Healthcare Applications and HIPAA

BA590-IT Governance
Final Term Project
Prof. Mike Shaw

Michael McIntosh
Table of Contents

1. Abstract 3
2. Introduction 3
3. Section 1: HIPAA definition and history 4
4. Section 2: Impacts of HIPAA 9
5. Section 3: HIPAA complaints and enforcements 11
6. Section 4: Trends in HIPAA compliance 13
7. Section 5: The future of HIPAA 14
8. References 16
Abstract
According to the United States Congress, who passed the Health Insurance Portability and Accountability Act of 1996, it has become increasingly important to protect the privacy of peoples’ health and medical records, also known as protected health information (PHI). However, since the passage of the Act in 1996 and the provisions that have passed since then, little to no progress has been made to secure the privacy of electronic health records. HIPAA violations can be found in news headlines with alarming regularity all across the country. The questions remain, why is HIPAA failing and what can be done to improve it?

Introduction
The original idea with HIPAA is to protect the rights of the people of the United States of America. Specifically it was created to protect electronic health records and ensure that they are kept private no matter what organization was holding the data. From health insurance companies to doctors’ offices to pharmacies, every business that held privileged information would have to adhere to these regulations. From a personal perspective, my family business, which I hope to run one day, is in the pharmaceutical business, which means that in order for me to both effectively run my business and stay complaint with all government regulations, it is imperative for me to know the ins and outs of every provision of HIPAA.

The purpose of this project is fivefold:

Section 1: HIPAA definition and history
In this section I will discuss the nature of the legislation and track it through different stages of implementation and execution. I will also include any information on revisions of legislation as it pertains to healthcare privacy.

**Section 2: Impacts of HIPAA**

In this section I will give sort of a state of the union with the current situation regarding privacy. I will give examples of both positive and negative impacts of HIPAA.

**Section 3: HIPAA complaints and enforcements**

In this section I will discuss statistics related to the complaints that have been filed to the Department of Health and Human Services. This section will include the types of complaints, the type of health care facility the complaints were filed against, and the enforcement resulting from the complaints.

**Section 4: Trends in HIPAA compliance**

This section will focus on recent trends involving HIPAA compliance such as what kinds of companies are most or least likely to become compliant and why.

**Section 5: The future of HIPAA**

This section will include some insight into what will possibly happen with the future of HIPAA and what the government and the companies can do in the future to increase compliance.

---

**Section 1: HIPAA definition and history**

---

Title I
HIPAA is generally separated into two sections called Title I and Title II. Title I is called “Health Care Access, Portability, and Renewability”, and it focuses on amending two acts: the Employee Retirement Income Security Act and the Public Health Service Act. The general purpose of Title I is to protect the insurance coverage of workers, and whomever else is covered by their insurance plan, when they change or lose their jobs. Although Title I is an important part of HIPAA, it is not the general focus of this research paper.

**Title II**

Title II of HIPAA, entitled “Preventing Health Care Fraud and Abuse; Administrative Simplification,” focuses on defining HIPAA offenses, setting penalties for violating HIPAA regulations, and creating programs to control fraud and abuse within the health care system. Title II specifies that the Department of Health and Human Services must develop rules and standards aimed towards handling health care information efficiently and securely. The Dept. of HHS came up with a set of five rules to satisfy this request. Those five rules are the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

**The Privacy Rule**

The HIPAA Privacy Rule represents a set of standards for the privacy of individually identifiable health information. It provides the first national standards for protecting the privacy of health information. This rule specifically regulates how health plans, health-care clearinghouses, and health-care providers who transmit health information in
electronic form disclose certain individually identifiable health information. According to a government website, the Privacy Rule is responsible for the following:

- gives patients more control over their health information;
- sets boundaries on the use and release of health records;
- establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;
- holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights;
- strikes a balance when public health responsibilities support disclosure of certain forms of data;
- enables patients to make informed choices based on how individual health information may be used;
- enables patients to find out how their information may be used and what disclosures of their information have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

**The Transactions and Code Sets Rule**
The purpose of this rule is to set a standard for codifying electronic health records for Electronic Data Interchange (EDI) transactions. Transactions that fit this standard are transactions for health care claims, send payments, enroll for benefits and/or maintenance, inquire about eligibility for benefits, check the status of a claim, and many others.

The Security Rule

The Security Rule addition to HIPAA was designed to address the American public’s concern about the privacy and security of private health records. This concern grew as disclosures of personal health conditions popped up in the news and stories developed of hackers and misdirected emails revealing other private information. The Security Rule acts as a type of framework with sections including a list of administrative procedures, which act as a list of twelve areas to implement and maintain, physical safeguards to prevent unauthorized access to information, technical security services to control access and authentication while still maintaining adequate access times, and technical security mechanisms designed to allow transmission of sensitive data over open networks (such as the internet) without being easily intercepted by third parties.

The Unique Identifiers Rule

In the past, healthcare organizations have used different numbers or names to identify each other when conducting business with each other electronically. The Employer Identification Number (EIN) was originally suggested to be used as an identification number for all companies in the original version of HIPAA. Since then, provisions have
been made and a new number called the National Provider Identifier (NPI) has been implemented. This is the identification that is required by all health care providers under the Unique Identifiers Rule. The compliance date for NPIs is May 23, 2007 for all covered entities except small health plans who get an extra year to comply. After all is settled, it will have taken over ten years to implement a consistent method of identification for electronic communications since the first HIPAA documents were passed.

The Enforcement Rule

The original version of HIPAA Title II only had four rules. The Enforcement Rule (or Final Rule) was designed to address concerns that HIPAA was not being enforced even though violations were repeatedly occurring. In order to give HIPAA more “teeth” the enforcement rule was created. Under this rule the Office of Civil Rights will enforce the civil side and the Department of Justice will enforce the criminal side. The maximum penalty for civil penalties is $100 for each violation with a cap of $25,000 for all identical violations during a single calendar year. For the criminal offences, which include obtaining or disclosing individual health information or fraudulent use of NPIs, the following chart of penalties will be enforced:

<table>
<thead>
<tr>
<th>Offence</th>
<th>Fine</th>
<th>Prison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowingly</td>
<td>$50,000</td>
<td>1 Year</td>
</tr>
<tr>
<td>False Pretenses</td>
<td>$100,000</td>
<td>5 Years</td>
</tr>
<tr>
<td>For Profit, Gain, or Harm</td>
<td>$250,000</td>
<td>10 Years</td>
</tr>
</tbody>
</table>

Section 2: Impacts of HIPAA

The regulations and security measures put in place by HIPAA has had a major impact on both clinical practice and research studies in the health care industry. Along with compliance comes an increased burden to implement safeguards and procedures to protect PHI and stay HIPAA compliant. Although the advent of HIPAA has improved the landscape of data protection and security, it has had other negative ramifications.

HIPAA on Research

Because of increased levels of security and more involved safeguards to protect information, it has become increasingly difficult for researchers and organizations associated with researchers to operate as quickly, cheaply, and efficiently as pre-HIPAA days. Several studies have shown a decline in participation rates in clinical trials and human research as a direct result of HIPAA regulations. One of the reasons behind the increased decline in studies is the informed consent process since the implementation of HIPAA regulations. Consent forms have become much longer and much more difficult for the common person to understand in order for them to fully grant the release of PHI. This has both decreased participation and undermined the goal to involve patients in the decision to participate in research. Rather than making them feel better about the security of their private information, this implication of HIPAA has dissuaded them from participating in potentially beneficial research studies.
Not only does HIPAA make it harder for researchers to get participation, it actually makes it more expensive and takes more time than in the past. One study analyzed data every week from January 2003 to December 2003 in order to compare the statistics of the study before and after HIPAA privacy implementation. Not surprisingly, the study showed a 70.1% decrease in patient participation, an increase of time and cost from 4.1 hours and $57 to 14.1 hours and $197 per participant. Finally, recruitment completion time for participants in the study increased from 60 weeks to 171 weeks as a direct result of HIPAA.

**HIPAA on Quality of Service**

Although estimates for the cost of HIPAA compliance range from the millions up to $25 billion, the fact remains that budgets of health care providers have changed drastically. Historically, the health care industry has lagged behind technologically, only spending 1 to 3 percent of its revenue on IT. According to some research, IT investments will increase drastically in order to reach the HIPAA compliance deadlines and avoid penalties. Many IT systems will need to be completely overhauled to become compliant, placing a large, unexpected financial burden. The major problem with these costs is that they are competing with other important budgeting items, such as new medical equipment or new personnel. The fear is that this will begin to affect the quality of service provided by HIPAA compliant organizations.

Another consideration of HIPAA’s effect on the quality of healthcare today is related to clinical workers not knowing exactly what they can disclose to which party. A common
problem is that physicians and their staff simply do not know who they are allowed to
disclose the information to, and rather than violate HIPAA sanctions they choose to err
on the side of caution. As a result, people who need PHI in order to perform their duties
are being denied. The only way to work around this problem is to spend extensive time
and money training your employees so that they know the precise limitations associated
with compliance.

Section 3: HIPAA complaints and enforcements

Filed complaints and investigations

According to the United States Department of Health and Human Services, they have
received over 26,000 HIPAA complaints since April of 2003. Of those complaints, 78%
or 20,477 cases have been resolved; 4,447 of those through investigation and
enforcement which resulted in a direct privacy practice change in the violating entity,
2,155 which after investigation showed no signs of a violation, and 13,875 which were
not eligible for enforcement under HIPAA. Of the compliance issues that did result in an
investigation, five most popular, in order, are:

1. Improper uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Uses or disclosures of more than the Minimum Necessary protected health information; and
5. Lack of or invalid authorizations for uses and disclosures of protected health information.

Also of the complaints that resulted in investigations, the most common types of entities
that required corrective action to achieve compliance are, in order:
For an annual comparison of the number of complaints filed and how they were handled, consult the figure below.

![Investigated Resolutions](http://www.hhs.gov/ocr/privacy/enforcement/numbersglance.html)

As you can see from the graph, the number of investigations has been increasing steadily over the last three years as public awareness and concern over HIPAA regulations and security has increased.

As of February 2007, of over 26,000 HIPAA complaints filed to the HHS, a mere 350 complaints were passed onto the Department of Justice for criminal enforcement. Over the four year period since 2003, a grand total of four criminal HIPAA violations were prosecuted in the United States. Only the most severe cases went to trial such as an
employee using PHI from patients with terminal cancer to obtain credit in their name or a case where a physician’s assistant knowingly attempted to sell medical records of an FBI agent to a believed drug trafficker. There is a severe lack of enforcement from the Department of Justice for HIPAA violations.

Section 4: Trends in HIPAA compliance

When HIPAA first went into effect, it was greatly criticized as not having enough “teeth.” Critics were saying that a lack of penalties for violations made HIPAA a truly voluntary idea and that the establishment of these rules and standards was futile without any form of punishment. The government responded with the final Enforcement Rule which went into effect in March of 2006. Despite efforts to revamp the enforcement of the HIPAA rules, according to most surveys HIPPA compliance declined in 2006. The reasons stated behind the decline are simple: the benefits are speculative and slight. Professor Mark Rothstein of the University of Louisville states that the “greatest value has been in translating an often-overlooked ethical imperative into a legal requirement.” Although this has great social implications, as far as the bottom line, health care players have no incentive to do anything more than the minimum to avoid huge HIPAA violations. The importance of 100% HIPAA compliance has continued to decline recently.

On the idea of a lack of compliance, larger hospitals have been especially slow to comply with standards. A study sponsored by Phoenix Health Systems and the Healthcare
Information and Management Systems Society showed that the complex systems and processes infrastructure involved in larger hospitals has been one of the key factors in slowing down their compliance. A possible cause of this is the cost associated with compliance, especially with a large IT infrastructure, weighed against the lack of financial benefits. As long as health care providers are allowed to voluntarily comply with regulations without facing penalties, large hospitals will continue to fall behind.

Section 5: The future of HIPAA

Since HIPAA compliance has become a painstakingly slow operation, questions have arisen about HIPAA being a failure. If you think about the goals at the core of HIPAA, securing information and providing privacy to the people, HIPAA has made some great successes: there have been significant increases in the utilization of electronic medical record systems, there have been many efforts to adopt secure, industry-wide messaging standards, a federal health information technology office was established in 2004, and early steps toward developing national health information networks have been taken.

Although there have been many positive strides with regards to securing and protecting sensitive health care information, there is still a long way to go. I believe there are some major changes that must occur before HIPAA compliance can really move forward. I think the next major step that must be taken is for HIPAA compliance to become a mandatory standard, comparable to Sarbanes-Oxley. The only way to ensure 100% compliance is to truly enforce the standards that have taken so much time and effort to
develop. The major complaint about HIPAA is that it is not being and cannot currently be enforced. A chain of events must occur before HIPAA compliance can move forward. First, the hypothetical benefits that were imagined at the early beginnings of HIPAA must begin to be realized. Until compliance can have a positive effect on efficiency and/or financial expectations, company’s will either hesitate to spend the money and resources to become compliant or they will just flat out not be able to afford it. Therefore if companies exist that cannot afford to succumb to the accepted standard, that standard will be impossible to enforce. Once the benefits can be realized, it is imperative that the government make HIPAA compliance mandatory instead of voluntary. Although I think this is the future of HIPAA compliance, I do not think it will happen for several years. Unfortunately major violations occur on an almost daily basis with very little legal recourse against the offenders. The future of medicine appears to be online treatment such as WebMD.com and various health sites. In order to continue to move healthcare to the front end of technology, we look towards the government and HIPAA to provide the framework and the guidelines to give the people assuredness that their information will be protected.
References


Health Insurance Portability and Accountability Act
http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

HHS Announces Its New Comprehensive “Enforcement Rule” for HIPAA Violations

HIPAA Enforcement Rule Overview

HIPAA Security, Privacy, Transactions and Code Sets, and National Identifiers Rule Overview and Summary

Phoenix Health Systems. HIPAAAdvisory
http://www.hipaadvisory.com/


Tucker, Stephen. *HIPAA Privacy Rule and Public Health* http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

United States Department of Health & Human Services
http://www.hhs.gov/