Ecora Corp.
500 Spaulding Turnpike, Suite W310
P.O. Box 3070
Portsmouth, NH 03802-3070
http://www.ecora.com

HIPAA

Administrative Simplification

Managing the Impact On Your IT Department

Prepared by Beverly Potter, MHCA

HIPAA Program Manager

E-mail: bev.potter@ecora.com

Table of Contents

Introduction

HIPAA, the Health Insurance Portability and Accountability Act of 1996, is going to significantly impact your IT department. The proposed security regulations have extensive and broad implications to corporate policies regarding the security and confidentiality of individually identifiable health information managed by your IT staff. To ensure organizational compliance and meet federally mandated compliance requirements; organizations must formally evaluate their administrative procedures, networks, and applications to meet HIPAA requirements. This does not require the hiring of new IT staff. Automation of the IT infrastructure documentation process, with the right tools, can significantly reduce the cost of compliance.This paper is about the documentation of your IT servers as part of a "best business practice" plan for compliance with HIPAA security standards.

IT Documentation: How does it apply to the Health Insurance Portability and Accountability Act of 1996?

The inevitable evolution of the information age within the health care industry was secured by the passage of HIPAA (Public Law 104-191.) The federal guidelines for the privacy and security of e-lectronic health information are found within HIPAA: TITLE II. Subtitle F-Administrative Simplification. They are far-reaching and require due diligence to compliance on the part of all health care providers, health care plans, and health care clearinghouses, considered “covered entities” under HIPAA. The privacy regulations set standards for individual identifiable health information. The security regulations set standards for ensuring a secure Information Technology (IT) enterprise-wide network on which the individual identifiable health information is housed. Compliance by these “covered entities” can be viewed as an insurmountable task or as an opportunity to develop enterprise-wide solutions to standardize and simplify health information networks. Although this is not a “technology” law, an integral part of compliance to the privacy standards is compliance with the security standards for e-lectronic health information. The protection of private medical information, as covered by the privacy rules, falls under the security rules. The IT architecture within the Information System (IS) plan of an organization is key to the success and compliance of the business.

Building the security strategy of the IT networks protects the privacy of individual health information and avoids potential civil and criminal penalties, while reducing the organization’s potential security breaches, liability, and possible loss to business reputation. Negative publicity in local and national news compromises the health care organization’s standing in the industry and the public’s view.

Organizational policies and procedures need to be enterprise-wide solutions to ensure an effective security compliance plan: individual departmental policies for the secure and confidential handling of private medical information will not meet compliance with HIPAA. Accrediting agencies look for documentation to prove that policies exist and are followed as written. In accreditation terms: **“If it isn’t documented, it isn’t done.”**

Administrative Simplification: Retooling Health Care Information Technology

The basic mandates to the Department of Health and Human Services (DHHS) for the development of the Administrative Simplification Act are very similar to the basic criteria of documenting your IT system's server configuration settings.

Basic mandates

- Be consistent and uniform
- Low implementation costs relative to the benefits
- Keep information collection paperwork burdens on users as low as is feasible
- Adapt to changes in IT infrastructure
- Precise, unambiguous and consistently applied
- Appropriate references to useable information
- Improve efficiency and effectiveness

What is IT documentation?

IT documentation is a written record of all the configuration settings on the components of a network. These components include servers, applications, routers, switches, databases, and more. Documentation is needed because these components are extraordinarily complex, configurable, and always changing. Technical staff is often responsible for large numbers of servers and devices, each with a complex collection of settings. IT documentation can provide a central repository of all the relevant information for these settings, their impact, and their values or options. What are the general benefits of documentation? A thorough understanding of your existing systems will significantly improve your planning and management of the IT infrastructure. This process starts with detailed documentation. This has not always been a priority because it requires time and resources. Most organizations rarely (if ever) document IT infrastructures because, until now, system documentation could only be done manually. By the time a system was entirely documented, the process had to begin all over again to stay current. Good IT documentation software enables you to:

- Create "Auditor-Ready" documents on demand
- Detect security vulnerabilities
- Simplify server consolidation and network servers
- Understand dependencies between parts of the network
- Optimize network and system configuration
- Standardize configuration settings across all networks and systems
- Accelerate problem resolution and troubleshooting
- Migrate to new platforms: knowing that baseline and subsequent changes are critical
- Manage and preserve system knowledge despite IT staff changes
- Speed up disaster recovery
- Educate new staff and consultants on the organization's IT infrastructure
- Create a standardized "workbook" for outside consultants

Documentation helps streamline migration to new information management applications and new platforms like Windows 2000 and Exchange 2000. These products depend on a well-designed network infrastructure. Studying the existing environment prior to migration helps to plan how you want to reconfigure it to make it more efficient.

What are the cost-benefits of IT documentation?

- One of the highest costs of Information Systems is the IT staff. Trying to deal with the tasks associated with the initial and continual manual documentation of network servers can keep IT staff from completing higher priority projects. Software that automatically documents current network server configurations in minutes in natural-language reports can be less than 10% of the cost of hiring an IT professional to do the same and requires virtually no time / attention from your current staff.

- The quality, utility, and consistency of the information collected are critical for disaster recovery, IT audits, IT staff training, and certification or accreditation agencies.

- Downtime is minimized because current, consistent, and accurate documentation is available for reference. IT systems should be available at all times to provide real-time availability of patient health information to those authorized to access it.

- Due to the increasing demand for a decreasing supply of trained IT professionals, staff turnover can be high. Therefore, an efficient method of knowledge retention and transfer is crucial. The right documentation becomes the basis for training new staff with up-to-date information.

- Security skills and resources are scarce. As organizations move from HIPAA awareness to assessment, development, and finally implementation of compliance plans; demand for these resources will only increase as the 2003 compliance deadline nears. The earlier core tools are in place, the lower the risk of the added expense of the last minute rush.

Why are server configuration settings important?

In terms of security, servers are the last line of defense. Servers are managed through their settings, so documenting them provides a record of how the server is configured, a check for inconsistencies and potential security vulnerabilities, and a useful troubleshooting tool. IT server configurations change regularly. Since it is key that all servers are configured to meet corporate HIPAA compliance plans and policies, IT documentation of server configurations should be a fundamental component of any HIPAA compliant plan to ensure consistent, documented compliance.

How are network and server configurations documented?

Although manual documentation is acceptable, it is time consuming, seldom current, often inaccurate, and a misuse of valuable staff resources. Until now, if network servers were documented at all, it was an expensive and tedious task. Documenting network servers can also be a record-keeping nightmare. The basic steps, in order of occurrence are:

1. Find all the servers on the network.
2. Find the servers' owners and physical locations (this can take days or weeks depending on the size of the organization).
3. Get access to the servers, assuming the owners are cooperative.
4. Locate, record, and examine configuration settings (this requires knowledge of where settings are stored, access to the data/interfaces, and time to open the applications and files required).
5. Interpret the data and settings gathered. Much or all of the information is in "raw-data" format, requiring definition, organization, and explanation to be comprehensible.
6. Produce a report with varying levels of detail appropriate for various audiences, IT staff, IT auditors, accreditation organizations, and compliance auditors.
7. Return to step 1 and repeat the process continually.

Now, the above steps can be accomplished in less time than it takes to make a cup of coffee. Automated documentation tools are available that build consistent, current, and comprehensive natural-language reports for you. These easily attainable and readable reports of network and server configurations provide valuable knowledge of the IT system. This knowledge is crucial for the optimal use of IT staff and IT budgets.

What is the difference between backup tapes and backup documentation for the network servers?

Backup tapes typically record raw data, not core configuration settings. The tapes are usually stored offline or offsite and the data is retrieved in the event of a problem or corruption. IT server configurations aren't necessarily "backed up" unless there is a software program on the system specifically designed for this. Most programs only provide server configuration data in partial or raw-data format and the files require a high-level IT professional to decipher and then reconfigure the servers. If you were not the one who originally installed and configured the servers, you might have quite a time restoring the servers without readily available, readable documentation.

Backing up network servers with documentation provides information on server configuration settings before a disaster occurs. It is important to bring the servers to a state of known configuration settings that worked within the IT security network environment prior to a disaster event. For example, one server might have many different applications that require very specific server configurations on one machine, i.e., Windows NT/2000 and Exchange. Reconfiguring a system from memory or multiple incomplete or generic sources is a fast track to a living nightmare.

How does documentation help with risk analysis & risk management?

Risk analysis is the process through which cost-effective security/control measures are selected by assessing the costs of these control measures against the losses that would be incurred if the measures were not in place. Risk analysis is a required implementation feature of the security management process. During the analysis, it is important to identify any security risks, assess the probability of an occurrence of a security risk, and analyze the potential adverse impact if a security breach occurs. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Ref: Federal Register/Vol.63, No.155/Wednesday, August 12, 1998/Proposed Rules p.43275

What is the difference between a security audit and an IT audit?

HIPAA defines security as mechanisms to guard data integrity, confidentiality, and availability. The HIPAA Security Matrix is comprised of four categories: administrative procedures, physical safeguards, technical security services, and technical security mechanisms. Security audits include both the physical and the informational components of security. Administrative procedures are informational policies such as documenting the IT infrastructure surrounding the data of a healthcare organization: servers, databases, workstations, routers and/or any points of network access.

IT audits encompass some of the physical security audits and all of the information audits. The IT department must have documentation of where hardware components physically exist: the shelf, the room, the floor, the building, the location, the city, and the country. IT audit trail documentation must provide a snapshot of who has access privileges to which servers and if any changes were made to the servers from one point in time to another. They must also document everyone who has physical access to those components at those locations.

The IT department must also audit all of their components from a technology perspective. Configuration settings affect how the components of the network interact with each other from both inside and outside the network. The IT audit provides knowledge that is key to how an organization's network is functioning, to the security of the patient information stored there, and to the survival of the business.

Ref: Federal Register/Vol.63, No.155/Wednesday, August 12, 1998/Proposed Rules p.43269-43271

What are the specific HIPAA rules related to IT documentation?

HIPAA Title II Subtitle F. Sec.262.Sec.1173 (d)

Security Standards for Health Information

- (1)(A) Take into account
  - (i) the technical capabilities of record systems used to maintain health information
  - (iv) the value of audit trails in computerized record systems
- (2)(B) to protect against any reasonably anticipated
  - (i) threats or hazards to the security or integrity of the information

What is the Collection of Information Requirements for HIPAA Security standards? **Ref: §142.308**

- The record-keeping burden associated with meeting and maintaining compliance documentation will vary depending upon individual business needs and the size of the organization. The form, format, or degree of documentation necessary to demonstrate compliance is relative to the extent of the IT network.

- HIPAA Security standard §142.308 states "entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated, updated, and kept current."

- A Contingency Plan and Security Configuration Management Plan are requirements of HIPAA Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability. The following is an overview of the major issues of both plans.

HIPAA Contingency Plan

Requirements

- Routinely updated plan for responding to a system emergency
- Required to perform periodic backups of data
- Preparing critical facilities for continuing operations in the event of an emergency and recovery from a disaster

Implementation

- Application and data criticality analysis
  - An entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits
- Data backup plan
  - A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information
- Disaster recovery plan
  - The part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure
- Emergency mode operation
  - The part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure
- Testing and revision procedures
  - The documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary

Documentation

- A current contingency plan for responding to system emergencies
- An analysis identifying all process-critical applications and data necessary to continue processing should a crisis occur
- A current plan for the back up of all applications and health care data
- Include backups at least once each business day
- Include a procedure for storage of backup media in a secure environment
- Include a data restoration plan should a crisis occur
- Specify appropriate backup retention times
- Have a documented disaster recovery plan in place, including customer and trading partner notification procedures.
- Have a documented emergency-mode operation plan describing procedures and processes, which would enable the continuation of operations in the event of an emergency
- Periodically test and revise contingency plans according to documented procedures

Start a HIPAA-Compliant Contingency Plan for Disaster Recovery

- Understand the need for the availability of information stored on the servers and network. You can only assure availability if the IT servers/networks are working properly.

- Reduce disaster recovery time. IT servers go down whether by natural causes, equipment failure, or human intrusion. Disasters happen. As part of the HIPAA compliance structure, a full disaster-recovery plan must be in place.

- Include hardware in your plan. All the backup tapes in the world won’t help if you don’t have a credible and available server on which to reload the restored data.

- Have auditor-ready IT documentation available on demand.

- Enhance security audits with IT audits.

HIPAA Security Configuration Management

Requirement

- Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.

Implementation

- Documentation
  - Written security plans, rules, procedures, and instructions concerning all components of an entity's security
- Hardware/software installation & maintenance review and testing for security features
  - Formal documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software
- Inventory
  - Formal, documented identification of hardware and software assets
- Security Testing
  - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification.
- Virus checking
  - A computer program that identifies and disables
    - Another virus computer program, typically hidden, that attaches itself to other programs and has the ability to replicate
    - A type of programmed threat. A code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.
    - Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function.

Documentation

- Implement measures, practices, and procedures for the security of information systems
- Have explicit, written documentation covering all components of system security configurations
- Have and employ policies and procedures that provide for periodic maintenance, review and testing of security features of all hardware/software installations
- Have and employ policies and procedures for maintaining an inventory of hardware and software assets
- Provide for periodic testing of the security features and procedures of the system

- Use effective virus protection and have policies and procedures in place for daily maintenance/updating of virus signatures, incident notification and response
- Identify and disable a “virus” computer program
    - Identify and disable a code embedded within a program
    - Identify and disable hostile macro code that is attached to office automation software (word processing, spreadsheet and presentation)
    - Identify and disable known hostile executable programs, either stand-alone or attached to e-mail.

Summary

Until recently, creating comprehensive documentation and keeping it current was tedious, time-consuming, expensive, and not legally mandated. Federal HIPAA law makes improved data management and the real-time availability of secure and confidential patient information a critical part of doing business in the health care industry. The common backbone of each of these is the IT systems on which the information resides. The implementation of security matrixes that meet the compliance requirements of HIPAA is best served by having core tools on which to build and maintain an organization’s IT infrastructure.

Being able to provide automated documentation of IT servers, with little human intervention, is a technology value-added solution to the HIPAA security compliance requirements facing health care organizations. Best practices need best solutions. Documentation is the key to proving an organization’s compliance with HIPAA.

REMEMBER: IF IT ISN’T DOCUMENTED IT ISN’T DONE

About the author

Beverly Potter has 26 years of clinical research experience at a major academic medical center in Boston, MA. She attained her graduate degree in Health Care Administration from Simmons College in Boston, MA and was a lecturer in health sciences at Northeastern University College for one year. Beverly was instrumental in the formation of a national association for NIH GCRC Core Laboratories. Her major area of interest was the development of an integrated clinical research information system. She is a consultant and speaker for the health sciences, focusing on federal legislation as it pertains to the health care industry, specifically HIPAA.