be seen as an open-network, with similar risks associated to the Internet.

1.3: My Role, as an Information Security Consultant

After defining the current scenario and related issues, I became very enthusiastic about the opportunity to lead our team and ultimately the Information Security department's efforts to update Information Security policies and standards; therefore, creating a HIPAA Security rule compliance program. I had recently transferred to the Information Security department, after working with the Company's Internal Audit department. Prior to my Internal Audit experience, I had worked for a major accounting and consulting firm performing IS reviews. My five years experience with IS auditing, along with the knowledge and training required to achieve my CISA (Certified Information Systems Auditor) certification, had provided me with a strong foundation in identifying control weaknesses and developing and implementing corresponding solutions and mitigating controls.

Part Two: Improving/Enhancing The Current Scenario

2.1: Identifying the Problem

To fully determine the extent of the problem (i.e., extent of revisions/additions needed to raise current Information Security policies and standards into federal compliance and to align with industry best practices) our team began gathering project or security requirements. Since the Company's goal is to incorporate federal requirements, business needs, etc. into one comprehensive Information Security Program, our Information Security policy and standards framework would need to address the Information Management standards contained within the Joint Commission of Accreditation of Healthcare Organizations or JCAHO accreditation program (due to a Company requirement for hospital facilities to be JCAHO accredited). Additionally, the final HIPAA Privacy rule, with a compliance date of April 14, 2003, "requires covered entities to implement appropriate administrative, technical, and physical safeguards to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that violates the Rule" (Final Privacy rule 53193). Therefore, security controls such as screensavers, positioning of monitors, and general security awareness and training on password management and logging off of sessions after completion would need to be incorporated into the framework prior to April 14, 2003.

To help identify requirements resulting from industry best practices, our team reviewed/researched information such as ISO 17799: Information technology — Code of practice for information security management, National Institute of Standards and Technology (NIST) publications, and Charles Cresson Wood's Information Security Policies Made Easy. The aforementioned does not include all Information Security input sources for our project, but are listed to highlight areas of significant contribution.

2.2: Defining/Implementing a Solution

When our project began, only the proposed HIPAA Security rule had been published to the Federal Register, not the final. However, as with many other HIPAA covered entities, our team was anxious to begin compliance efforts versus waiting for publication of the final Security rule. As a result, we reviewed proposed Security rule requirements and industry guidance, specifically identifying components that should be incorporated into any prudent Information Security program. We also placed greater emphasis on proposed Security rule requirements that we did not expect to dramatically change with the posting of a final Security rule (e.g., security awareness and training, identification and authentication, workstation security measures, virus control, physical access controls, etc.). Any proposed Security rule requirements with major changes/clarification anticipated (e.g., audit controls, chain of trust partner agreements, business contingency planning, etc.) were "tabled" pending final Security rule publication or upon completion of the previously identified items, whichever occurred first.

Additionally, as previously mentioned, the HIPAA Privacy rule had been published to the Federal Register, including requirements for "administrative, technical, and physical safeguards to reasonably safeguard protected health information" (Final Privacy rule 53193). And, since privacy and security controls are complementary, our team worked closely with the Company's Chief Privacy Officer to identify and incorporate appropriate administrative, technical, and physical safeguards into project requirements. For example, our two teams collaborated to build an on-line employee awareness and training course to include both privacy and security requirements for safeguarding protected health information. Examples of items/materials that were included in the training course include, but are not limited to, instructions for creating strong passwords and appropriate password management, education on logging off of sessions upon completion, use of screen savers and password protected screen savers for unattended workstations, and physical safeguards for securing workstations such as positioning of monitors away from public viewing and physical locking devices.

2.3: Security Governance Process

As Charles Cresson Wood states in Information Security Policies Made Easy, "Before beginning to write a policy document, the policy writer should check with management to make sure that they are all talking about the same thing, and that they understand why a policy development effort is important" (Wood 7). To help ensure that Information Security policy and standards met business owner needs, as well as regulatory requirements, our team designed a Security Governance process. The governance process commences with internal (within Information Security) development/drafting of Information Security policies and standards, and then expands into appropriate business departments for feedback. Lastly, the Company's Ethics & Compliance department must grant final approval for Information Security policy.

The Security Governance structure that will be discussed in succeeding paragraphs is presented in Diagram 1 below.

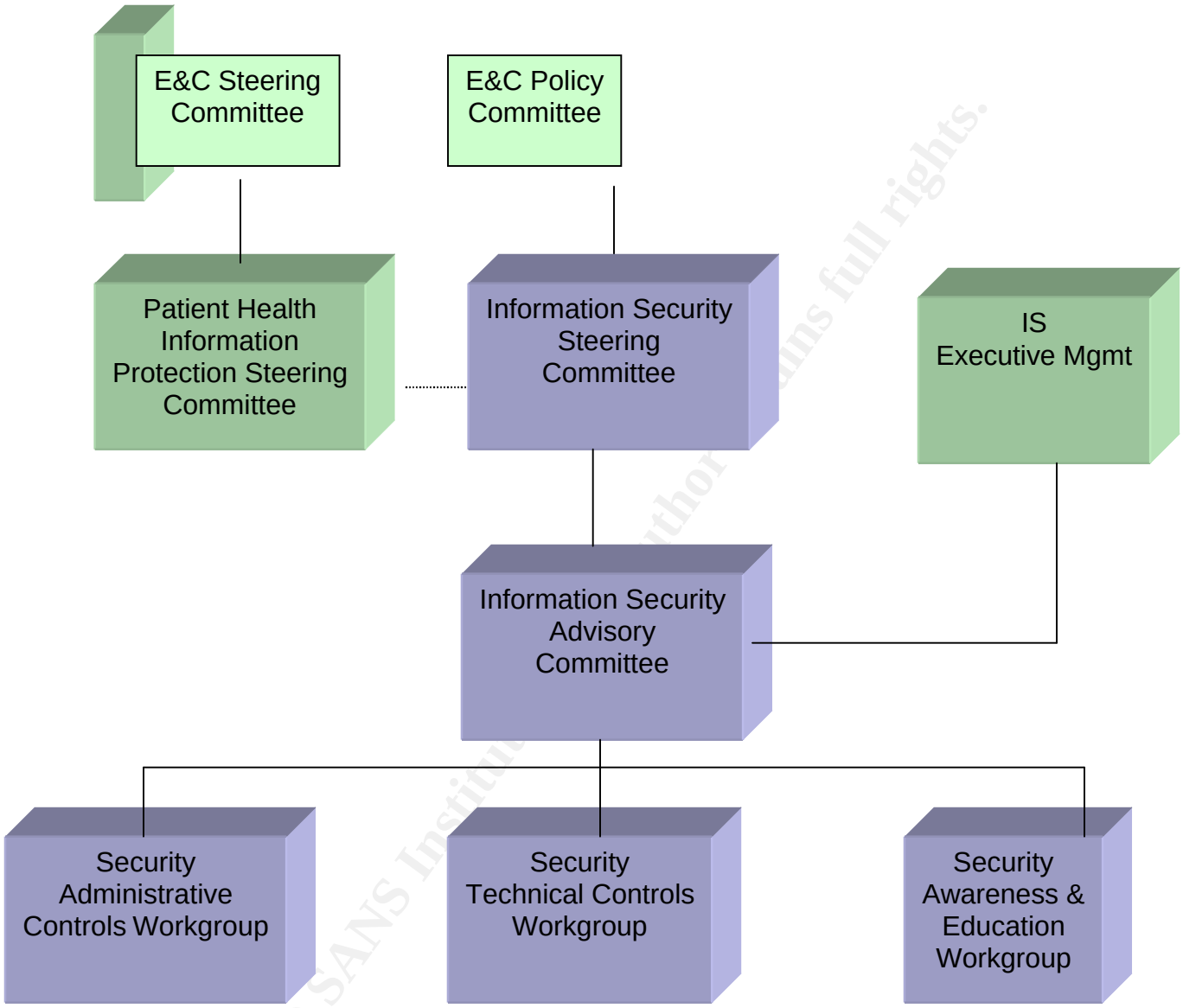

Diagram 1

At the base of our Security Governance process are three workgroups: Security Administrative Controls, Security Technical Controls, and Security Awareness & Education. The objective for each of these workgroups is: To establish security policy, standards, tools/techniques, and a scorecard to enhance security measures and mitigate risk. Each workgroup is assigned specific scope areas. The Security Administrative Controls workgroup is responsible for areas of general controls, administrative controls (including contracts) and applications. The Security Technical Controls workgroup is responsible for areas of secure communications, perimeter control, network controls, and operating systems controls. And, lastly, the Security Awareness & Education workgroup is responsible for overall security awareness, ensuring the Security message is communicated and understood by the workforce (including approximately 300,000 users). Each of these workgroups drafts initial Information Security policy and standards for its respective areas and/or reviews output from other workgroups. These workgroups also help validate both the technological and operational effectiveness of the underlying security controls. An Information Security representative leads each of these workgroups; with workgroup membership composed of business areas such as Human Resources, Legal, Clinical, Financial Services, and other IS areas, including hospital facility representation.

The next layer of our Security Governance process is our Information Security Advisory Committee. The objectives of this committee are: To approve security strategies to mitigate security risks for the Information Security Steering Committee, and To guide Information Security program development through risk mitigation. The Information Security Advisory committee reviews security documents prepared and finalized by the sub-workgroups and provides input prior to advancing to the Information Security Steering Committee.

After approval by the Information Security Advisory Committee, security strategies, including Information Security policy and standards proceed to the Information Security Steering Committee for additional consideration.

Business owners are incorporated into the Security Governance process via the Information Security Advisory and Information Security Steering Committees. Representatives on these committees include areas such as Legal, Health Information Management (including the Chief Privacy Officer and linkage to the Company's HIPAA Privacy Program), Human Resources, Financial Services, Information Systems (both Corporate and hospital facilities), Internal Audit, Ethics & Compliance, and others on an as needed basis. This is the final level of approval/feedback for security standards. However, note that Information Security policy must go through an additional level of approval, the Ethics & Compliance Policy Committee.

While the Company's Chief Information Officer (CIO) is not a member of the Information Security Advisory or Information Security Steering Committee,

security strategies are informally presented/validated during periodic updates (e.g., status reports, staff meetings) and formally presented to the CIO simultaneously with presentation to the Information Security Advisory Committee.

The last level of approval for Company Information Security policy is the Ethics & Compliance Policy Committee. Ethics & Compliance reviews and approves enterprise-level policies to create an overall acceptable level of integrity. Once an Information Security policy is approved by the Ethics & Compliance Policy Committee, the Ethics & Compliance department communicates the policy to Ethics & Compliance Officers at each of the Company's hospital facilities.

Both the Patient Health Information Protection Steering Committee and the Ethics & Compliance Steering Committee are leveraged on an as needed basis. For example, an Information Security Enforcement & Discipline Policy was drafted and presented to the Security Governance Process. Due to the nature and impact of such a policy (disciplinary actions to be taken for hospital facility employees), the draft policy was presented to both of these committees. However, as previously mentioned, patient health information protection is also achieved in the Security Governance process by Chief Privacy Officer direct participation in the Information Security Steering Committee.

Our Company realizes that occasionally to support business operations, compliance with Information Security policy or standards may not be possible. As a result, Information Security created a security exception process. The security exception process allows a hospital facility to document the security requirement causing difficulty, along with the associated risks and any alternative solutions. The Information Security Advisory Committee reviews the requested security exception and formulates a final decision, including any alternative security solutions. If a security exception is granted, the approval period is limited (e.g., one year) and follow-up is performed upon expiration to ensure the security exception is still valid.

Under the Company's Ethics & Compliance Program, published Information Security policies must be reviewed annually and necessary revisions identified. Revisions are then made following the Security Governance process. Information Security standards are revised on an as needed basis. Submitted security exception requests serve as key contributors to Information Security policy and standard revisions (e.g., which may indicate that security requirements do not adequately support the business). User or hospital facility feedback, along with technological changes are also considered.

2.4: Developing Security Standards

Since the Company's Information Security standards had not been updated since 1995, and since security standards are more detailed than security policies, the

security standards required more effort. As a result, the remainder of this practical will focus on Information Security standard development.

The Information Security Strategy and Programs department (my department) performs initial development of Information Security standards. By gathering project and security requirements, we identified security areas needing new standards or revisions. The security standard areas were then divided into logical groupings (common categories). For example, one category is entitled "User Security Measures" and includes security standards for Identification, Authentication, Workstation Security, Mobile Computing, and Electronic Mail Systems. Security standards were then created for each of the logical groupings.

To assist hospital facilities in complying with Information Security policies and standards, security toolkits were also created for each logical grouping or category. A security toolkit is a package of information, such as tools, techniques, a sample implementation plan, etc. to help explain Information Security policies and standards and to help provide tools for implementation. In the example category, User Security Measures, toolkit components include items such as the following:

- Toolkit Roles and Responsibilities – This section identifies key participants and their roles in compliance for the identified security standards. Examples include Human Resources to work with Information Security in identifying terminated or transferred employees so that system access may be modified, and the user or workforce member to comply with requirements such as configuring strong passwords, implementing screen savers and using email signature disclaimers.

- References to Information Security Policies and Standards – This toolkit section includes cross-references to Information Security policies and standards that support the respective toolkit. In the User Security Measures toolkit, we reference an Information Security Confidentiality and Security Agreements Policy that is an agreement that all individuals granted system access must sign and abide by.

- Information Security Guide - The Information Security Guide is an introduction to Information Security and exposes readers to security topics such as creating quality passwords, virus protection, social engineering, workstation security, etc. The booklet is designed to heighten awareness about good security measures.

- Termination and Transfer Checklist - This is a checklist used by Human Resources, Department Managers, and the Information Security department to help manage access and equipment. For example, the checklist helps identify users and items/access to be

removed or modified due to leaving the Company or a change in job responsibility.

- Implementation Checklist – This checklist helps hospital facilities develop a plan to incorporate toolkit items. It identifies the top ten (10) items that should be an initial starting point for implementing this toolkit.

- Self-Assessment/Compliance Checklist – This checklist serves as a monitoring/auditing tool, identifying items that should be reviewed on a pre-defined interval. For example, tasks include performing a physical walkthrough looking for workstations with no screensavers or active but non-attended sessions.

2.5: Communicating/Implementing Information Security Requirements

Each hospital facility, as well as the Company's Corporate Campus, must assign a Primary Local Security Coordinator (PLSC) who is responsible for Information Security at the local level. This role fulfills the "Assigned Security Responsibility" requirement within the final Security rule, which states "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity" (Final Security Rule 8377). Since the PLSC is charged with implementing Information Security policies and standards, initial communication and training is targeted toward this role.

As new Information Security policies, standards, and/or security toolkits are approved and posted to the Company's intranet, remote training sessions are conducted. Remote training begins with enterprise conference calls to present and discuss each published security item. Presentations are prepared and distributed prior to the call, including links to the published security toolkit. The conference calls consist of a 45-minute presentation with a remaining 45-minute question and answer session. A transcript of each call is generated, as well as an audio of the call overlaid with the presentation. These items are posted to the Company's intranet for future access by any attendees unable to participate.

Our Company has an established Security Awareness & Education Program for both the PLSC and the general workforce. As new Information Security policies and standards are created, the requirements are incorporated into the Security Awareness & Education Program. This helps ensure the PLSC and the average user receives adequate security training commensurate with the job role.

While we will not discuss an in-depth Security Awareness & Education Program in this practical, refer to "National Institute of Standards and Technology Special Publication 800-50: Building an Information Technology Security Awareness and Training Program" for more information. As Mark Wilson and Joan Hash state in

the Executive Summary, “A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources” (Wilson and Hash ES-1).

2.6: Measuring Compliance

To help ensure on-going compliance with Information Security policy and standards, our Company primarily leverages the Company’s Ethics & Compliance Program and Internal Audit. As part of the Ethics & Compliance Program, a Code of Conduct was developed to ensure the Company meets its ethical standards and complies with applicable laws and regulations. A comprehensive set of compliance policies and procedures, including Information Security, expands upon, or supplements, many of the principles articulated in the Code. An Ethics & Compliance Officer at each hospital facility helps ensure facility level compliance with the Code and therefore Company policies. Additionally, employees annually acknowledge the Code of Conduct by attending Code of Conduct training, and annual performance reviews include evaluations based upon the Code. A 1-800 hotline is available for employees to anonymously report unethical behavior, including policy violations.

As part of Internal Audit, our Company has an Information Systems Internal Audit department. This area performs tests of system controls, including Information Security. Audits are performed to help ensure facility compliance with Company security policies and standards. Any areas of non-compliance are reported to management and an action plan developed. Internal Audit consults with Information Security to clarify and resolve enterprise level security concerns.

Part Three: Closing Comments

3.1: Problem Resolved?

To determine the success of any project, you may ask, “Were all of the potential vulnerabilities and risks related to the initial problem resolved?” Well, there are inherent risks to every Information Security program and related business operations. Additionally, since technology is constantly changing, security controls should also evolve. Therefore, an Information Security program is never complete. While weaknesses in security controls and the possibility for security breaches may always exist, by updating and enhancing our Information Security policies and standards, our Company improved its overall Security program, helping mitigate security risk levels.

3.2: Lessons Learned

During this project experience, many "successes" and "lessons learned" became apparent. Three items to highlight in this practical include the importance of a Security Governance process, the importance of project management in solution delivery, and the need for consistent security documentation (design/format of Information Security policies, standards, etc.).

To help ensure desired security controls are effective and efficient in an operational setting, it is imperative to validate assumptions/theories with business owners. For example, when creating security standards for automatic log-offs and workstation screensavers, it was helpful for us to understand how workstations are used/shared in a clinical setting, having a direct impact on patient care. Involving business owners/representatives in the creation of Information Security policies and standards will not only help ensure applicability and effectiveness of the controls, but will also help gain buy-in and support for security initiatives. Information Security is not merely a technology issue, but also includes people and processes. To accurately and thoroughly understand the people and process aspects of security, business owners and users must be represented in the creation of Information Security policies and standards.

Project management is a critical component to effective solution delivery. At the beginning of our project, I served as both the functional manager and the project manager. As the project evolved, it became apparent that project management principles were critical for success and our project needed more project management expertise. Subsequently, a project manager was assigned and our team began formally defining project requirements. As requirements were identified, we conducted work breakdown sessions to identify all tasks needed to complete/meet project requirements, as well as to identify resources, hours, start dates, finish dates, and task dependencies. This information was then used to create our project plan and verify that the project end date was consistent with the desired end date or federal compliance date. By gathering this information in our project plan, we were also able to identify project resources that were over allocated and assign additional resources/reallocate work to ensure that our project end date would not slip.

The design/format of Information Security policies, standards, and toolkits is critical for successful implementation. Formats should be clear, easy to read and understandable. As a general rule, we attempt to create security documentation at an 8th grade reading level to ensure that users and administrators of various educational backgrounds are able to comprehend and comply with the security controls.

Also related to format, our Company Information Security policies and standards are designed to be controls specific versus product or application specific. This allows more flexibility, when possible, for hospital facilities to make local

implementation decisions. For example, a remote control software standard may define security requirements for remote control software, such as access controls, logging, encryption, etc., but may not require facilities to purchase one specific product (facilities may use freeware that meets the standards). Developing Information Security policies and standards that are control specific versus product specific also have a greater ability to withstand time and advances in technology. Any specific best practices or approved/supported product listing can be included in security toolkits (or procedures) that may be more easily revised over time.

Bibliography

Department of Health and Human Services. "45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule." 12 August 1998. URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/nprm/secnprm.pdf (27 February 2004).

Department of Health and Human Services. "45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule." 20 February 2003. URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (27 February 2004).

Department of Health and Human Services. "45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule." 14 August 2002. URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/finalrule/privrulepd.pdf (27 February 2004).

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). ISO/IEC 17799: Information technology — Code of practice for information security management. United Kingdom: British Standards Publishing Limited (BSPL), First Edition December 2000.

Wilson, Mark, and Joan Hash. "National Institute of Standards and Technology Special Publication 800-50: Building an Information Technology Security Awareness and Training Program." October 2003. URL: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (27 February 2004).

Wood, Charles Cresson. Information Security Policies Made Easy, Version 7. Sausalito, CA: Baseline Software, Inc., October 1999.