

HIPAA Compliance

SystemExperts Corporation

Jonathan Gossels and Landon Curt Noll

Abstract

In 1996, Congress passed the Health Insurance Portability and Accountability Act (“HIPAA” and the “Act”). The intent of this Act was to simplify and standardize the administrative functions of healthcare. The Administrative Simplification section (Title II) of this law requires adaptation and implementation of standards for the security, privacy, and management of electronic healthcare transactions.

The law applies to all healthcare organizations that choose to exchange data electronically. It further requires that such organizations, providers, insurers, billing agencies, clearinghouses, vendors and employers comply with the Act by the year 2003. Some portions of the Act required compliance as early as the fall of 2002.

As healthcare providers and organizations migrate their patient records to various electronic forms, the actions necessary to become HIPAA compliant will vary. Consulting with an experienced information security organization can greatly smooth the transition.

Inside

- How will HIPAA affect healthcare organizations?
- What are the HIPAA security requirements?
- How can an organization maintain compliancy?
- Resources to find out more about HIPAA.

Contact Information

**Boston New York Washington D.C Tampa
San Francisco Los Angeles Sacramento**

Toll free (USA only): +1 888 749 9800

From outside USA: +1 978 440 9388

www.systemexperts.com

info@systemexperts.com

How does an organization become HIPAA compliant?

Becoming HIPAA compliant requires substantial effort but should not be traumatic for most organizations. In fact, many of the Act's requirements are simply good business practices for the management of sensitive information and records. In particular the Act requires organization-wide implementation of:

- Administrative procedures aimed at creating or enhancing appropriate information security policies
- Appropriate industry accepted safeguards and measures to adequately protect the healthcare information within your organization

How will HIPAA affect healthcare organizations?

HIPAA will affect the way that your organization handles health care records, information, and transactions. Your organization will need to comply with the HIPAA security, privacy, and management requirements for electronic healthcare information.

Healthcare organizations will be required to address the following four areas as defined by the Department of Health and Human Services (DHHS):

1. **Administrative procedures** — Procedures for establishing and enforcing security policies
2. **Physical safeguards** — Safeguards that protect physical computer and network facilities
3. **Technical security services** — Services that protect, control, and monitor access to health care information
4. **Technical security mechanisms** — Mechanisms for protecting information and restricting access to data transmitted over networks

The entire service and product delivery cycle must become HIPAA aware and where needed, brought into compliance. Information and data security will need to become a priority throughout your organization.

In order to satisfactorily comply with this Act, your organization will need to assess which areas are susceptible to electronic vulnerabilities and identify where your information management practices are inadequate. Your network, systems, procedures and appropriate personnel will require a comprehensive review. Your operation will need to undergo a

thorough risk assessment. Although such a thorough analysis may seem extreme, it is necessary to establish a strong foundation from which your operation will be able to build a reliable information security posture.

Your management and technical teams will need to develop a comprehensive plan to become HIPAA compliant. In particular your organization will need to:

- Develop a course of action outlining detailed roles, responsibilities and time frames for HIPAA compliancy
- Determine the impact of the electronic healthcare information transactions and identifier standards on your organization
- Enable and adjust your organization's current environment to support standard HIPAA electronic transactions

What are the HIPAA security requirements?

HIPAA mandates the manner in which your Information Systems handle healthcare information. These mandates touch upon your entire IS infrastructure including applications, databases, computer systems, network, personnel, procedures, and your physical site. The security of patient healthcare information and data is central to these requirements.

Some of the HIPAA requirements are highly detailed such as; unique user identification, auto logoff, audit trails for certain transactions, virus detection, backups and disaster recovery. Changes in hardware and/or software may be required to meet the regulations. In other areas, HIPAA provides only broad guidelines.

HIPAA mandates several fundamental security areas. These include:

Administrative Procedures: The proper introduction, management, and dissemination of patient healthcare information within a HIPAA compliant operation will necessitate embracing certain security practices.

Organizations need to create and maintain the following:

- Chain of trust partner agreements for transmitted healthcare data
- Emergency response plan for system & network failures
- Schedule for internal system & network security audits

- Process for providing access to healthcare information
- Employee security responsibility training program
- Master policy for healthcare data processing
- Multiple levels of authorization for healthcare access
- Software, system and network change management process
- Security incident and response procedure
- Healthcare access termination process for employees and partners
- Position of a Chief Security Officer
- Positions for maintaining and auditing system & network security
- Security training program for security related personnel

Information and Data Security: All aspects of your information and data systems must provide a level of HIPAA compliant data security including access control, data field validation, data encryption, accountability, and record management. An inventory of your critical information assets and individually identifiable health records are also required.

Each organization will need to assess its disaster recovery needs. If its current disaster recovery methods are inadequate, it will need to design and implement an effective enterprise-wide recovery program. Such an assessment includes all facets of disaster recovery planning: identifying vital business processes and applications; determining financial impacts of disasters; identifying potential risks; and defining critical technology and resources during disaster situations.

Healthcare organizations will need to establish and maintain the following security services:

- Healthcare information and data access controls based on “need to know”
- System and network activity and access audits
- Method to obtain and record consent for use and disclosure of healthcare data
- Healthcare data integrity validation
- Authentication / validation of identity of an entity accessing healthcare data

Systems Security: The combination of your applications and the computer systems on which they run must provide a level of HIPAA compliant system security including user authentication, access control and audit logs. Your management and technical teams will need to provide an analysis of your current business and IS practices and

strategies, and develop a set of security architecture principles and a standards-based framework that can be used to make management and technology decisions consistent with HIPAA security objectives including:

- Cryptographic data privacy
- Data access control based on an authenticated entity's authorization
- Data integrity checking
- Message authentication
- Security alarm system
- Secure audit trail logs
- Secure system event logging
- Intrusion detection system
- Log filtering system

Process Security: Many business processes extend beyond the systems themselves and are sources of potential security exposure. HIPAA requires that these risks be assessed as well. Such a review addresses policy, organization, personnel, physical controls, asset classification and control, system access control, network and computer management, business continuity, application development, and maintenance and compliance processes.

Network Security: Your computer system and network infrastructure must provide HIPAA compliant network security including system authentication, network traffic access control, traffic filtering, intrusion detection, data integrity protection, and message privacy encryption.

A thorough security audit of your present networks, including penetration testing and web application exposure profiling is usually a good place to start. With a clear understanding of your present network security posture, you will be able to develop a program to correct your vulnerabilities and create or enhance appropriate security policies and practices.

Physical Security: The facilities that house your data storage, and systems and network infrastructure must provide HIPAA compliant physical access protection.

Your current physical security and emergency plans will require an assessment. You will need to ensure that the following safeguards are in place:

- System & network hardware installation/removal procedure
- Physical access controls to systems & networks
- Physical access controls to healthcare related workstations

- Physical access controls to data backups and data storage
- Visual activity logs near critical system & network equipment

How can you stay HIPAA compliant?

As with any enterprise, maintaining a secure environment requires vigilance and consistency. Satisfying HIPAA may require your organization to enhance its current set of practices and procedures. Once those new policies and practices are in place, you should review them periodically (either internally or by using an outside third-party) to make sure they are effective.

It is important to understand that while the HIPAA requirements may seem onerous, they are not substantially different than what would be necessary for any organization to protect its electronic resources and the privacy of its records. Since these practices are new for many healthcare organizations, it will take some time to get used to them and to become security aware in daily behavior.

Since HIPAA security compliance covers a wide range of issues, it is important not to delay. Compliance with most of the requirements will be straight forward for most

organizations. Satisfying certain of the requirements will be more of a challenge. Starting the assessment work early to identify what really needs to be done will enable your organization to develop sensible plans that can be implemented at an affordable cost.

Resources to find out more about HIPAA

Health Care Financing Administration
<http://www.hcfa.gov/medicaid/hipaa/default.asp>

American Hospital Association HIPAA links
<http://www.aha.org/hipaa/links.asp>

Health Hippo: HIPAA Page
<http://hippo.findlaw.com/hipaa.html>

HCFA HIPAA Fact Sheet
<http://www.hcfa.gov/facts/f9702as.htm>

Searchable HIPAA Regulations
<http://www.hipaadvisory.com/regs/>

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Network-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800.

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento
www.SystemExperts.com **info@SystemExperts.com**