Global Information Assurance Certification Paper

Preparing Organizations For HIPAA

James M. White
December 17, 2000

The Health Insurance Portability and Accountability Act of 1996 (referred to as HIPAA hereafter) was enacted with the goal of making employee health insurance portable and to simplify its administration. As with previous Federal regulations "mission creep" can generate additional issues that must be addressed and HIPAA is no exception. In the four years since it's passage the Act has generated a variety of issues related to its implementation, inspection for compliance and enforcement.

The purpose of this document is to discuss HIPAA requirements and the general process organizations should follow to secure identifiable patient information from unauthorized parties and the to bring themselves into compliance. Privacy issues, electronic signatures and the creation of a standard transaction data set for the transfer of patient and procedure information will not be addressed in this paper.

When addressing any new issue it is best if the security professional asks the basic questions of Who, What, When, Where, Why and How to quickly get to the important issues and avoid spending time on ancillary matters that can be addressed later.

In their shortest form the questions (and their answers) are:

Q: Who is affected?

A: Hospitals of any size, Group Practices, Individual Health Practitioners, Health Insurance Carriers, Insurance Clearinghouses, and any other organizations that share identifiable patient information electronically must conform to HIPAA standards for security[1].

Q: What must be protected?

A: All electronic records that contain identifiable patient information (IPI) and their progeny (i.e. printouts, backup tapes, CD-ROMs) whether static or in transit (residing on a hard drive or being transmitted over intra or extra net). Identifiable Patient Information is defined as "…any information including demographic information collected for an individual, that— (i) 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."[2]

Q: When will these regulations go into effect?

A: Compliance inspection and enforcement is expected to begin 24 months after publication of the final security rules for large organizations and compliance inspections for all other organizations should start 12 months after that date[3]. At the present time HHS says the final rules will be published in early 2001.

Q: Where can I go for more information?

A: The single best authority is the Health and Human Services Administrative Simplification web site at http://aspe.hhs.gov. This site is devoted specifically to all HIPAA issues.

Q: Why must my organization comply with these regulations?

A: To avoid the penalties for noncompliance. As written the law provides for fines of up to $250,000 per year and imprisonment of up to 10 years for violations of HIPAA security standards[4]. However the greatest threat would be the refusal of the Health Care Financing Administration (HCFA) to approve any payment requests made by a negligent organization

Q: How much of the existing security services may be retained?

A: Fortunately the two controlling Federal agencies, Health and Human Services (HHS) and the Health Care Financing Administration (HCFA) do not require the installation or implementation of specific hardware or software. Their only requirement is that organizations that fall under HIPAA guidelines must "implement safeguards to protect it (IPI) from inappropriate access, use or disclosure."[5]. Therefore already established electronic safeguards may not need to be replaced.

Q: (Bonus Question) What are the categories that need to be examined?

A: If we exclude electronic signatures, all of the HIPAA security requirements fall under at least one of five broad categories. These categories are: administrative procedures, physical safeguards, security configuration management, technical security services and technical mechanisms[6].

So, having defined the challenge, and mindful that no two organizations data systems are identical, what reasonable and prudent steps should security professionals take to bring their organization into compliance?

First of all, compliance implementation is going to be a manpower and money issue so the first people on board must be the senior decision makers for your

organization. This step shouldn't be too hard since the penalties for non-compliance are both well defined and mandatory as is the time frame. At this time the organization should also decide which member of management shall be responsible for successful HIPAA compliance implementation.

Having secured management support the next step is to form a working group (or groups) to consider the categories mentioned, i.e.

Administrative Procedures
Physical Safeguards
Security Configuration Management
Technical Security Services
Technical Mechanisms

When examining each area the responsible working group should ask "What is happening, or not happening here to prevent Identifiable Patient Information from being accessed by unauthorized parties?" Two items that every workgroup member would find very worthwhile to review are the HIPAA Security Matrix Mapping addendum at http://aspe.hhs.gov/amnsimp/nprm/sec16.htm, and the section on Critical Steps[7] published on IBM's security web site. Both are good tools for giving workgroups a foundation for their research and the Matrix Mapping addendum also has the handy feature of cross-reference tagging to known published standards.

Having formulated their initial findings these groups should then look for input from every department on the effect of their decisions. Certainly the security and maintenance departments need to be consulted about which doors should be locked and at what times, but what about the nursing staff, or administrative support or the administrators themselves? Don't forget to also get input from any 3rd parties the organization does business with. If the receiving area is locked from 5 pm to 8 am how does the baker get his 6 am delivery to the cafeteria?

As an organization begins to evolve standards to cover everything from firewall configurations to fire door installations and security awareness training to secure off site storage it must document, document, document all of these security practices and then turn those documents over to a trusted third party for review and comment.

Finally pay close attention to how HIPAA will affect the healthcare organizations business partners. The proposed regulations specify that a *"Chain of Trust Partner Agreement"*[8] must be entered into between the healthcare organization and every third party with whom they electronically exchange data. In short, if any third party doesn't meet security requirements then neither do any of the organizations they are exchanging data with.

As a HIPPA exercise for those of you who read this far and would like a sample issue to sink your teeth into, find the answer to the following question.

Q: If a hospital's purchasing department currently orders it's mops electronically (via the internet) from a local supplier who orders electronically (also via the internet) from a regional distributor who places his orders electronically (again, via the internet) with the manufacturer, how many Chain of Trust Partner Agreements need to be signed?

References:

1. Summary, Federal Register/Vol. 63, No. 155/Wednesday, August 12, 1998/Proposed Rules page 43242

2. Sec. 1171 (6) Individually Identifiable Health Information, Public Law 104-191, August 21st, 1996, URL: http://aspe.hhs.gov/admnsimp/pl104191.htm

3. C. Effective Dates – General, Federal Register/Vol. 63, No. 155/Wednesday, August 12, 1998/Proposed Rules page 43249

4. Sec. 1177. (a) Offense, Public Law 104-191, August 21st, 1996, URL: http://aspe.hhs.gov/admnsimp/pl104191.htm

5. Section 8, Administrative Requirements and Policy Development and Documentation, Federal Register/Vol. 64, No. 212/Wednesday, November 3, 1999/Proposed Rules page 59926

6. WEDi, "Security Standards" 24 November, 2000. URL: http://www.wedi.org/SNIP/Learn

7. Shanna Koss "Getting Ready for HIPAA Security Requirements" IBM. December 1999. URL: http://houns54.clearlake.ibm.com/solutions/healthcare/helpub.nsf/Files/HIPPAA/$File/HIPPAA.pdf

8. D. Security Standards, b., Federal Register/Vol. 63, No. 155/Wednesday, August 12, 1998/Proposed Rules page 43252

Resources:

http://aspe.hhs.gov/admnsimp/Index.htm The HHS website for administrative simplification and the only site most security professionals will need to follow.

http://ncvhs.hhs.gov/ The National Committee on Vital and Health Statistics Web Site

http://www.wedi.org/ Web site of the Workgroup for Electronic Data Interchange

http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm the full Notice for Proposed Rule Making for security and signature standards.

http://aspe.hhs.gov/admnsimp/lsnotify.htm this listserv should be subscribed to for email notifications of changes/addendums to HIPPA regulations.

http://www.nchica.org/activities/EarlyView/nchicahipaa_earlyview_tool.htm Web site of the North Carolina Healthcare Information and Communications Alliance, Inc. This nonprofit organization created the HIPAA EarlyView assessment tool.