Healthcare Applications and HIPPA

BA 458 Final Project

Ross Pierson

Table of Contents

1. Intro

The healthcare industry faces many policies and regulations and is also one of the fastest growing areas for technology. These two characteristics may not seem to be related but they are because these regulations have had a great impact on IT in the healthcare industry. The health care industry has had to adopt new IT systems very quickly to meet the many challenges that they are facing. They must try to reduce their cost, improve patient care, and meet these strict regulations.

The Health Insurance Portability and Accountability Act of 1996 is one of the regulations that must be complied with. It was originally put in place to help to keep patients data private, make it easier for Americans to keep health insurance when they changed jobs, and standardize healthcare-related information systems.

Although HIPAA has increased the use of IT and expanded the possibilities for these healthcare companies, it has also created many challenges. Healthcare providers are now using electronic records instead of paper records. These health care companies must make sure that these records are easily accessible to authorized medical personnel but not to unauthorized people. They also must make sure that the information is secure when being transferred between different organizations. It is important to recognize how HIPAA has affected the different business processes and IT systems and analyze how health care companies can continue to drive change while still complying with HIPAA.

2. Key Terms:

PHI or protected health information refers to any patient information in any form that is: 1.) Created or received by a covered entity 2.) Relates to a patient's health condition in the past, present, or future 3.) Identifies the patient. It can include information transmitted or maintained in any form, such as prescription records, billing records, patient profiles, and oral communications. ("HIPAA Made Simple")

A covered entity is "every person, business, or agency that provides bills or receives payment for medical care and transmits protected health information already in electronic storage media." (Lawrence)

A healthcare clearinghouse is a "public or private entity that does either of the following functions: 1. processes health information received from another entity in a nonstandard format or containing nonstandard data into a standard format. 2. Receives a standard transaction from another entity and processes health information into nonstandard format." (Standards for Privacy)

A Health care provider is "a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." (Standards for Privacy)

EDI or electronic data interchange refers to the "electronic transfer of information in a standard format between trading partners. It takes substantially less time than paper in sending, processing, and storing these documents. It is also important to help streamline processing tasks which can in turn result in less administrative burden, lower operating costs, and improved overall data quality." (Health Insurance Reform)

Privacy is defined as “seclusion from public view through unwarranted government intrusion into personal lives or the open disclosure of facts that are highly offensive to a reasonable person and not of legitimate concern to the public. They even specifically include medical data to these technical safeguards for citizens’ privacy.” (Lawrence)

Confidentiality on the other hand is “the property that data or information is not made available or disclosed to unauthorized persons or processes.” It applies to interactions among people as well as computers. Even if the data is private, it may be used in many computer systems, but is still confidential because the person can’t be identified. (Lawrence)

Disclosure is the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

3. What is HIPAA?

HIPAA is the Health Insurance Portability and Accounting Act passed by congress in 1996. The intent was to reduce or eliminate the denial of benefits for when people changed jobs. They also wanted to facilitate EDI, reduce fraud, and reduce costs. HIPAA can be broken down into two titles.

Title I protects health insurance coverage for workers and their families when they change or lose their jobs. It placed restrictions that health plans can place on benefits for preexisting conditions.

Title II requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

It was put in place to help control fraud and abuse within the health care system. It is broken down into the privacy rule, security rule, transaction standards, and unique identifiers. (“Health Insurance Portability and Accountability Act”)

Privacy Rule

The privacy rule took effect in 2003 and established regulations for the use and disclosure of PHI. Covered entities were required to disclose PHI to the individual within 30 days upon request. The privacy rule also allows individuals the right to correct any inaccurate PHI. Covered entities must disclose PHI when required to do so by law as well. A covered entity may disclose PHI to facilitate treatment, payment, or health care operations.

The rule is retroactive and it applies to all existing records held by a covered entity, no matter how old it is. The privacy rule covers the records of the dead as well as the living and gives no time limits for how long records of the deceased must be protected. Health care system, however, would not be able to operate without access to health care data so the privacy rule provides many different ways for disclosing this information. This allows these different systems to be created and have access to PHI. (Lawrence)

Transactions Rules

This rule was supposed to take effect on October 16, 2003 however many companies didn’t understand how to implement this in time. It was not until July 1, 2005 that companies were finally expected to become compliant. The transaction rule covers several key EDI transactions. (“Health Insurance Portability and Accountability Act”)

Although many companies were already developing standardized EDI's, there still wasn't an industry standard before the rule was put in place. This will help these companies communicate with each other, reduce errors, and improve overall efficiency in their information systems.

Security Rule

The security rule took effect on April 21, 2003 and companies had until April 21, 2005 to become compliant. The security rule deals specifically with PHI in electronic format and it sets three different safeguards that must be met for compliance; administrative, physical, and technical.

The Administrative safeguards were put in place to show how the company is complying with HIPAA. Covered entities are required to adopt a set of written policies and designate a privacy officer in charge of these policies. The company must also show that they are continuing to become compliant through training of their employees. It also recommends that companies should put a contingency plan in place in case of emergencies. As we learned in class, this type of plan can be very useful and may save the company a lot of time and money if it is ever needed. Leaking of medical records could lead to the loss of money as well as reputation for these healthcare companies. ("Health Insurance Portability and Accountability Act")

Physical safeguards were put in place to help control physical access to machines and protected data. Companies must put controls in place so that hardware and software can't be removed from the network. Employees now have increased access to flash drives and other mobile devices such as laptops which makes it very easy for them to make the

data portable and take it with them. Companies must also monitor access to equipment and software that has access to protected information. A maintenance record and visitors log are also required to track everyone that has access to these areas.

Technical safeguards were put in place by controlling access to computers systems and not allowing anyone to intercept this private data on these networks. The companies are required to use some type of encryption in case the data is intercepted or stolen. Software is also used to make sure the integrity of the data remains very high. Medical records will not do anyone any good if they are incorrect or missing information.

Unique Identifiers Rule

All covered entities using electronic communications are required to use a single new NPI. It is a 10 digit number without any outside meaning used to identify covered healthcare providers in standard transactions.

4. Impacts of HIPAA

HIPAA was intended to create standard ethical practices into standardized rules of conduct and record management for the twenty-first-century health services. Very few people will argue that privacy isn't important when it comes to medical records, however, HIPAA has also had many unforeseen and unintended consequences as well. (Lawrence)

First of all, the law is very long and hard to interpret. "Confusion persists, however, and likely will for some time, over how HIPAA applies to records containing PHI in various public and private repositories. Historians need to be ready to deal with

HIPAA concerns so that records that could be accessible are not unnecessarily restricted or closed."

" Because the regulations about research access to decedent's information are confusing, to say the last, those responsible for approving historians' use of their records may well ask researchers to sign a confidentiality document modeled on the "data use agreement" that the Privacy Rules describes for release of "limited data sets" with information on living people. For sensitive collections and for materials that are highly likely to include details on living patients, historians will almost certainly need to apply for access and use through and Institutional Review Board (IRB) or a Privacy Board." (Lawrence)

Effects on research

The enactment of the Privacy and Security Rules has caused major changes in the way physicians and medical centers operate. Patient privacy was always a major concern, however, HIPAA has now complicated the process. The new rules and regulations have increased paperwork and the cost of implementing these security measures.

"HIPAA restrictions on researchers have affected their ability to perform retrospective, chart-based research as well as their ability to prospectively evaluate patients by contacting them for follow-up. A study from the University of Michigan showed that implementation of the HIPAA Privacy rule resulted in a drop from 96% to 34% in the proportion of follow-up surveys completed by study patients being followed after a heart attack. Another study, detailing the effects of HIPAA on recruitment for a study on cancer prevention, demonstrated that HIPAA-mandated changes led to a 73%

decrease in patient accrual, a tripling of time spent recruiting patients, and a tripling of mean recruitment costs." ("Health Insurance Portability and Accountability Act")

5. Case study

"Many researchers have expressed concerns that the Privacy Rule has adversely affected the progress of biomedical research." Many epidemiological and clinical studies have been hampered by the rule, however, single institution and peer reviewed journals have been hit the hardest. Epidemiologists were surveyed because they are an identifiable professional group of scientists engaged in human subject research, and their research often involves the use of medical records. E-mails were sent out to many organizations asking their members to respond to an e-mail survey and responding to the survey was anonymous. 13 societies decided to participate and over 10,347 people were sent the survey. Only people who were "professionals engaged in the conduct of US-based human subjects research and who recognized the term HIPAA" were asked to respond. 1527 people actually responded to the survey. (Ness)

The survey asked questions about the positive and negative influences the HIPAA Privacy Rule would have on their research. People were asked to quantitatively answer questions about the frequency of various types of activities such as data collection, changes in recruitment, level of difficulty in obtaining different types of data, and studies that were thought about but not submitted due to privacy concerns. They also asked researchers to rate their perceptions on a 5 point scale about the ease of conducting research and how it has affected participant privacy. Respondents were also asked to review 5 case studies and decide whether the IRB would approve them or not. They were also asked some open ended questions to learn more about their research.

Results:

Most of the people responding were women and most were employed in academia. When responding to their general perceptions about the impact of HIPAA's Privacy Rule, 84.1% reported that they believed the rule did not make research easier. 67.8% rated it a 5/5 in terms of how much it made their research more difficult. Costs were rated a 4 or 5 by 40% of the people and half rated the increased amount of time was a 4 or 5 as well. Nearly half of the respondents said that they had accessed data without authorization.

In the 5 case studies, all should have been allowable without patient authorization or a waiver. 4.7% - 20% responded that they though the case would be disapproved. 33.8% believed that it would be unconditionally approved, while 13.3% - 26.7% indicated they didn't know. 2/3 of the respondents rated that the rule made research more difficult a 4 or 5. As you can see this is a major problem. If researchers don't even understand the rules, how can they be expected to follow them?

In the open ended questions, 90% were negative comments about the effect of HIPAA, 5% were neutral, and 5% were positive. Researchers constantly expressed frustration and concern that the Privacy Rule had added burden without increasing privacy that much. Respondents also voiced concern with how HIPAA has slowed research. One person was quoted as saying "In the main, HIPAA has not prevented any research that I have desired to pursue. What it has done is to slow the research enterprise through its training and compliance elements. I and my staff spend more and more time doing compliance related things and less and less time doing actual research." (Ness)

Table 2. Scaled Perceptions of the Impact of the HIPAA Privacy Rule

Has the HIPAA Privacy Rule	No. (%)[a] 1-2	3	4-5	Don't Know
Made research easier	1085 (84.1)	82 (6.4)	18 (1.4)	105 (8.1)
Made research more difficult	112 (8.7)	210 (16.3)	875 (67.8)	93 (7.2)
Strengthened public trust	752 (58.2)	159 (12.3)	136 (10.5)	244 (18.9)
Enhanced confidentiality	603 (46.7)	262 (20.3)	334 (25.9)	92 (7.1)
Added cost	288 (22.3)	275 (21.3)	500 (38.8)	227 (17.6)
Delayed time to study completion	276 (21.4)	243 (18.8)	657 (51.0)	114 (8.8)
Affected research related to public health surveillance	163 (12.6)	165 (12.8)	601 (46.6)	361 (28.0)

Abbreviation: HIPAA, Health Insurance Portability and Accountability Act.
[a]On a Likert scale anchored by 1 = none and 5 = a great deal.

Table 5. Case Studies

	Would Your IRB Approve This Study?, No. (%) No	Yes, Unconditional	Yes, With Waiver	Yes, With Approval	Yes, Other Conditions	Don't Know
Participants from medical records contacted for interview/blood draw	184 (12.6)	123 (8.5)	262 (18.0)	522 (35.9)	135 (9.3)	229 (15.7)
Participants from cancer registry contacted to consent for interview	196 (13.5)	157 (10.8)	261 (18.0)	468 (32.3)[a]	175 (12.1)	193 (13.3)
Tissue bank to supply deidentified data for assay not in original consent	222 (15.6)	199 (14.0)	159 (11.2)	262 (18.4)[b]	291 (20.4)[c]	290 (20.4)
Medical record review from subjects now dead	61 (4.7)	435 (33.8)	280 (21.8)	109 (8.5)[d]	121 (9.4)	281 (21.8)
Limited data set from another hospital; research cannot be done without some identifiers	239 (20.2)	58 (4.9)	260 (21.2)	427 (36.0)[e]	123 (10.4)	317 (26.7)

Abbreviation: IRB, institutional review board.
[a]With physician approval.
[b]With authorization and reconsent from patients.
[c]Limited data set or other special circumstances.
[d]With approval from executor of estate.
[e]With limited data set agreement.

6. Compliance

In 2006 a survey was conducted by 1,117 hospitals and health systems. The American Health information Management Association found that compliance with HIPAA has declined. According to the survey, 85% of healthcare privacy officers and other related jobs indicated that their institution is more than 85% complaint, down from 91% in 2005. There was also an increase in the number of people who said they were less

than 85% compliant, up to 15% from 9% in 2005. Respondents said they thought that management support has also decreased as well.

Over half responded that they had trouble complying with rules dealing with PHI. The survey also claims that patients are becoming more concerned about their medical records as more people are asking questions about their data and how it is being protected. (“HIPAA Compliance Declines”)

Although compliance is going down, the government is not doing much about it. As of 2004, there had been over 19,000 complaints of failure to comply with HIPAA regulations. In 2006 only two criminal cases and no civil cases had been filed. According to the Washington Post the most common violations have been that personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained, or patients had problems getting their own records.

The government has ruled in over 14,000 cases that there was either no violation or to allow the violator time to fix their problem without penalty. The government is allowing them to resolve complains informally, letting those who have lapsed to reform voluntarily, without levying fines. This is significant for these companies because fines can be $25,000 for civil violations and $250,000 for criminal ones. Critics claim that without these fines, that HIPAA has no real power and companies have no reason to be compliant. (“Government Not Enforcing HIPAA)

Future of HIPAA / Conclusion

As we have seen, HIPAA has had a large effect on the industry today, both positive and negative. Companies are now protecting medical data more thoroughly, but this also has caused many hindrances. “For all its flaws, it was the catalyst that started the IT movement in this country. It opened the doors for a new relationship between providers and payers and trying to save money throughout the system.” Even though it hasn’t been heavily enforced, it has at least provided a blueprint for companies to follow. It makes them think strategically without breaking the bank. (HIPAA 10 years later)

However much has changed since HIPAA was first put into place. EMR were thought to be very cost effective over paper records when HIPAA was implemented. It has taken more than a decade for this to finally become true for these companies. Now that EMR’s are actually in place, more refinement and regulations will be needed. Over the course of the last ten years, the way companies have implemented EMR’s has surely deviated from the way that HIPAA prescribed. (“Health Insurance Portability and Accountability Act”)

The type of health information being recorded has also changed. Things that were previously not recorded are now common place in medical records. This means that regulations need to be put in place to make sure that they are covered under the same restrictions as all other types of data covered under HIPAA.

HIPAA needs to understand the direction that Healthcare companies are going in and what technologies they are adopting. They need to continually update HIPAA to cover these new technologies as well as continue to work on improving HIPAA overall. Research is extremely important to health care. Steps need to be taken in order to remove

some of the bureaucracy from the research process in order to maximize health benefits for everyone worldwide.

References:

"Government Not Enforcing HIPAA". The Information Management Journal. Sept./Oct. 2006.

"Health Insurance Portability and Accountability Act". Wikipedia. 20 Apr. 2008 http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

"Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets". Federal Register Vol. 68 No. 34. 20 Feb. 2003

"HIPAA and its Legal Implications for Health Care Information Technology Solution Providers". Information Technology Association of America and the Rotbert Law Group, LLC. April 20, 2004 http://www.itaa.org/isec/docs/hippawhitepaper.pdf

"HIPAA Compliance Declines, Survey Says". The Information Management Journal. July/Aug. 2006.

"HIPAA Made Simple: Pharmacist's Survival Guide." Pharmacist's Letter. Therapeutic Research Center, 2002. http://www.accessidaho.org/bop/education/HIPAA%2002014.pdf

Lawrence, Susan. "Access Anxiety: HIPAA and Historical Research. Journal of the History of Medicine and Allied Sciences". Vol. 62. No. 4. 2007

Ness, Roberta. "Influence of the HIPAA Privacy Rule on Health Research". Jama Vol. 298. No 18. November 14, 2007

"Standards for Privacy of Individually Identifiable Health Information as Pertains to Pharmacy." Department of Health and Human Services http://www.etreby.com/PDF_Files/HIPAA/HIPAA%20Privacy%20Standards%20for%20Pharmacies.pdf