A Guide for using the HIPPA Security

Compiled by

Houphouet Wooten

A Research Paper on HIPPA

Columbia College of Missouri
Jacksonville, Florida

Abstract

HIPPA compliance has definite identifiable traits. These traits are that patient’s medical records have to be guarded, if you change jobs and medical providers you can be covered for
pre-existing conditions and if there is a leak in information because of poor security methods within your organization there is a penalty to pay. The penalty consists of possible jail time and monetary fines. Other traits are not as well defined for HIPPA and such as health care employee’s personal security habits that could inadvertently disclose patient’s medical information.
Introduction

This is the history of HIPPA starting with it becoming law on August 21, 1996. The bill that became HIPPA (HR 3103) was initially introduced to solve a social problem commonly referred to as “job lock.” Group health insurers were imposing exclusions from coverage for up to one year for preexisting medical conditions when employees and others changed jobs or otherwise obtained new coverage. In the course of the legislative process, the bill became a magnet for a variety of issues. For instance, an entire chapter was added to strengthen the laws regulating fraud and abuse in health care and certain other insurance matters. (Wu, 2007)

Many of the parties that pay for health care (insurers and health plans) went to Congress to seek “administrative simplification” of health care business transactions. Specifically, through the standardization of health care information and processing. They proposed legislation to establish mandatory and Internet-friendly uniform rules and formats for electronic transmissions among health care providers, health plans, and health care clearinghouses that were perceived to be most important. The proposals also sought to standardize their forms and transaction formats remained in use in the United States. Backers claimed that this standardization process could save many tens of billions of dollars. (Wu, 2007) The legislation was the administrative simplification provision. The goal was to improve the efficiency and effectiveness of the health care system, by encouraging the development of a health care system through the establishment of standards and requirements for the electronic transmission of certain health information. (Wu, 2007)
Privacy advocates sought enhanced privacy and security protections for this soon-to-be readily accessible, but highly confidential, health information. (Wu, 2007)
Method

This research effort is the results of internet searches and books. I researched the HIPPA rules by searching the internet and reading printed material. Articles were read to gain the most recent knowledge relating to the subject. Several articles were read to culminate the paper.
Discussion

HIPAA is an acronym or the Health Insurance Portability and Accountability Act. This Act was introduced in 1996, but not fully implemented until 2003. HIPAA was created to insure that people between jobs would still have access to quality health care coverage, since in the past it was difficult or impossible to change insurance carriers without facing lowered coverage or exorbitant premiums. HIPAA was also intended to protect private health care information and create a uniform standard for dispersing personal information (Holetzky, 2003-2010). The privacy of your healthcare information is very important because unwanted disclosure could lead to possible discrimination.

The Rehabilitation Act of 1973, as amended, protects qualified employees and applicants with disabilities in the Executive Branch of the Federal government from employment discrimination based on disability. In 1992, the substantive employment standards of the Americans with Disabilities Act, 42 U.S.C. Section 12111, et seq., were made applicable to the Federal Government through the Rehabilitation Act. The amended law requires Federal employers to provide reasonable accommodations to qualified individuals with disabilities so that employees with disabilities can enjoy the benefits and privileges of employment equal to those enjoyed by similarly situated employees without disabilities. It requires Federal agencies to provide reasonable accommodation for known physical or mental limitations of qualified
employees and applicants, unless to do so would cause undue hardship. The law also ensures equal access to Federal programs, activities, and facilities to people with disabilities.

(\text{http://www.nrcs.usda.gov/about/civilrights/Discrimination_Types-Basis.html})

What does portability mean? Before HIPAA, if a person lost his job and therefore his insurance coverage, the next insurance company he used could classify his health needs as "pre-existing conditions." Doing so allowed the insurance provider to pay little or nothing for services needed to remedy such conditions, despite the fact that the client was paying for the insurance. For example, if a person was regularly taking prescription medicine for high blood pressure, the new insurance provider could refuse to pay for his medication under the pre-existing policy, but the premium would remain the same, often for at least one year (Holetzky, 2003-2010). Now with portability you will be covered for pre-existing conditions by a predecessor insurance company.

What does accountability mean? In regard to HIPAA, accountability refers to the standards by which private health care information is exchanged between insurance companies, health care providers, pharmacies, employers and patients. In the age of technology, electronic transfer of information makes it very easy to violate a patient's privacy, even inadvertently. (Holetzky, 2003-2010)

When the Health Insurance Portability and Accountability Act (HIPAA) passed in 1996, it called for the creation of national standards and requirements for the electronic transmission of health information. The purpose of the "administrative simplification" provisions of the law was
to standardize claims processes and procedures, for example, by requiring insurers to use and accept the same form. In seeking to streamline the Byzantine world of health claims and other health-care reimbursement information, the goal was to simplify administrative matters for providers and patients. (http://nces.ed.gov/pubs98/safetech/chapter3.asp#afwo) All forms for claims will use the same codes.

The HIPAA system was born of a request in the early 1990s from the major players in health care who went to HHS (Health and Human Services) and to Congress seeking to bring to health care some of the electronic efficiencies that have been so successful in the banking industry. The belief was, and remains, that electronic transaction will lower health-care system costs. For example, armed with automatic teller machines and a host of other technologies, banks can instantaneously process thousands of transactions across the country because they have long had uniform standards for electronic transmissions. Compare that to health care, where submitting, receiving, approving and paying claims are an industry within an industry and can take weeks or months to be settled—an administrative jumble that eats up as much as a quarter of the health-care dollar. (http://nces.ed.gov/pubs98/safetech/chapter3.asp#afwo). There will be a savings realized that will be beneficial to the health care provider.

HHS has been working since the law was passed in 1996 to set up the standards, but has been delayed by the complexity of both the system and of getting it through the regulatory approval process. (FOXHALL, 2001)

The rules for health-care privacy mandated under HIPAA were essential to implementing
electronic transmission, but they could also present a sea of change for health-care and psychology practitioners. (FOXHALL, 2001)

Delayed briefly by the Bush administration, the privacy rules are now moving forward in the form finalized by the Clinton administration last December, although HHS Secretary Tommy Thompson has said the department will offer guidelines and possible modifications. (FOXHALL, 2001)

Compliance was be required by April 14, 2003. The rules mandate that providers get patients' consent to share records for even routine purposes such as treatment, payment or health-care operations. Beyond that patients must give separate authorization for release of psychotherapy notes--what practicing psychologists typically refer to as "process notes"--to parties beyond the treating provider, thereby affording heightened protection for these notes. (FOXHALL, 2001)

When records are disclosed for nontreatment purposes, the law requires that only the minimum information necessary be disclosed. The law also gives patients the right to see and get copies of their records, and to get a history of any nonroutine disclosures of their records. (FOXHALL, 2001)

The administrative requirements of the privacy rule are "scalable." A popular buzzword that refers to how well a Hardware or software system can adapt to increased demands. For example, a scalable network system would be one that can start with just a few nodes but can
easily expand to thousands of nodes. According to Doug Walter, JD, legislative counsel on the Practice Directorate's government relations staff, this means that a covered entity "reasonably" meets the requirements according to its size and type of activities related to records transactions. For example, an entity covered by this rule must train all members of its workforce on the policies and procedures to protect individually identifiable patient information. The HHS has recognized that training must be flexible, leaving it to the covered entity to decide the nature and method of training to achieve this requirement. (FOXHALL, 2001)

As another example, a covered entity is required to designate a privacy officer responsible for developing policies and procedures. A reasonable analysis of the scalability principle would suggest that a psychologist may identify herself or himself as the privacy official in solo practice, whereas in a large insurance company, the privacy official may constitute a full-time staff position. (FOXHALL, 2001)

The security rules are another change under HIPAA's administrative simplification that will affect psychologists. HHS regulations to implement those requirements, aimed at guarding against improper access to electronically stored information, were proposed in the Federal Register, Aug. 12, 1998. People close to the HIPAA process expect that the final standards will be published in the next few months. (FOXHALL, 2001)

The proposed rules require any health-care provider who transmits records in electronic form to have:

- Documented administrative procedures to guard data integrity, confidentiality and availability.
Physical safeguards for protecting data, including protection from fire and other hazards and intrusions. This covers use of locks, keys and administrative control over access to computer systems and facilities.

Technical security processes to restrict access to data to employees with a business need for it. This includes aspects such as passwords, personal identification and automatic logoff.

Technical security mechanisms to guard data transmitted over a communications network so that it cannot easily be intercepted or accessed.

Employees must be told in writing:

- What is and is not acceptable use of equipment.
- What the penalties for violating regulations will be.
- That their activities may be monitored.
- That security will be a part of performance reviews (users who do their share should be rewarded, whereas those who lag behind might be reprimanded or retrained).

Employees must be told in writing:

- What is and is not acceptable use of equipment.
- What the penalties for violating regulations will be.
- That their activities may be monitored.
That security will be a part of performance reviews (users who do their share
should be rewarded, whereas those who lag behind might be reprimanded or
retrained).

Employees should be reminded that:

- Organizational resources, including computers, belong to the organization
- There should be no expectation of privacy for information stored on or
  transmitted with the organization's equipment.

Employees should be required to sign a Security Agreement to acknowledge that they are
aware of their responsibilities and verify that they will comply with security policy. This
requires that:

- Staff should have ample opportunity to read and review all policies and
  regulations for which they will be held accountable.
- Staff should be provided an appropriate forum for clarifying questions or
  concerns they may have about the organization's expectations.
- Staff should not be given access to the system until a signed agreement is
  accounted for and maintained in a safe place.

All new employees should be expected to meet the organization's security requirements
and procedures as a part of their job description. Once hired, new employees should be
informed of, and trained on, security policy as a part of their initial orientation in order to
impress the importance of security upon them.
Outside organizations should be expected to guarantee (via binding agreements) that they and their employees will use and secure shared information appropriately.

A Special Note on Outsiders

Outsiders (e.g., repair technicians, consultants, and temporary help) and outside organizations (e.g., other departments, other educational institutions, and contractors) with access to your system should also sign agreements that require them to respect and maintain the confidentiality of your information. But be careful not to share more about your security operation with outsiders than is necessary. Even apparently harmless warnings about what to expect of your defenses can give a skilled intruder an edge in tampering with your system. Instead, limit security briefings to those levels required to (1) keep them from breaching your defenses, (2) impress upon them that you are serious about protecting your system assets, and (3) ensure that they handle your assets in a secure manner.

Having said this, sharing general news with the public--parents, local organizations, business partners, and lawmakers to name few--about your organization's commitment to securing confidential information can instill a feeling of confidence throughout your organization and community. (http://nces.ed.gov/Pubs98/Safetech/chapter3.asp#war-) 2008-2009

It's important to note that the security
It is important to note the standards, like the privacy standards, also will be "scalable."

Scalability a popular buzzword that refers to how well a hardware or software system can adapt to increased demands. For example, a scalable network system would be one that can start with just a few nodes but can easily expand to thousands of nodes. Scalability can be a very important feature because it means that you can invest in a system with confidence you won't outgrow it. This is what will be required to create the same level of security will be easier for small practices than for large organizations. For purposes of its discussion, HHS describes "a small or rural provider" as one-to-four physicians [apparently the same for psychologists] with two-to-five additional employees. HHS states, "For example, in a small physician practice, a contingency plan for system emergencies might be only a few pages long and cover issues such as where backup disks should be stored, and the location of the backup personal computer." (FOXHALL, 2001)

While policies themselves don't solve problems, and in fact can actually complicate things unless they are clearly written and observed, policy does define the ideal toward which all organizational efforts should point. By definition, security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. Good policy protects not only information and systems, but also individual employees and the organization as a whole. It also serves as a prominent statement to the outside world about the organization's commitment to security.

HIPAA defines protected health information (PHI) [2] as "any information, whether oral or recorded in any form or medium" that
"[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and

"[r]elates 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."

In short PHI is information that is identifiable to a certain person that includes health information. PHI data is the target of protection, as covered by the security rule. The security rule for PHI only applies if the PHI data is electronically transmitted or received by a covered entity. If the data is covered by HIPAA security rule then the law requires the customer (covered entity) to: "Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified". Thus the covered entity is mandated to protect the PHI while allowing only authorized access, as needed.

Covered entities have been advised by the HIPAA regulators to work with their software vendors in producing software that will help their security rule compliance efforts. Therefore, when performing the requirements analysis phase of systems design, you may be prompted by customers, who are covered entities, to provide an explanation of how your system design features map to various HIPAA security rule standards. In other cases, software applications will have to be redesigned or modified to fit specific security compliancy objectives of individual covered entities. In many cases, HIPAA security rule technical standards compliance will be gained by small adjustments to existing security posture of the covered entity. In such cases, the ability to integrate into existing security architectures will be a key to effecting compliance.
If you are developing PHI related software applications one person on the client side who will probably have input into the design requirements is the Information Security Officer (ISO). Covered entities are mandated by HIPAA to designate someone as the ISO, the person responsible for implementing HIPAA security rules. The ISO can be someone with a security background or can literally be anyone designated as such, regardless of experience. ISO responsibilities include setting up user accounts, controlling authorization and access controls, and emergency access contingency plans. These will be major discussion points in developing requirements for software systems that must be comply with the HIPAA security rule.

(Pasley, 2004 when)

The U.S. Department of Health and Human Services (HHS) published rules that require updated versions of the standards for electronic transactions under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These updated standards (Versions 5010 and D.0) will replace the current standards (Versions 4010/4010A1 and 5.1) and are designed to promote greater efficiency in electronic transactions. Compliance with the new HIPAA 5010 and NCPDP D.0 standards is required by January 12, 2012. The ICD-10 code sets are required in transactions as of October 1, 2013. http://www.news-medical.net/news/20100123/Emdeon-introduces-HIPAA-Simplified-to-help-guide-healthcare-industrys-transition-to-new-standards.aspx

The HIPAA Privacy Rule for the first time creates national standards to protect individuals’ medical records and other personal health information.
It gives patients more control over their health information.

It sets boundaries on the use and release of health records.

It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.

It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients’ privacy rights.

And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.

It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.

It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.

It empowers individuals to control certain uses and disclosures of their health information.

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality
provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. (John 2009)

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. (John 2009)

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. (John 2009)

Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20,
The Health Information Technology for Economic and Clinical Health Act’s (HITECH) major goal is to increase EHR adoption. The major questions are “Is it enough?” and “Will it work?” Let’s take a look at each of these questions.

The incentive funding that will available to health care providers.

**Background:**

The Health Information Technology for Economic and Clinical Health Act (HITECH) provides $18 million in incentives through Medicare and Medicaid reimbursements. Starting in 2011, physicians who show that they are “meaningfully” using health IT would be eligible for $40,000 to $65,000, and hospitals would be eligible for several million dollars. The incentives would be phased out over time, with penalties in place by 2016.

**Answer:**

$40,000 seems like a large chunk of money for EHR. Of course, we have to remember that it’s spread out over 5 years, but $40k isn’t insignificant. Sure, many EHR out there cost $200k plus to implement. However, not all of them are this expensive. In fact, I’d say that the EHR market has shifted from mostly high priced EHR to more moderately priced EHR with unique pricing structures.

The possible problem with the HITECH legislation is that we still don’t know how HHS will interpret what a certified EHR will be. If they say it’s a CCHIT (The Certification Commission for Health Information Technology [CCHIT] is a private not-for-profit organization that serves as a recognized US certification authority for electronic health records (EHR) and their networks) certified EHR, then $40k might not be enough reimbursement. If they create a better standard
for certification which will include specialty EHR and smaller but effective EHR software, then $40k is probably enough for many doctors to turn the corner and implement an EHR.

Obama has held very strong on his commitment of $10 billion a year for 5 years in health care. Obama’s set the audacious goal of full digital health records by 2014. The question is if it’s even possible to invest that much money in health care IT in such a short period and will we be able to reach the goal of full EHR by 2014.

A recent CNN Money article pointed out some important problems with investing so much in health care IT. The biggest of these is finding enough qualified IT professionals that can navigate the complex health care IT systems. There really is a lack of qualified health care IT professionals. Some jobs I’ve seen listed for EMR professionals have gone unfulfilled for months just because they couldn’t find qualified candidates.

Many reports are also suggesting hundreds of thousands of jobs will be created by this investment in health care IT. This of course would be true if you had enough people to fill those jobs. It’s hard enough for an IT professional to move into health care IT. It will take a lot more training for a blue collar worker to try and implement an electronic medical record.

Certainly it’s not impossible for someone to learn from scratch. I know, because I did it myself. However, it is literally like learning to talk a different language. It takes a lot of work and training and a unique person who can balance the IT needs, the health care requirements, with the business requirements.

I also think that it’s sad to say that $50 billion might be enough to achieve the goal of interoperable EHR by 2014. A look at a small Massachusetts Example gives a good measure of what it will actually cost:
Massachusetts has developed a plan to fully computerize records at its 14,000 physicians’ offices by 2012 and its 63 hospitals by 2014. After a pilot program, the state legislature estimates it will cost about $340 million to build the statewide computer system, with a cost of about $2 million per hospital.

“[Obama's] timeframe is very ambitious, but there is a need to be able to track data on patients and talk across providers and health care systems,” said Dr. JudyAnn Bigby, Secretary of Health and Human Services for Massachusetts. “The program will allow for greater patient safety.”

Despite being less than what might be needed, it certainly would give it a good start that could build into the future.

I’m still planning on writing a few words about whether I think the investment is worthwhile or not. However, I think it’s important to have as much of an understanding as possible at the goals Obama has proposed for investment in IT for health care. (John 2009)

Disclosure of Personal Information

We may use or disclose protected health information to the Food and Drug Administration (“FDA”) in connection with the reporting of adverse events, product defects or problems, product tracking or for other purposes as required by the FDA. We may use or disclose protected health information during the course of clinical research activities. We may also disclose personal information as required by law. Individual Rights to Access and Correct Personal Information We have procedures in place for individuals to have access to protected health information, and procedures in place to ensure the integrity of our information and for the timely correction of incorrect information. (2007 Galil Medical.)
A date of April 14, 2003 was set for compliance. Small health plans, those with annual receipts of $5 million or less, had until April 14, 2004, according to the DMA.

The information protected includes name, specific dates—such as birth date, admission or discharge dates and the date of death—social security number, medical record number, photographs, city, Zip code and other geographic identifiers.

According to the rule, written permission must be obtained from individuals—by way of a signed authorization form—before health-related information is shared or used for marketing or fundraising. Covered entities must receive a written agreement from each of its business associates acting on its behalf prior to disclosing any protected health information.

In addition, patients have to right to receive a privacy notice, request that the use of their information be protected, inspect their medical records, receive an accounting of the disclosure of their protected information and file a complaint.

The fines for violating the rules are stiff. Violators can be sentenced for up to 10 years in prison and fined up to $250,000 in criminal penalties. Civil penalties can be imposed that include $100 per violation and up to $25,000 per person, per year for each violation.

The DMA is conducting a seminar on the revisions to HIPPA this spring as part of its Corporate Responsibility Series, which began last year. No date has been set. (Patricia Odell 2003) This collection of guidebooks represents a unique collaboration between the American Health Lawyers Association and the Office of Inspector General Department of Health and Human Services (OIG). Each resource provides unique insight into the OIG’s priorities and gives practical tools for healthcare organization boards to carry out their fiduciary responsibilities. The three guidebooks in this collection are valuable reading for healthcare boards of directors that
want to understand their role in overseeing the quality of care provided by their organizations.

The Corporate Responsibility series is also featured on the Governance Institute website's home page. (American Health Lawyers Association 2010)
Results

HIPPA will be used by health care providers to protect patient’s information. HIPPA will be used for the simplification of filing claims and allowing the insured the ability to be insured for pre-existing conditions through portability.

Privacy will result in less discriminatory acts by employers or anyone that does not have the need to know about a person’s medical condition.

Preexisting conditions will be covered by the next insurer. This will be a helpful aspect for aging or previously diagnosed individuals.

Making patient records electronic will save the providers money. This is mainly accomplished by the coding of medical conditions. The codes of medical conditions for electronic filing and for insurance claims will be uniformed throughout the industry.

What is HIPPA it stands for Health Insurance Portability and Accountability Act. Insurance Portability means you will be covered for pre-existing conditions by a predecessor insurance company. Accountability means accountability refers to the standards by which private health care information is exchanged between insurance companies, health care providers, pharmacies, employers and patients.
References


Keith Paisley. Date unknown. [Online] Available:


Author Unknown [Online] Available:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

Written by: John [Online] Available:

http://www.nrcs.usda.gov/about/civilrights/Discrimination_Types-Basis.html

Written by: John [Online] Available


(Patricia Odell) [Online] Available:
http://directmag.com/news/marketing_new_hippa_revisions/
