HIPAA – Security and Privacy in the Healthcare Industry: A Survey of Industry Practices and Trends Relating to HIPAA

Kathrine Meus

May, 2006

Table of Contents

1. Overview

As information in today's world moves closer to being completely electronic, issues in privacy and security become more and more prevalent. Protecting personal information becomes of great concern to the individual, and in turn to the service-providing entities dealing with the sensitive personal information of the individual in daily operation, be they financial institutions, healthcare providers, or insurers. Official response to such concerns has come in the form of a number of legislative motions.

The issues of privacy and security are particularly of interest within the realm of the healthcare industry. The piece of legislation relating to this industry is the Health Insurance Portability and Accountability Act, commonly referred to as HIPAA. Title II of the HIPAA regulation, or the Administrative Simplification provisions, addresses the privacy and security of health data, among other things, which will be discussed shortly. The implications of HIPAA, which was passed in 1996, continue today, even after all the compliance deadlines have passed.

2. Background: Key Terms

In discussing HIPAA, one needs to be familiar with certain terms relating to the healthcare industry as well as terms specific to the legislation itself. One such term is *covered entity*. Covered entities can be institutions, organizations, or persons. According to the HIPAA rules, a covered entity is defined as a health plan, health care clearinghouse, or health care provider that transfers, both accepts and transmits, health information electronically in connection with a HIPAA transaction. Such transactions may include billing or payment for healthcare services or insurance.

A *health plan* is an individual or group plan that provides, or pays the cost of, medical care. Insurance companies and HMOs are included in this category. There are a number of specific organizations and government programs which are included under the official definition of a health plan, along with a couple of exclusions.

A *health care clearinghouse* is a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "valueadded" networks and switches that either process or facilitate the processing of nonstandard data elements of health information received from another entity into standard data elements. These companies may provide specific services such as claims submission or premium payment.

A *health care provider* is a hospital, doctor, or any other person or organization who furnishes, bills, or is paid for health care, and who transfers health information electronically. Researchers can be covered entities if they are also health care providers who electronically transmit health information. Physicians conducting clinical studies would be covered entities under this definition, for example.

Protected health information, or *PHI,* is at the heart of HIPAA and is the basis for many of the requirements under HIPAA. PHI is any health related information that is created, maintained, transferred or received by the covered entity that identifies an individual, or reasonably could be used to identify an individual. PHI relates to a past, present, or future physical or mental condition of an individual, or the provision or payment of health care. Examples would include information on an application for health insurance, medical records, social security numbers, policy numbers, etc.

3. Background: What is HIPAA?

3.1. Title I

HIPAA is an amendment to the Employee Retirement Income Security Act of 1974, the Internal Revenue Code of 1986, and the Public Health Service Act. The HIPAA law comes in two main parts. The 'P' in HIPAA stands for 'Portability', and it is exactly this that Title I of the Act addresses. The first part of HIPAA protects health insurance coverage for employees and their families when they change or lose their employment. Its provisions primarily affect employers and health insurers.

3.2. Title II

Title II is the more substantial section of the Act. This section is known as the Administrative Simplification provisions. These address the first 'A' in HIPAA, or 'Accountability'. The provisions in this section are only applicable to the covered entities, as described earlier. Title II is composed of four parts. Each is centered on protecting health information in some way.

3.2.1. Standard Transactions

The first of these concerns standards for electronic health transactions. These transactions include health plan eligibility, plan enrollment and disenrollment, payments for health care and health plan premiums, health claim status, first injury reports, coordination of benefits, and other related transactions. HIPAA calls for a national transactions standard which must be adopted by virtually all health plans. Providers using non-electronic transactions are not required to adopt the standards for use with commercial healthcare payers. However, electronic transactions are required by Medicare, and all Medicare providers must adopt the standards for these transactions. If a provider does not adopt the standard, it must contract with a clearinghouse to provide translation services to comply with HIPAA. In addition to standardized electronic health transactions, HIPAA calls for standardized code sets describing health problems, causes, symptoms, etc. The goal of this section of the HIPAA mandate is to improve efficiency and reduce error in healthcare delivery by standardizing electronic data interchange.

3.2.2. Unique National Identifiers

Title II also requires hospitals, doctors, nursing homes, and other healthcare providers to obtain a unique National Provider Identifier (NPI) for use in all transactions related to the rendition of and payment for health care services. Ultimately, the NPI will replace all existing identification numbers including Medicare, Medicaid and all payers' identification numbers. This would ultimately reduce error and costs, not to mention confusion among healthcare organizations.

3.2.3. The Privacy Rule

The HIPAA Privacy Rule took effect on April 14, 2004. It establishes the first "set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care" [Primer].

The Privacy Rule states the rights of the individual with regards to PHI, such as one's right to ask covered entities which maintain PHI about them to take reasonable steps to ensure that their communications with the individual are confidential, or an individual's right to file formal privacy-related complaints to the Department of Health and Human Services Office for Civil Rights. It also outlines the rights and responsibilities of the covered entity.

3.2.4. The Security Rule

The HIPAA Security Rule, described in Title II of the law, took effect April 21, 2003, and had a compliance deadline of April 21, 2005, with a one-year extension for certain eligible small plans. The Security Rule is complementary to the Privacy Rule previously described. HIPAA defines three segments of security safeguards for compliance: administrative, physical, and technical. Administrative safeguards are documented policies and procedures which are meant to show how the entity is complying with HIPAA. Key provisions under the administrative safeguards include the requirement for clear documentation of privacy practices and the designation of a privacy officer to oversee development and implementation of all required policies and procedures. This section of the Security Rule also calls for clear identification of employees or classes of employees who have access to PHI, and requires that this access be restricted only to those who necessarily need PHI to perform their duties.

Physical safeguards control physical access to protect against inappropriate access to PHI. Some key requirements under this segment include the careful monitoring and controlling of installation and removal of hardware and software from the network, the proper disposal of equipment no longer being utilized, and proper access controls to facilities. HIPAA also requires that workstations be kept out of high traffic areas, and monitors should be out of direct view of the public so as to reduce the chance of passersby viewing PHI inappropriately.

Technical safeguards refer to controlling access to computer systems and protecting communications containing PHI transmitted over open networks. It requires the use of some type of encryption in open systems, with encryption being optional if a closed system is used. HIPAA mandates that all technical compliance initiatives be documented and made available to the government. Responses to the compliance requirements are not standard, since it would be impossible to devise a standard solution that would fit each of the diverse healthcare organizations. However, covered entities are required to make all reasonable efforts to protect PHI and to keep the security of their systems as tight as possible.

4. Secure Messaging & IT

Email is used extensively in the healthcare industry, and the messages being sent through this channel often contain PHI. As such, HIPAA mandates that such email be encrypted and secured to protect this sensitive information. Since

The key to an effective secure messaging solution is complete automation. It should not rely on the user to make correct decisions because the end user often forgets, or simply does not know, that an email should be encrypted. A good example of an automated HIPAA-compliant decision making protocol is that of Zix's Virtual Private Messenger (VPM), a secure email solution. It initiates encryption at two points in the emailing process [McNamara05]. When an end user wishes to send a secure email, he can type the trigger word 'secure' in the subject line before sending the email. Additionally, VPM scans the email's text and attachments for certain combinations of words and numbers which may be indications of PHI. If the software finds such combinations, it automatically encrypts the email, regardless of whether or not the end user indicated that it should be secure. When a recipient receives an encrypted email, they receive a link to a website where they are authenticated and setup a password, allowing them to retrieve the encrypted message.

PostX, the secure messaging solution endorsed by the American Hospital Association, also employs an automated policy manager which examines emails, and takes appropriate action according to the established policies. If the examination reveals PHI in the email, the solution encrypts the message. It then communicates with the recipient's email server and delivers the message according to the correct protocol. PostX has audit capabilities as well. It produces reports suitable for compliance audit, as required by the HIPAA law [PostX]. The solution can also report on exactly when the message was opened by the recipient. These features are very important in tracking HIPAA compliance and ensuring that the PHI is handled with the utmost care.

5. PHI at Risk

Even after all the efforts made to ensure the protection of PHI, breaches of privacy continue to be prevalent. News reports all over the country tell of stolen employee laptops containing patients' medical information, hacking attempts on healthcare organization computer systems, and increasingly, medical identity theft.

Early this year, Providence Health Systems, a health care provider in the Northwest, reported that some 365,000 medical records had been stolen from them. A Providence employee had brought home a number of disks and tapes in order to make backups. He left the media unattended in his car, and a thief walked away with it all. The records held names, addresses, dates of birth, health conditions and drug prescriptions. 250,000 of the records included Social Security numbers. The negligence of one man led to loss of his job, as well as the jobs of three of his colleagues, a class-action lawsuit against Providence, and a huge blow to Providence's reputation. Only a couple months later, thieves in two separate car break-ins walked away with laptops containing 122 Providence Health System patient records. The laptops had been left in the cars unattended by the people who were authorized to have access to the PHI contained on the computers.

In June 2004, a hacker broke into the computer system at University of Washington Medicine. The intrusion was not discovered until December 2005, 18 months later. For 18 months, more than two million patient records were vulnerable, but reportedly none of them were accessed. The breach occurred because of human forgetfulness – someone had forgotten to install the necessary security patches on the system, leaving a wide open hole to be exploited.

World Privacy Forum, a nonprofit research group, reports that there are more than 19,000 complaints of medical identity theft on file with the federal government [Harris06]. Medical ID theft occurs when a criminal uses his victim's personal identifying information to receive medical services under his victim's name. Not only does this cause financial damage for the victim, but it can cause a caregiver to provide a patient with incorrect medical care. If an individual is a victim of medical ID theft, his medical chart may not match his own body. It may contain incorrect information such as the wrong blood type or a false medical history, possibly leading to dangerous, incorrect diagnoses and care.

6. Training

As shown in the examples above, it is often human error that makes PHI vulnerable to theft and malicious use. The solution to this, as is always the case, is education and training. The HIPAA law mandates that covered entities show that they are providing an ongoing training program regarding the handling of PHI to employee performing health plan administrative functions. They must also train any contractors or agents who might perform such functions.

Employee HIPAA training should aim to make the employee understand the importance of keeping PHI protected. Policies and procedures regarding PHI should be clear and firmly enforced. Many of the common human errors leading to security breaches are easily avoided. Simple things such as avoiding password sharing, locking one's computer when leaving it unattended, and avoiding bringing home sensitive information can all help prevent theft of PHI.

7. Are We Done With HIPAA?

The deadlines for HIPAA compliance have passed, but can the healthcare industry breath their sigh of relief just yet? A number of legislative movements and industry initiatives would have us responding ‘not quite’.

One issue which is closely tied to the HIPAA Privacy and Security Rules is the development of Personal Health Records (PHRs). This is defined as any “internet-accessible application that enables a patient (or care provider for a patient, e.g., the 'mom') to create, review, annotate, or maintain a record of any aspect(s) of their health condition, medications, medical problems, allergies, vaccination history, visit history, or communications with their healthcare providers” [Upham06]. This presents an interesting shift in healthcare record-keeping, allowing the patient to become more involved in his own care. At the same time, it opens the door for potential risks relating to the confidentiality of the information kept in the PHR.

Representatives Tim Murphy and Patrick Kennedy are pushing for a new law which would encourage and support the use of health care information technology. They would like to “authorize up to 20 grants to [regional health information organizations] over a three-year period to develop and implement a plan that would, among other things, allow electronic sharing of health information among providers, give consumers access to their own health information and allow them to control who can access their information, ensure interoperability and provide privacy protections” [Fried06]. A companion bill was introduced in the Senate by Senators Mel Martinez and Hillary Rodham Clinton.

Legislation such as these bills shows that the issues that were important when HIPAA was passed are just as, perhaps even more, important now. HIPAA was just the first step on the way to completely electronic health records and completely integrated healthcare information technology. The healthcare industry is on a trend toward interoperability, and privacy and security concerns will develop as new innovations come about.

8. Annotated References

[Fried05] Bruce Merlin Fried, Esq. **Let the Legislating Begin**. iHealth Beat. May 2005. http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemid=111506.

The author describes the Murphy/Kennedy bill which calls for the support of health care information technology.

[Gue03] D'Arcy Guerin Gue. **Training – The First and Last Word in Privacy Compliance**. HIPAA Advisory. October 2003. http://www.hipaadvisory.com/action/awareness/privacytraining.htm

The author discusses the importance of a formal, ongoing, enterprise-wide training program on privacy policies and procedures.

[Harris06] Dan Harris. **Medical ID Theft Can Wreck Victims' Health and Finances**. Good Morning America. ABC News. May 2006. http://www.abcnews.go.com/GMA/Health/story?id=1917165&page=1.

ABC News reports on medical identity theft. Criminals use their victim's social security number, date of birth, or insurance information to receive medical services. Not only does this lead to financial difficulty, it can also cause bad medical treatment for the victim, whose medical record now has the wrong information on it.

[HIMSS] **U.S. Healthcare Industry HIPAA Compliance Survey Results: Winter 2006**. HIMSS/Phoenix Health Systems. Winter 2006. http://www.himss.org/Content/files/Winter_Survey_2006.pdf

The Healthcare Information and Management Systems Society, together with Phoenix Health Systems, conduct a semi-annual survey of the healthcare industry regarding HIPAA compliance. The Winter 2006 report features a new section focusing on the impact HIPAA has had on the respondents' organizations, as well as the industry's move to implement return on investment initiatives relating to HIPAA.

[McNamara05] Paul McNamara. **You've Got Mail**. Network World. August 2005. http://www.networkworld.com/techinsider/2005/081505techinsider-mail.html.

This article discusses the need for secure messaging solutions and focuses on one such solution, Zix's VPM.

[PostX] Brian Lane, Shawn Eldridge, Gregg Timmons, Michael Krieger. **HIPAA Simplified: The American Hospital Association Endorses Secure Messaging**. Borderware/PostX. April 2006. http://www.eseminarslive.com/article2/0,2144,1943155,00.asp

In this webcast, PostX and Borderware representatives discuss their integrated solution that allows email administrators to offer secure email delivery as part of a complete email security and HIPAA compliance solution for the healthcare industry. A representative of the American Hospital Association discusses how the AHA came to choose PostX/Borderware as its secure messaging vendor.

[Primer] HIPAA Advisory. **HIPAA Primer**. Phoenix Health Systems. Updated July 2005. http://www.hipaadvisory.com/regs/HIPAAprimer.htm.

A brief overview of the HIPAA regulation, outlining important points such as who is affected, fines, deadlines, and rules under HIPAA.

[Richman06] Dan Richman. **Hacker at UW Medicine revealed**. Seattle Post-Intelligencer. February 2006. http://seattlepi.nwsource.com/local/259725_computer16.html.

A hacker gained access to University of Washington Medicine's computer system in June 2004, and remained undetected for 18 months. The hacker reportedly did not access patient records.

[Rojas0206] Joe Rojas-Burke. **4 depart Providence after theft of records**. The Oregonian. February 2006. http://www.oregonlive.com/news/oregonian/index.ssf?/base/news/1140839716241210.xml&coll=7.

Four employees were forced out of Providence Health System after they are deemed responsible for a security lapse that allowed a thief to walk away with computer disks and tapes containing medical records on about 365,000 patients.

[Rojas0306] Joe Rojas-Burke. **Providence hit again in thefts of patient info**. The Oregonian. March 2006. http://www.oregonlive.com/business/oregonian/index.ssf?/base/business/1141716784147250.xml&coll=7.

This news article describes two incidents of PHI theft relating to the Providence Health System in Washington State wherein thieves stole laptops out of cars. The laptops contained PHI on 122 hospice and home-care patients.

[SC05] Paul Kurtz, Owen Hathaway, Stuart Ranch. **Best Practices for Securing Electronic Private Health Information**. Secure Computing. September 2005. http://whitepapers.businessweek.com/detail/RES/1131716764_402.html&src=TRM_TOPN

This webcast, presented by the Secure Computing Corporation, features Paul Kurtz, of the Cyber Security Industry Alliance, Owen Hathaway, Technical Services Manager of the Longmont United Hospital, and Stuart Rauch, of the Secure Computing Corporation. They discuss health information technology (HIT) systems and how to achieve secure HIT systems. Hathaway presents a case study focused on his team at the Longmont United Hospital.

[Upham06] Randa Upham. **HIPAA Is Not Done: How HIPAA & New Healthcare Initiatives Intersect**. HIPAA Advisory. Updated March 2006. http://www.hipaadvisory.com/action/notdone.htm

The author considers the ongoing implications of the HIPAA regulation, even after the final deadline for compliance has passed. Upham looks at possible new areas of compliance which may appear in the next few years.

[WIKI] http://en.wikipedia.org/wiki/HIPAA
This Wikipedia article gives a description of the HIPAA legislation, with emphasis on the Administrative Simplification Provisions relating to privacy, security, and HIPAA/EDI.