Global Information Assurance Certification Paper

HIPAA Compliance Beyond Health Care Organizations – A Primer
GSEC Practical Assignment Version 1.2d
Peter Koso
May 24, 2001

Introduction

This review is intended to assist Security Officers with the first implementation steps for meeting any or all of the requirements included in HIPAA. Although HIPAA applies to many entities within the health care system, it also affects many other businesses whose client base includes health care companies. If you do not know whether HIPAA affects your company or how to evaluate your options, this document should help. There are many aspects of HIPPA covering such areas as Human Resource Policies on insurance portability as well as the reduction and restructuring of EDI forms for claims processing. This document is intended as a Primer for the Privacy and Security sections of HIPPA Covered under Title II – Subsection F – Administrative Simplification. It is these sections that can apply to businesses outside of health care.

HIPAA stands for Health Insurance Portability and Accountability Act. It is federal legislation intended to implement simplifications in the administration of health care plans and their associated claim and payment processes. Health care organizations will need to be fully compliant with this legislation no later than April, 2003. HIPAA mandates no specific technical practices for privacy or security and is by design "Technology Neutral". However, there are many policy and procedural requirements that must be implemented by any *covered entity* (see definitions below). Although no technical solutions are specified, there are areas that most likely will require a technical solution and must be addressed if you are a *covered entity* or if you plan to do business with a *covered entity*. To HIPPA, technology is only necessary as part of supporting your company's privacy and security policies. There is no such thing as a HIPAA compliant technology.

In order to determine if your organization has obligations covered by HIPAA, you first need to understand certain terms defined in the federal regulation.

Definitions

Covered Entity: "… all health plans, all health care clearinghouses, and all health care providers that transmit health information in an electronic form in connection with a standard transaction."[1]

Protected Health Information: "… individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity."[2]

Individually identifiable health information: "… information that is a subset of health information, including demographic information collected from an individual, and that:

(a) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

(b) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

(i) Which identifies the individual, or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[3]

Standard Transaction

"*Standard* means a set of rules for a set of codes, data elements, transactions, or identifiers promulgated either by an organization accredited by the American National Standards Institute or HHS for the electronic transmission of health information.

Transaction means the exchange of information between two parties to carry out financial and administrative activities related to health care. It includes the following:

(1) Health claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health claims status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions as the Secretary may prescribe by regulation."[4]

Business Partner: "… a person to whom a covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity….."[5]

Affected Organizations

If your company does business in the health care environment, the first step is to determine whether your business is affected by HIPAA. There are two groups defined by HIPAA that must comply with the regulation. They are defined as a *Covered Entity* and a *Business Partner (*see above). *Covered entities* must comply with all aspects of HIPAA and it is towards these organizations that the legislation is directed. *Business partners* would be required to comply with HIPAA through individual contracts with each *covered entity*. The purpose of these contracts would be to extend the "sphere of privacy"[6] coverage that exists for the primary health care organization on to the *business partner's* organization. Remember, as a *business partner*, you are not directly accountable to HIPAA. It is the *covered entity* – through your new contract with them – that will impose HIPAA compliance on your organization.

The fact that a company does business in the health care environment does not in itself mandate HIPAA compliance. It depends on how you interact with the *covered entity*. You must comply with HIPAA (through a contract with each individual *covered entity*) if you store or process p*rotected health information* as described above. Take the time to read and fully understand the definitions listed above. It is how your company relates to these definitions that determines your obligations under HIPAA.

Possible Course of Action – De-Identify the data

Although this option is not viable for most business models, it does represent a way to avoid the administrative burden of HIPAA compliant contracts. If your business does not require that you possess individually identifiable health information, you may choose to require that all *covered entities* with whom you do business provide you with "De-Identified" information. To be considered "de-identified" all of the following must be removed: Name; address, including street address, city, county, zip code, or equivalent geocodes; names of relatives and employers; birth date; telephone and fax numbers; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/ license number; any vehicle or other device serial number; web URL; Internet Protocol (IP) address; finger or voice prints; photographic images; and any other unique identifying number, characteristic, or code (whether generally available in the public realm or not) **and** you must also insure that "any reasonably anticipated recipient of such information could [not] use the information alone, or in combination with other information, to identify an individual."[7]

Probable Course of Action

In the event that your organization must possess or process *protected health information*, **and** your company does not fit the definition of a *covered entity* your obligations are not specifically defined by HIPAA. Rather, each *covered entity* is required to bind your organization in a contract that mandates that your business adhere to the same privacy standards as the *covered entity*. In the case where a company provides services to multiple *covered entities*, the task of HIPAA compliance becomes very large as each *covered entity* may develop a different policy for how they process and disseminate *protected heath information*. Under HIPAA a contract must exist between every *covered entity* and each of their *business partners* prior to sharing any *protected health information*. This contract has many specific requirements. These include:

- Prohibiting the use of *protected health information* for any use not specifically stated in the contract and requiring a publicly available statement of how this information is used and disclosed.
- Requiring safeguards for the data and the reporting of any unauthorized disclosure.
- Requiring that the HHS can review internal practices for compliance.
- Requiring audit trails for all people who have routine or special access to data.
- Requiring access by individuals to view and update their own health information
- Agreeing to destroy all protected health information at the end of the contract.
- Requiring a provision to terminate the contract for non-compliance

The intent of this contract is to bind the *business associate* to the same ethical and legal standard as the *covered entity*. *Covered entities* have a very limited ability to disseminate protected data and they are required to put those same restrictions onto your business. Basically this means that unless you are disclosing *protected health information* for the purposes of treatment or payment, you need each individual's written permission to release their data and that permission is revocable by the individual.

The result of these stipulations is to require every company looking to do business in the health care arena that possesses individually identifiable health data to be as HIPAA compliant as any hospital or doctor's office. In the end, every affected business will need to enact very strict privacy and security policies.

Internal Audit

Begin the journey towards HIPAA compliance with an internal review of current systems, business processes, and storage mechanisms that handle *protected health information*. It is this information – and this information alone – that HIPAA addresses. It is important at this stage to document all sources and storage locations of this data along with the individuals (or roles) that have access to the data.

Once you have a formal understanding of how *protected health information* moves through your company, you can begin to develop policies to address HIPAA compliance. HIPAA (like most privacy/security issues) is mostly about policy. The fundamental concerns being addressed by HIPAA are intended to be handled through the implementation and adherence to a clear policy that is monitored, enforced and verified by technology.

Privacy and Security – Two Necessary Policies

One of the important concepts to HIPAA is that, unlike Y2K, it is not a destination, it is a process. A company cannot certify that its current systems and policies are HIPAA compliant and stop there. HIPAA mandates an ongoing process of auditing existing policies, data access rights, and employee training to insure ongoing HIPAA compliance. As a security officer, one can encounter push-back to developing and enforcing security rules that may appear burdensome or counter-cultural. If this has happened to you, HIPAA may provide you with the legal authority to successfully implement strict, enforceable policies.

Although HIPAA does not specifically mention the need for a privacy policy for *business partners*, the required contracts between *covered entities* and *business partners* do require that the privacy of health data is audited and verifiable. The only practical way to do this is to enact strict privacy and security policies. HIPAA also requires *covered entities* to appoint a privacy officer and a security officer. These too, while not mandated, are advisable for a *business partners* in order to insure that their policies are up-to-date and enforced.

The privacy policy must insure that *protected health information* be carefully guarded and only revealed following strict guidelines. Key components of a privacy policy include:

- A statement as to what information maintained by the company is to be considered private.
- A procedure to disclose protected information that has been authorized for release.

- A procedure to deny disclose protected information that has **not** been authorized for release.
- A section on staff training with an ongoing education requirement (maximum three years between trainings)

The requirements for a security policy under HIPAA are much more extensive and detailed containing over 20 specific areas that require policies and procedures in place to insure the integrity, availability and security of *protected health information*. There is an extensive list known as the HIPAA Security Matrix contained within the legislation that details each of the areas required. The level to which each of these areas needs to be addressed is intentionally undefined. Each organization must review its exposure, risk, and cost of abatement and set its own level of compliance. A two person business has a much different risk/benefit than a 400 bed hospital. HIPAA accounts for that by leaving the specifics of compliance up to each individual organization. Key areas are as follows:

- Contingency plans for disaster recovery, including incident response procedures
- Formal mechanisms for authorizing access to data.
- Background checks, personnel security training, and formal hiring and termination procedures
- Physical and media access controls.
- Policies for end-user workstation and laptop security
- Strict audit of routine and ad-hoc access to protected data.
- Standard network security including physical access control, virus protection and firewalls.

Going Forward

Accurate, enforceable privacy and security policies are the foundation for HIPAA compliance but their scope and impact will vary by organization. No one has tested HIPAA "in the courts" yet, and most experts agree that much of the final practical approach will be determined through a combination of the legal system and the court of public opinion. It is generally believed that any organization stigmatized as being "lax" in protecting personal health information will have trouble maintaining its business relationships. This negative effect on business has already been felt at hospitals where security breaches have been made public.

As with many public policy issues, HIPAA compliance will become a combination of form and substance. A formal legal review of all documents, a formal training program, and a long term budget line item are all part of implementing HIPAA. Depending on the organization, substantial cultural change may also be required. Restricted access to protected health data, coupled with detailed auditing may be a difficult cultural change. Every part of the organization must be part of the compliance program if it is to succeed.

Quoted References

1. Standards For Privacy of Individually Identifiable Health Information: Proposed Rule Federal Register, Vol. 64. No 212, Wednesday, November 3, 1999, Page 59927

2. Ibid, Page 59927

3. Security and Electronic Signature Standards; Proposed Rule Federal Register, Vol. 63. No 155, Wednesday, August 12, 1998, Page 43248

4. Ibid, Page 43265

5. Standards For Privacy of Individually Identifiable Health Information: Proposed Rule Federal Register, Vol. 64. No 212, Wednesday, November 3, 1999, Page 60052

6. Ibid, Page 59924

7. Ibid, Page 60054

Complete List of References

Security and Electronic Signature Standards; Proposed Rule
Federal Register, Vol. 63. No 155, Wednesday, August 12, 1998

Standards For Privacy of Individually Identifiable Health Information: Proposed Rule
Federal Register, Vol. 64. No 212, Wednesday, November 3, 1998

Myths and Facts about the HIPAA Privacy Regulation, Ms. Janlori Goldman, Director, Health Privacy Project, Georgetown University.
http://www.hipaadvisory.com/views/Patient/myths.htm

Successful HIPAA implementations require comprehensive training, on-going employee education, Michael Doscher
http://www.hipaa-u.com/news/04-19-01.html

Overview of HIPAA's Security Concepts, Marcia Branco, April 13, 2000
http://www.sans.org/infosecFAQ/legal/HIPAA.htm

Preparing Organizations For HIPAA, James M. White, December 17, 2000
http://www.sans.org/infosecFAQ/legal/HIPAA3.htm

HIPAA and Compliance, John Rockwood, December 21, 2000
http://www.sans.org/infosecFAQ/legal/HIPAA2.htm

HIPAA – Security Standard, How It Will Impact Healthcare & Security in Information Technology, Gaudy Alvarez, January 27, 2001
http://www.sans.org/infosecFAQ/legal/HIPAA4.htm

HIPAA: What it Means For Privacy and Security, Stanton Meyer, March 3, 2001
http://www.sans.org/infosecFAQ/legal/HIPAAsec.htm