HIPAA: The Application and Challenges of Implementing Healthcare Information Technology

Eric Kolman
May 2007
Professor Shaw
Table of Contents

1. Introduction ................................................................. 3
2. Overview: Key Terms ....................................................... 4
3. Overview: What is HIPAA? ............................................... 5
   3.1. Title I ........................................................................ 6
   3.2. Title II ........................................................................ 6
4. Review of Technology ....................................................... 9
5. Issues with Technology ...................................................... 10
   5.1 Implementation status of clinical IT ......................... 12
6. Case Study: HIPAA Compliance Survey Results, Winter 2006 .... 13
7. Conclusion ...................................................................... 16
8. References ..................................................................... 17
1. Introduction

The Healthcare Industry has been undergoing radical transformations and has been rapidly changing to adopt information technology solutions to meet the challenges of regulatory burdens, cost reduction, and patient care. A few examples of the solutions being implemented are computerized physician order entry initiatives (CPOE), electronic medical records (EMR), and electronic claims processing. A recently study has shown that healthcare providers in the United States will increase IT spending from $15.1 billion in 2002 to $17.3 billion in 2007.\(^1\) The demand for healthcare technology has significantly increased and has created remarkable opportunities for health care solution providers. The expanding use of IT though has also created numerous challenges for organizations. As information in the healthcare industry moves to becoming completely electronic, privacy and security concerns are increasing. The foremost concerns hospitals and healthcare systems face are protecting the patients’ information and making sure it is secure and preventing people from accessing the information who should not have access. Healthcare organizations look to IT to help them solve this problem but fulfilling the promise of technology is an ongoing and daunting task due to limited budgets, the need for legacy system migration and new technology insertion. A regulatory framework has been put into place in order to respond to these rising concerns. Part of this regulatory framework is the Health Insurance Portability and Accountability Act, otherwise known as HIPAA. Health plans and health care providers who transmit health information in electronic form must be in compliance with HIPAA or face the possibility of significant fines or even jail time.

\(^1\) Robert Law Group, LLC and Information Technology Association of America. “HIPAA and its Legal Implications for Health Care Information Technology Solution Providers.”
2. Overview: Key Terms

To fully understand the implication of HIPAA, it is first necessary to establish a core understanding of some of the key terms that will be discussed. It is important to distinguish between many of the terms used in this paper in order to prevent confusion. Some of the terms that will be discussed are covered entity, health plans, health care clearinghouse, health care provider, PHI, EMR and CPOE.

First, a covered entity includes a health care provider that provides, bills for, or is paid for health care. A covered entity can be classified as institutions, organizations or people. According to HIPAA, covered entities can be health plans, health care clearinghouse or any health care provider who transmits any health information in an electronic transaction (e.g., Hospitals, Physicians, Public Health Departments, Home Health.) Health plans means any individual or group plan that provides, or pays the cost of, medical care including public and private health insurance issuers, HMO’s or other managed care organizations, Medicare and Medicaid programs or any other program for which the main purpose is to provide or pay for health care services.²

A health care provider then can be classified as a provider of medical or health services, and any other person or organizations that furnish, bills, or is paid for health care in the normal course of business.³ A health care clearing house on the other hand is public or private entity, including a billing service, re-pricing company, community health information system that either processes or facilitates the processing of health information.⁴

Next it is important to discuss PHI, which stands for protected health information. Protected health information means individually identifiable health information that is

² “Privacy/Data Protection Project.”
³ “Privacy/Data Protection Project.”
⁴ “Privacy/Data Protection Project.”
transmitted electronically, maintained in any medium that is defined as being electronic media, or transmitted in any other form or medium. PHI is the basis for many of the requirements under HIPAA. Examples of PHI would include medical records, social security numbers or even policy numbers.

In this paper, I will constantly talk about EMR and CPOE. EMR stands for Electronic Medical Records. EMR is one of the new technologies that have been implemented in hospitals and healthcare systems to make medical records more efficient and secure. An EMR facilitates access of patient data by clinical staff at any given location, an increase in liability coverage, standardization of care pathways and protocols, prescriptions, scheduling, and other functions.

CPOE stands for computerized physician order entry. A CPOE is a process of electronic entry of physician instructions for the treatment of patients under his or her care. The orders are communicated over a computer network to the medical staff which could include nurses and other physicians or communicated to different departments such as pharmacy or laboratory that are responsible for fulfilling the order. CPOE decreases the delay it takes to complete orders and reduces the errors related to handwriting which can be very costly to organizations.

3. Overview: What is HIPAA?

In 1996 HIPAA was enacted by congress as part of an attempt to reform health care. HIPAA aims to make changes or reforms in the following areas: portability of health insurance, prevent healthcare fraud and abuse, administrative simplification, tax related provisions, group health plan requirement and revenue offset. HIPAA was created with the purpose to lower health care administrative costs, improve the efficiency and effectiveness of health care system and also to protect patient health information. HIPAA can be broken down into Title I and Title II.
3.1. Title I

Title I of HIPAA addresses the “Portability” aspect in HIPAA. Basically Title I protects health insurance coverage for workers and their families when they change or lose their jobs. Title I prohibits any group health plan from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability.

3.2. Title II

Title II is more important as it makes up the majority of HIPAA. Title II requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Title II is composed of four parts: privacy, security, transaction standards and code sets, and unique identifiers.

The privacy rule of HIPAA took effect on April 14, 2003. The privacy rule establishes regulations for the use and disclosure of PHI. It states that the customers have a right to ask covered entities, who maintain PHI information about them, to take reasonable steps to ensure that their communications with the individual are kept confidential. At the same time, the privacy rule also outlines the rights and responsibilities to the covered entity. A covered entity may disclose PHI to facilitate treatment, payment, or health care operations. However, if a covered entity discloses any PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose. As we will discuss in the next paragraph, the Security Rule complements the Privacy Rule.

The Security Rule took effect on April 21, 2003. It was mandated that most covered entities were compliant by April 21, 2005 and for “small plans” the date was April 21, 2006. The Security Rule is primary composed of three types of security safeguards: administrative, physical, and technical. The rule identifies various standards for each safeguard. Administrative safeguards are policies and procedures designed to clearly show how the entity will comply with
HIPAA. A few provisions under the administrative safeguards are as follows. Covered entities must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures. Another provision is that procedures should clearly identify employees or classes of employees who will have access to PHI. This provision is one of the more important provisions as patient health data is very sensitive and without the right safeguards in place, there is a great possibility that the information could be leaked to the wrong source. The purpose of physical safeguards is quite straightforward; to physically control access to protect against those who attempt to access protected data. The main safeguard here is that access to the equipment containing health information should be carefully controlled and monitored. This can happen by limiting usage of hardware and software to properly authorized individuals and also implementing access controls such as security plans, maintenance records and visitor sign-in. Technical safeguards basically control and protect the communications containing PHI that is transmitted electronically over networks from being intercepted from hackers or unintended recipients. To ensure this happens, data corroboration must be in place which includes the use of check sum, double keying, message authentication, and digital signature. Covered entities must also implement an authentication system which involves making sure that an entity is who it claims to be. Email has become the preferred channel of communication among many organizations. E-mail messages that contain sensitive or confidential information must be encrypted and delivered securely to protect privacy. According to the AHA, IronPort Email encryption provides secure point-to-point delivery of message without requiring the recipient to install any software\(^5\).

The Transaction and Code Sets Rule was scheduled to take effect October 16, 2003 but because of widespread confusion and difficulties of integration, there was a one year extension to

\(^5\)“Secure Messaging.” AHA Solutions.
all parties. The TCS Rule basically is concerned about standards for electronic health transactions. Regulations associated with the TCS Rule mandate uniform electronic interchange formats for all covered entities. Unlike the Privacy Rule which applies to PHI in any form or medium, the TCS Rule covers only PHI in electronic form. In addition to the standardized electronic health transactions, HIPAA calls for standardized code sets describing health problems, causes, symptoms, etc. While many entities in the health sector have developed or are in the process of developing EDI standards, the consensus remains that the lack or common industry-wide standards is a major obstacle to realizing profit efficiency and savings. With the standard, payers must accept a standard transmission; they can not pay a non-standard transaction. The information includes what information is sent, the data type and field properties of the information being sent, and finally how the information is arranged and sent for a claim. For example, the content would be a subscriber’s name or address. The format could entail the maximum characters a name can have or the format that the date is sent in. And the form would specify if the subscriber was a patient that it should take a certain path. The goal of these standards is to improve efficiency and reduce errors in healthcare delivery.

The Unique Identifiers which was effective May 2006, states that all covered entities using electronic communications must a single new National Provider Identifier. The National Provider Identifier replaces all other identifiers used by health plans, Medicare, Medicaid and other government programs. The NPI consists of 10 numbers, the last being a checksum. The NPI is merely a number, it is unique and national, it is never re-used and typically a provider can only have one. The NPI ultimately will reduce errors and costs for organizations.

---

**Review of Technology**

Currently, hospitals and healthcare systems are in the dinosaur age in terms of technology. A majority of hospitals are beginning to implement the technologies of CPOE and EMR. Here, I will give an overall description of the technologies and their function.

CPOE, as we learned before stands for Computerized physician order entry. CPOE systems allow physicians to electronically order medications, tests, and consultations. They provide advice on best practices and alerts to the possible adverse consequences of a therapy. There have been numerous studies that have shown that CPOE can lead to fewer adverse drug events and other improvements which is a primary reason for a call for universal CPOE adoption. Some of the features that CPOE improves are: Ordering, patient safety features, intuitive human interface, regulatory compliance and security, portability, management and billing. In regulatory compliance, access is secure and a permanent record is created with electronic signature. Ordering allows physician orders to be standardized across the organization, yet also individualized for each doctor by using order sets. Orders are communicated to all departments and involved caregivers. CPOE has had much success in some health care systems. For example, the Veterans Health Administration has seen a 75% reduction in medication errors. Implementation of CPOE technology has decreased the rate of non-missed-dose medication errors. The next technology that will be discussed is EMR.

The development of standards for EMR interoperability is at the forefront of the national health care agenda. Basically an EMR is a patient record, in which all information is stored electronically in such way that it may be found and reused by means of computer tools. Without interoperable EMRs, practicing physicians, pharmacies and hospitals cannot share patient information, which is necessary for timely, patient-centered and portable care. EMRs are

---

7 “Trends to Watch in Healthcare Information Technology”
very beneficial because they populate a patient's lifetime digital record which includes medication history, lab tests, and radiology images can even be secured and shared between multiple providers to improve the quality of care. EMRs also can prevent medical errors by having a patient’s complete medical history on hand and so on. Currently there are multiple vendors of EMR systems, each selling software that is not compatible with their competitors'. According to a recent survey by the American Hospital Association (AHA), over two-thirds of hospitals had either fully or partially implemented EMR (Electronic Health Record) in 2006. The 11% with fully implemented EMRs were most likely large, urban or teaching hospitals. Hospitals without an EMR were primarily small, rural, non-teaching, and did not belong to a health system.

**Issues with Technology**

While the advancements of technology in the healthcare industry have been revolutionized health care, there are still several issues with certain technologies which are hindering their expansion. There are many risks associated with implementing CPOE. New types of errors arise which can cause several different dangers. The first issue is with inexperience with the product. Staff inexperience could cause slower entry of orders, use more staff time and also cause slower person-to-person communication in an emergency situation. The communication between physicians and nurses could also be effected if each group works by themselves at their workstations. Even though the CPOE is designed to reduce errors, moving to a computer based system can still create problems. Frequent alerts and warnings that the computers give could interrupt work flow, which would result in the user either ignoring or overriding the messages. Another issue with CPOE systems is that each hospital and healthcare system is so complex in a sense of their needs and unique patients and care settings, that the

---

8 “Continued Progress: Hospital Use of Information Technology” AHA
system could take years to install and configure so it is run effectively and efficiently. Much of
the resistance to adopt CPOE technology is because doctors do not want to move away from
their current practice patterns, there are many costs including training time involved, and there are
concerns with interoperability and compliance with future national standards.

The issues that arise with EMR are very similar. In order to reap the benefits of
accessibility, efficiency, patient safety and cost savings by EMR, the old paper medical records
that are currently used by hospitals should be ideally be incorporated into the patients health
record. The scanning process in order to convert them to EMR is expensive and time-consuming
and also must meet many standards to ensure exact capture of the content. Also, the destruction
of original healthcare records must be done in a way that ensures that they are completely and
confidentially destroyed. If the information is not properly destroyed, this could substantially
hurt the reputation of hospital or physician. One main issue with EMR that HIPAA is addressing
is privacy concerns. Many individuals, ranging from nurses to physicians to billing clerks have
access to at least part of the patient’s records. It is a very difficult and time consuming process to
determine which people have access to which information and then to implement these controls
into the system. Finally, there are several limitations in software, hardware and networking
technology that have made it hard for EMR to be implemented in small healthcare organizations
that may not necessarily have the budget to adopt the technology. Until recently, most EMR
systems used Visual Basic and C++. However, now most EMRs are being developed using new
.NET and Java technology. The widespread adoption of wireless internet also raises red flags.
Because some wireless networks needed multiple access points, it created many holes for
intruders to get into the network granting them unauthorized access. New wireless technologies
such as IEEE 802.11 g and n have been developed which have allowed wireless technologies to
be more secure and increase transfer speeds. The main issue that arises with hospitals and health care systems is that costs outweigh the benefits that CPOE and EMR can provide. Many hospitals do not want to take the time to switch to using new healthcare technology because their current system is working fine. Next, I will discuss the implementation status with clinical IT.

**Implementation status of Clinical IT**

In this section, I will give an update on the current implementation status of clinical IT. According to the lecture notes of A.F. Cutilletta, MD, the overall perception is that physicians are not eager to adapt to new information technology. According to a recent survey, 84% of the 256 respondents said that clinical IT would be very valuable to their institution. However, when asked what the top reason for non-adoption, 75% responded “unwillingness to change.” For those who have already implemented clinical IT into their institution, the question of “How much value has clinical IT demonstrated?” was asked. 49% of respondents said very valuable, while 47% said somewhat valuable.\(^9\) So the main question arises: Why the problem of non-adoption? This question can not be answered because of four issues. The first reason is that there is a lack of measurement. There are no evaluative definitions for success which leads to goals being left unmet. Also, having no definition for success means that full value can never be attainable. The next issue is that it is not being designed for users. There is too much of a focus on prioritizing system install and budget while there should be a greater focus on process change. Next is the issue of settling for low adoption. If smaller hospitals do decide to implement clinical IT, they will only do the minimum to just get by and be compliant. Hospitals are under-preparing users for change and under-selling the importance of IT. Not having proper utilization prohibits value creation. The last issue is that hospitals are viewing implementation of IT as an end state. They view the project of implementing IT as “complete” after installation and do not

---

\(^9\) Cutilletta, MD, A F. "Clinical IT: the Wiring of Healthcare."
take any means to increase its effectiveness. Next we will look at a current case of how compliant hospitals and healthcare systems have been with HIPAA.

**Case Study: HIPAA Compliance Survey Results**

The survey that I will discuss is published bi-annually by HIMSS and Phoenix Health Systems. A total of 324 healthcare industry representatives responded to email notices about the Survey that were sent to HIMSS members and to Phoenix HIPAAAlert subscribers. In this survey, the main issue is how compliant health care systems and hospitals are being with HIPAA. HIPAA’s impact on the healthcare industry is evolving from “compliance” to an emphasis on new electronic opportunities for better communication across the continuum of care. Both Providers and Payers varied there responses in their ranking of the roadblocks they have faced in achieving compliance with the Privacy, Security and Transactions regulations. The results are as follows: changes in regulations/deadlines, organizational constraints, and no anticipated legal consequences for non-compliance are the top three for reasons for Providers and interpretation of regulations, inadequate expertise available, and achieving successful integration of new systems and process are the top three for Payers. Many organizations merely have limited resources available or simply there is a lack of buy-in from senior leadership. Results from this survey reflect Privacy, Security and Transaction and Code sets compliance.

First I will address Privacy compliance. As of January 2006, 80% of Providers and 86% of Payers indicated that they were compliant with the HIPAA Privacy Regulations. Among Providers, hospitals with more than 400 beds were the most compliant at 85% while hospitals with less than 100 beds were the least compliant at 80%. On the next page you will see graphs representing this information.10

---

There has been a steady increase since the last survey, but the numbers are still not up to par.

Next is how compliant hospitals have been with the Security standards. Even though the deadline for compliance was April 20, 2005, a large number of Providers and Payers remained non-compliant. Providers have made little progress from 43% in July 2005 to 55% in January 2006. Among providers, hospitals with over 100 beds had the lowest compliance at 48%. Payer compliance levels actually decreased from 74% to 72%. When non-compliant respondents were asked to list the Security standards their organizations had implemented, contingency planning and emergency access procedures ranked the lowest. Risk management and workstation use and security were ranked the highest. Below is a graph to represent the data.\textsuperscript{11}

Finally, we will see how compliant organizations are with the Transactions and Code Sets Standards. TCS compliance is a little different than Privacy or Security compliance. Respondents interpret “ready to conduct” or “capable of conducting” transactions as being compliant. In those regards, TCS compliance has steadily improved recently. There has been an increase from 80% to 84% of Providers who say they are fully compliant. However, when the respondents were asked if they were actually conducting all the necessary standard transactions for their organizations, only 46% responded. Even though many non-compliant organizations plan to do so in the future, 7% of non-compliant Providers and 33% of non-compliant Payers reported that they have no plans to become compliant. Below is an overall comparison of TCS compliance.\(^\text{12}\)

\[\text{Industry TCS Compliance Comparison: Winter 2006 with Summer 2005}\]

The top three obstacles to TCS Implementation are insufficient management support, installation of critical software not complete, and ambiguities in information released by CMS regarding standard transactions requirements.

Conclusion

In conclusion, the potential of health information technology to improve the care patients receive and the overall efficiency of the health care system has become a central part of the national health care debate. Many hospitals and health systems have embarked on the challenging journey of IT adoption. Advances in IT have allowed hospitals to become more efficient and secure in dealing with patient information. The idea of moving completely wireless in the healthcare industry is a concept that is becoming more and more feasible to reach. However, use of health IT is not yet universal due to financial, technical, implementation, and policy barriers. Technology is only a tool and if used effectively can improve the flow of information and potentially improve the efficiency of the physician’s practice. However in reality, if “change” is not embraced, the probability of success is very low. The benefits of implementing healthcare technology and being completely compliant must be very clear to smaller healthcare organizations in order to become widespread.
References


