Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

HIPAA Security Standards v1.2d

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, is legislation that was enacted to streamline healthcare industry inefficiencies, reduce paperwork, make it easier to detect and prosecute fraud and abuse and enable workers of all professions to change jobs, even if they (or family members) had pre-existing medical conditions. The focus of this paper is the creation of certain baseline information security standards to protect electronic medical records.

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

HIPAA Security Standards v1.2d

Introduction

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords have significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, State and Federal agencies, Medicare and Medicaid beneficiaries, and researchers. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. (Rada) Couple such Internet-based security risks with the everyday risks associated with processing thousands of claims and other related medical documents, the Federal government felt a necessity to take action to protect the confidentiality of medical records.

As so you have it – The Health Insurance Portability and Accountability Act of 1996, or HIPAA as it has come to be known. While this piece of legislation was devised to address a number of issues, a key element and the focus of this paper, is the creation of certain baseline information security standards to protect electronic medical records. Many argue that these standards go to far, placing an undue burden on the healthcare industry, creating the next "Y2K", and padding the pockets of consulting organizations. Yet others argue that the standards do not go far enough, leaving the American public at the mercy of those it trusts the most, its doctors and other healthcare providers, to ensure the privacy of its most personal information.

HIPAA – A Brief Overview

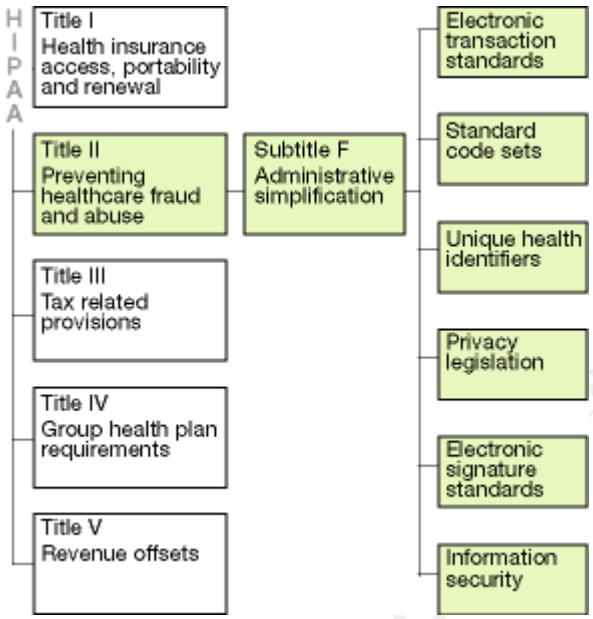
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was the result of efforts by the Clinton Administration and congressional healthcare reform proponents to reform healthcare in a way that would streamline industry inefficiencies, reduce paperwork, make it easier to detect and prosecute fraud and abuse and enable workers of all professions to change jobs, even if they (or family members) had pre-existing medical conditions.

The HIPAA legislation had four primary objectives:

1. Assure health insurance portability by eliminating job-lock due to pre-existing medical conditions
2. Reduce healthcare fraud and abuse
3. Enforce standards for health information
4. Guarantee security and privacy of health information

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The law is divided into five key sections, as shown in the chart below. It is within the second section, Title II – Administrative Simplification, that the government addresses the need for security standards to protect patient data, and sets forth-specific requirements that those affected by HIPAA must adhere to.



Source: Arthur Andersen LLP

The HIPAA regulations do not affect every organization in the healthcare industry, but those that fall into one of three categories:

1. Health care clearinghouse.

The statute defines a "health care clearinghouse" as a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. It further explains that such an entity is one that currently receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended recipient and forwards the processed transaction to appropriate payers and clearinghouses, as necessary, for further action.

2. Health care provider.

As defined by section 1171(3) of the Act, a "health care provider" is a provider of services as defined in section 1861(u) of the Act, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes health care services or supplies. The regulations would define "health care provider" as the statute does and clarify that the definition of a health care provider is

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

limited to those entities that furnish, or bill and are paid for, health care services in the normal course of business.

3. Health Plan

A "health plan" would be an individual or group health plan that provides, or pays the cost of, medical care.

The Security Standard

Those responsible for the creation of the HIPAA security standard identified that "There is no recognized single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and technical mechanisms) that must be in place to preserve health information confidentiality and privacy… Therefore, we are designating a new, comprehensive standard, which defines security requirements to be fulfilled." (Federal Register)

In creating this new standard, the government recognized that there are in fact many security standards in existence today. They have been created by different groups with different objectives, and thus, could not be used in whole to address the needs of HIPAA. To establish a framework from which to build the HIPAA standard, a set of high-level concepts was created, which state that:

1. The standard must be comprehensive.
2. A need for a standard that addressed all aspects of security in a concerted fashion.
3. The standard must be technology neutral.
4. The standard must be scalable.

In general, the authors of HIPAA set forth to design 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." (Federal Register)

More specifically, the HIPAA security standard requires those covered by its rules to address four key areas:

1. Administrative Procedures – these rules call for the creation of documented procedures and policies aimed at guarding the integrity, confidentiality and availability of patient data. These rules include items such as disaster recovery and/or business continuity plans, information security policies and procedures, information security testing or assessments, awareness training for employees, and a set of sanctions for those in violation of these policies.
2. Physical Safeguards – these rules include provisions necessary to ensure that physical access to patient data in restricted and that data is protected from known hazards and unforeseen risks such as environmental disasters.
3. Technical Security Services – these rules address the need to protect, control and monitor access to patient records via the use of computer systems. Specifically,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

HIPAA mandates that information systems have the capability to create audit trails and provide an in-depth historical record of who has accessed data. It requires that medical systems be capable of restricting access and provide non-repudiation.

4. Technical Security Mechanisms – these rules address the need to protect data as it is transmitted over computer networks. Included are requirements surrounding encryption of data, event reporting, audit trails, etc.

In addition, HIPAA addresses the need to create a standard for the healthcare industry with regards to the use of electronic signatures. Widely accepted as a way to "sign" electronic documents and provide a means of proving the identity of the sender, electronic signatures are viewed as a vital component of using the Internet to share patient data and transmit orders, prescriptions, etc. However, many types of electronic signature technologies exist, and until HIPAA, no standard within the healthcare industry had been put in place. Specifically, HIPAA requires that a standard be set that addresses the need for message integrity, non-repudiation and user authentication when using electronic signatures.

Reacting to the HIPAA Legislation

Few legislative acts in recent memory that affect the healthcare industry have spurred such a swift, strong and overwhelming reaction from industry members, as has HIPAA. Take for instance, an article in the current Journal of the American Medical Association, which argues "The Health Insurance Portability and Accountability Act may threaten the ability of health care professionals to use and share full medical information when treating patients," and "the provision of patient care in a timely and proficient manner." (Gostin) Articles like this, and letters to legislators continue to pour in as organizations react to and plan for HIPAA.

However, not everyone is against HIPAA. In particular, information security professionals across the country are saying "its about time." While the cost of preparing a large hospital for HIPAA will be expensive, many practitioners of information security argue that what the law requires is just good business. Most hospitals, until recently, had distributed information systems environments. Many departments had their own IT staff and supported their own systems. Standards, policies, etc. did not exist and as such, security over patient data was weak at best. Proponents of the law argue that it would only take one large lawsuit of improper disclosure of a patient's file to cover the cost of HIPAA. Furthermore, they say, healthcare institutions have a moral responsibility to ensure that a patient's medical record is secured.

Finally, one of the reasons for the creation of HIPAA is to achieve efficiencies in healthcare. Experts argue that over the next several years, HIPAA will create billions of dollars of savings in the industry, improving profits while making healthcare more affordable.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Whatever side of the argument one falls in, emotions are running high. It is doubtful that no more changes to the HIPAA standards will occur. In fact, one must remember that at this time, the security standards have not been finalized, and may take on a whole new look when all is said and done.

Getting Ready for HIPAA

Much has been said and written about the HIPAA security standards. In any case, all agree that the cost and effort to achieve compliance with all that HIPAA mandates will be significant. In fact, The Gartner Group estimates that HIPAA compliance will equal or exceed Year 2000 compliance costs. Meanwhile, violating the HIPAA regulations can lead to US$250,000 in fines and up to 10 years imprisonment. Other risks include the threat of civil litigation, negative effects on accreditation status, damaged reputation and loss of contracts that require HIPAA compliance.

Many in the healthcare industry continue to fight the standard and are pushing legislators to either ease the requirements or due away with HIPAA altogether. As recently as this May, members of the House Committee on Ways and Means were encouraged by their constituents to send a letter to President Bush, asking the administration to fix the rule to "balance a patient's privacy rights against legitimate health care needs." (Lutes) While the battle continues, most healthcare and security experts agree that HIPAA is not likely to go away, and that providers, health plans and clearinghouses should begin to take action now to achieve compliance by the mandated dates.

Consultants and others charged with assisting affected entities to address their HIPAA needs generally espouse a five-phased approach to HIPAA compliance, such as the one depicted below from Arthur Andersen LLP.

1. Educate — Enhance personal and organizational awareness of HIPAA among your executive management team.
2. Evaluate risk — Perform a baseline HIPAA readiness assessment and study your current and future systems' functionality.
3. Develop an action plan (based on the final regulations) — Incorporate your security infrastructure and consider new technology/infrastructure in your action plan.
4. Implement (based on the final regulations) — Obtaining HIPAA compliance will require a well-coordinated, resource-intensive effort for every healthcare organization.
5. Monitor — One achieved, HIPAA compliance must be maintained. Responsibility for monitor HIPAA compliance must be assigned and a plan to monitor it put into place.

A program like this one generally cannot be completed overnight. The government has allowed affected organizations 24 months to become compliant with the law. For large institutions, this may not be enough time. Others contend that even if it were,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the cost of meeting each standard letter-for-letter is too high. They say they will take a prudent approach to compliance, and focus on the areas that present the greatest risk to both patient records as well as the organization itself. The key, however, is to begin sooner rather that later.

Conclusion

The Health Insurance Portability and Accountability Act has generated much debate, a good amount of fear and a lot of work for many. The Security Standards are likely to be the most difficult and costly piece to implement, but may also do the most to protect the privacy of medical information. It is an exciting time for information security professionals – they will get to "play" with new technology and see the role of information security within their organizations take on a new light. Let's get busy!

Sources:

Arthur Andersen LLP:
http://www.arthurandersen.com/website.nsf/content/IndustriesHealthcareResourcesHIPAAResourceCtr?OpenDocument

Gostin, Lawrence. "National Health Information Privacy – Regulations Under the Health Insurance Portability and Accountability Act" *Journal of the American Medical Association*, Vol. 285 No. 23, June 20, 2001
http://jama.ama-assn.org/issues/v285n23/abs/jlm10003.html

U.S. Department of Health and Human Services. "Security and Electronic Signature Standards; Proposed Rule" *The Federal Register*, 45 CFR Part 142, August 12, 1998
http://aspe.hhs.gov/admnsimp/Index.htm

Rada, Roy. "How HIPAA Compliant Can Any Technology Be?" HIPAA Advisory: Phoenix Health Systems
http://www.hipaadvisory.com/

Lutes, Mark "The HIPAA privacy regulations: After the hype" *TIPS on Managed Care*,Vol.5 No.2, March/April 2000
http://www.hipaacomply.com/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

QUESTION & ANSWERS (answers in Red)

1. HIPAA requires that affected entities prepare a disaster recovery plan (T/F)
2. The first, and one of the most important steps to prepare for HIPAA is to:
    a. Contact vendors
    b. Complete Assessment
    c. Educate the organization about HIPAA
    d. Hire a consultant
3. Which of the following was not an objective of HIPAA
    a. Prepare for a national healthcare system
    b. Reduce healthcare fraud and abuse
    c. Enforce standards for health information
    d. Guarantee security and privacy of health information
4. HIPAA compliance is expected to be less costly than Y2K (T/F)
5. Which of the following is NOT one of the four areas the security standards cover
    a. Physical Safeguards
    b. Technical Security Mechanisms
    c. Virtual Private Networking
    d. Administrative Procedures
6. Covered entities will have 36 months to comply with the HIPAA standards (T/F)
7. Which of the following is not a type of covered entity
    a. Health Plan
    b. Patient
    c. Clearinghouse
    d. Provider
8. Many in the information security business feel that the security standards specified by HIPAA are good business practices, regardless of HIPAA (T/F)
9. The HIPAA legislation has not yet been signed into law (T/F)
10. The high-level concepts utilized as a framework to create the security standards include all of the following except
    a. The standard must be comprehensive
    b. A need for a standard that addressed all aspects of security in a concerted fashion
    c. The standard must be technology neutral
    d. The standard must utilize the leading vendors products in each area

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced