https://doi.org/10.48009/2_iis_2009_439-443

CUSTOMER PRIVACY CAN BE COSTLY: THE CASE OF HIPAA

Wallace A. Wood, Bryant University, wwood@bryant.edu

==========

ABSTRACT

The Health Insurance Portability and Accountability Act (HIPAA) was originally intended as a vehicle to protect patients with long term illnesses or injuries. It was designed to provide protection from insurance plan to insurance plan so that individuals could not be denied insurance based on pre-existing conditions and could not be subjected to waiver periods. This paper examines the privacy rules (one of five sets of rules) established under HIPAA with regard to their complexity, degree of compliance by healthcare organizations, cost of compliance and their impact on medical research. It was found that patient (customer) privacy has been partially achieved at a high cost.

Keywords: HIPAA, patient privacy, electronic medical records

INTRODUCTION

With today's mobile society, patient health care involves seeing a variety of providers and specialists. Unfortunately, these providers and specialists currently have no systemized way to get the whole picture of a patient's medical history and care. What is needed is an electronic health information network which will enable continuity of care independent of provider type, location or other circumstance. This sharing and synchronization of medical information and knowledge will provide many benefits to patients, not the least of which will be a reduction in medical errors. Efforts to bring about this sharing of medical information are proceeding on many fronts. Hopefully, one day in the not too distant future, comprehensive medical information will be there for every patient - a comforting thought when that patient needs emergency room care. Recently, President Obama has made a nationwide comprehensive electronic medical record system a priority for his administration with a deadline of 2014. This is consistent with the 10 year timetable established by President Bush in his 2004 State of the Union address calling for the computerizing of health records.

A major concern in developing a comprehensive network of patient medical information is that of security of this information in order to maintain patient privacy. Both the security and privacy of this information has been addressed by health care organizations with much effort and expense since 1996 because of the passage of The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA, previously known as the Kennedy-Kassebaum bill, was signed into law on August 21, 1996, and was intended to improve the portability of health care benefits and create greater accountability to reduce health care fraud [1]. The privacy regulations set forth by the federal government under Title II of HIPAA in 1996 were to mitigate the risks of healthcare fraud and abuse, create opportunity and efficiencies through administrative simplification, and to promulgate medical liability reform. The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic data interchange; standardized transaction and code sets; unique identifiers for providers, employers and health plans; specific security procedures; and standards for the protection of the privacy of patient's identifiable health information.

Within each category, laws have been enacted describing the responsibilities required for healthcare organizations to become compliant. The Privacy and Security Standards have been the most challenging to comply with [5]. The HIPAA Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information called protected health information (PHI). Among other provisions, the Privacy Rule

- 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 [17].

Changes to HIPAA were recently enacted under The Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the recent American Recovery and Investment Act, but these do not go into effect until February 2010 [13]. Another change scheduled to be effective May 1, 2009 is the 'red flag" rule being applied to physicians which requires many physicians to assist the government in detecting, preventing, and mitigating "red flags" of identity theft. A red flag is defined by Federal Trade Commission as a "pattern, practice, or specific activity that indicates the possible existence of identity theft [7]." However, this paper will concentrate on the present privacy and security aspects of HIPAA.

IMPLEMENTING HIPAA

As might be expected with a law as complicated and comprehensive as HIPAA, healthcare organizations coming under its provisions face a variety of problems in becoming compliant. Under HIPAA there are three general groups of organizations: covered entities, business associates, and everyone else. Covered entities are health care organizations and health insurance companies. Business associates are organizations that support covered entities and handle protected health information (PHI) such as on-line backup providers, billing agencies and organizations that support eHealth products. Everyone else includes patients (customers) who will likely be required to identify themselves more strongly to business associates to gain access to their information [13]. Protected health information (PHI) is individually identifiable health information relating to an individual's past, present or future physical or mental health condition, provision of health care, or payment for the provision of health care. It also includes names, addresses, telephone numbers, medical record numbers, and Social Security numbers [9].

Some of these problems faced by these three groups are detailed in the following sections along with some difficulties that might not have been foreseen by the drafters of the legislation.

Problems in Complying

Since 1996, healthcare organizations have struggled to adapt and conform to these loosely defined federal statutes of HIPAA with many still trying to achieve compliance because of the lack of clarity, openness to interpretation and the constant change of the privacy and security rules. The complexities of HIPAA when combined with the constant HIPAA rule modifications make compliance a daunting task [6].

The compliance of the various stakeholders under the HIPAA privacy regulations has been difficult to evaluate because of the lack of published data by health care organizations.

A major exception is The Healthcare Information and Management Systems Society's (HiMSS) 2006 survey. This survey revealed that 78% of healthcare providers and 87% of health plans reported compliance with the privacy regulations [18]. However, a closer examination reveals that no health plan or provider was compliant with every key privacy rule provision, but more importantly, patient's privacy breeches were prevalent [4]. The survey also reveals that 52% of providers and 60% of health plans that claim compliance had experienced privacy breaches during the preceding six months [18] which indicates that there is ample opportunity for improvement in implementing the privacy regulations.

The privacy provisions that are difficult to implement vary based on the stakeholders. For health care providers, training their staff was selected as the most difficult task in implementing the privacy regulations (23%). This was followed by managing "accounting of disclosures" (22%) and maintaining "Business Associate Agreements" (15%). For health plans, maintaining the "minimum necessary" restriction was the most difficult (33%) followed by training the staff (23%) and managing "accounting of disclosures" (13%). Briefly, the "accounting of disclosures" refers to the obligation that individuals have a right to receive an accounting of disclosures of their PHI made by the covered entity during the past six years. The "minimum necessary" restriction states that covered entities must make reasonable efforts to limit information to a minimum to accomplish the intended purpose—a rule that is fraught with ambiguity and interpretation bias. The "business associate agreement" constitutes obtaining "satisfactory assurances" that they will protect the information—again, fraught with ambiguity and interpretation bias [18].

The HiMSS survey reveals that 22% of healthcare providers and 13% of health plans freely acknowledge their failure to comply with the privacy regulations with budgetary concerns and lack of enforcement as the two major reasons given for the non-compliance. Since the inception of the privacy regulations until 2006, 19,000 formal complaints had been filed with zero penalties assessed [18]. This lack of enforcement has contributed to organizational failures. The American Insurance Group (AIG) exposed 903,000 patient records when a server was stolen [4]. Empire Blue Cross and Blue Shield had a significant failure when a CD containing personal and medical information of 75,000 patients was lost. This information, initially trusted to the program administrator (Magellan Behavioral Health Services) was subcontracted to a third-party. The third party did not have to comply with the initial "Business Associate Agreement" to encrypt or password protect the data—a significant oversight by Empire Blue Cross and Blue Shield [19].

Lack of enforcement of HIPAA privacy rules may be changing in light of a $100,000 fine in July 2008 levied against Providence Health System for security lapses and a $2.5 million fine in February 2009 against the CVS pharmacy chain over potential HIPAA privacy violations [2].

Overwhelming organizational successes are difficult to assess. Based on the HiMSS survey, it is evident that the majority of covered entities view themselves as compliant organizations; however no health plan or provider was compliant with every key privacy rule provision [18]. Nonetheless, there are organizational successes. The Geisinger Health System was recognized by AIIM with the Industry Best Practices Award for HIPAA-compliant system [7].

The final HIPAA Privacy rule is actually a "disclosure regulation" as it actually provides far less privacy of patient data than the original regulation intended. Effective in April 2003, the federal government gave six hundred thousand "covered entities" — such as health care plans, clearing houses, and health management organizations "regulatory permission to use or disclose protected health information for treatment, payment, and health care operations" without patient consent [6]. This focus on disclosure versus privacy has resulted in an actual increase in patient information disclosures; most in the form of data breeches [15].

Many of the entities covered under HIPAA were making considerable progress in becoming compliant with the security rules. These security efforts may be fueled by a growing concern within the healthcare industry around the security risks and implementation of security protections to comply with organizational and regulatory compliance. Another major driver towards security compliance may include the influence of accrediting bodies such as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the National Committee for Quality Assurance (NCQA), and the increasing occurrence of security threats and incidents within government [18].

Cost of Compliance

One of the most controversial issues surrounding HIPAA has been the cost of compliance. For most healthcare organizations, large and small, meeting HIPAA requirements has consumed substantial amounts of time; both for healthcare professionals and patients. The research firm The Gartner Group has estimated that HIPAA is expected to cost the healthcare industry at least $3.8 billion between 2003 and 2008, and potentially even higher [11]. According to American Hospital Association funded research, hospitals have spent as much as $22 billion during the first five years to comply with applicable HIPAA laws. This same study estimated the average cost just to train an employee on HIPAA subject matter was $16 per employee [10]. Hospital budgeting to facilitate HIPAA requirements has been challenging with most organizations having spent

hundreds of thousands of dollars on initial compliance efforts resulting in little benefit and with no end in sight [12].

HIPAA also mandates that entities that provide health care must have someone designated as chief privacy officer and also requires a chief security officer. In smaller organizations this can be the same individual and it is not necessarily a full time position. However, in larger organization it usually is a full time position and hence the term "HIPAA Nazi" can be heard in some HIPAA compliant organizations.

Impact on Medical Research

A specific area of cost-concern as a result of sweeping HIPAA regulations has been the negative impact privacy and security rules have had on the research community. In a paper published in the Archives of Internal Medicine, researchers from the Cardiovascular Center (CVC) report how research on heart attack care has been hampered by the national medical privacy regulations under HIPAA. They report that the changes needed to comply with HIPAA have led to a drastic drop—from 96 percent to 34 percent—in the proportion of follow-up surveys completed after patients leave the hospital while costing $8,704.50 in the first year of a research project, and $4,558.50 per year after that to do HIPAA compliant surveys [15].

A survey of 1,527 epidemiology researchers found overwhelmingly that HIPAA had made research more difficult [16] and the Institute of Medicine in a February 2009 recommends numerous changes to the HIPAA privacy rules with respect to medical research [12].

Positive Aspects of HIPAA

Although most of the impact of HIPAA regulations on healthcare has been negative, there have been some positive results achieved. HIPAA regulations have brought higher level privacy and security issues to the forefront of most physician practices, Prior to HIPAA, privacy and security controls at the practice level were inadequate. Today many physician practices are implementing technology to help them facilitate HIPAA compliance as well as provide safer patient care; these systems provide multiple benefits to physician and patient alike [14].

An Example

Hospital Group X located in Southern New England is an administratively organized group of four hospitals is now fully compliant with all aspects of HIPAA. This was achieved after much time and effort and the expenditure of over $8 million dollars despite the fact that it is a leader in the use of information technology in the region [20]. Although this has provided Hospital Group X with greater levels of security and privacy; it has yet to benefit from the savings promised by the HIPAA promoters. The risk of protected health information disclosure has been minimized; infrastructures which govern and control the transmission of patient information have been strengthened and secured to maximize performance while maintaining security. Patient privacy and security are now part of the Hospital Group X culture which has increased patient confidence and trust as seen in the results of patient satisfaction surveys [20]. From a Hospital Group X perspective though, the question remains whether it was all worth it and how much more will need to be spent to maintain compliance.

CONCLUSIONS

HIPAA was presented as an example of how maintaining customer (patient) privacy which is both necessary and desirable is difficult to achieve while at the same time providing for the sharing of patient health care information and the sharing and synchronization of medical research knowledge. While such sharing is both laudable and necessary for patient health, the privacy portion of HIPAA in its present form has proven to be difficult and costly to implement for a variety of reasons and the recently enacted additional rules under the American Recovery and Investment Act scheduled to go into effect in February 2010 will only compound the problem. Organizations which have been able to become compliant have done so only after much effort and expense.

REFERENCES

1. Association of Physicians and Surgeons, Vol 57, No 6, June 2001. Retrieved April 12, 2009 from http://www.aapsonline. org/ news letters/june01.htm
2. Baumstein, A (2009). "Time to Get Serious About HIPAA," Retrieved April 1, 2009 from http://www.informationweek.com/news/show Article.jhtml?articleID=214600332
3. Beaver, K and H Rebecca (2003). "The practical guide to HIPAA privacy and security compliance", Chapter 3, (p. 23), Auerbach Publications, December 17, 2003. Retrieved April 4, 2009 from http://searchdata manage

ment.techtarget.com/tip/0,289483,sid91_gci1140016,00.html.
4. Carr, J (2007). Health care: Where are the penalties for failing to comply with HIPAA? Retrieved March 28, 2009 from http://www.scmagazineus.com/Health-care-Where-are-the-penalties-for-failing-to-comply-with-HIPAA/PrintArticle/34561/.
5. Doscher M. HIPAA: A Short- and Long-Term Perspective for Health Care. Chicago, Ill: American Medical Association Press; 2002:2-12, 68.
6. Gavin, K (2005), "HIPAA rule hikes cost of research", The University RECORD Online, University of Michigan, June 23, 2005. Retrieved April 12, 2009 from http://www.ur.umich.edu/0405/Jun13_05/11.shtml.
7. Geisinger Health System Recognized by AIIM with Industry Best Practice Award for HIPAA Compliant Solution. (2004). Retrieved April 4, 2009 from http://findarticles.com/p/articles/mi_m0EIN/is_2004_March_31/ai_114789075
8. Harris, S (2009). Red flag rules on identity theft take effect soon, Retrieved April 1, 2009 from http://www.ama-assn.org/ amednews/ 2009/03/30/bica0330.htm
9. Hartman, L. (2005) HIPAA: A Few Years later. Retrieved April 12, 2009 from http://nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Volume102005/No2May05/tpc27_216018.aspx?css=print
10. "HIPAA Privacy White Papers August 2004", SNIP Security and Privacy Workgroup, Workgroup for Electronic Data Interchange (WEDI), 2002-2004; Retrieved April 3, 2009 from http://www.wedi.org/snip/public/articles/2004-08005PrivacyOutline.pdf
11. Institute of Medicine of the National Academies (2009), Report Brief February 2009 Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Retrieved April 11, 2009 from http://www.iom.edu/CMS/3740/ 43729/61796/61836.aspx
12. Kilbridge, P MD (2003). "The Cost of HIPAA Compliance", The New England Journal of Medicine, Vol. 348:1423-1424 April 10, 2003, No. 15 (p. 1424).
13. Mortman, D. "HIPAA compliance: New regulations change the game," Retrieved April 14, 2009 from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1352102,00.html.
14. "Physicians Welcome Increased Role for the Internet", The Frabotta Company, 2000-2001, About.com: Mental Health; "Internet Use by Medical Groups" was conducted by Harris Interactive on behalf of the Health Technology Center (HealthTech) in cooperation with PricewaterhouseCoopers and the Institute for the Future. Retrieved April 4, 2009 from http://mentalhealth.about.com/library/sci/0301/blmdint301.htm.
15. Sobel, R (2007). "The HIPAA PARADOX: The Privacy Rule That's Not", Hastings Center Report 37, No. 4 July-August 2007: (p. 40-50). Retrieved April 7, 20090 from http://www.patientprivacyrights. org/site/ DocServer/HIPAA_Paradox.pdf?docID=1981.
16. Survey: HIPAA privacy rule slows scientific discovery and adds cost to research (2007), Retrieved March 25, 2009 from http://compliancehome.com/news/HIPAA/11735.html.
17. Thacker, S. (2003). HIPAA Privacy Rule and Public Health. Guidance from CDC and the U. S. Department of Health and Human Services. Retrieved April 4, 2009 from http://www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm
18. U. S. Healthcare Industry HIPAA Compliance Survey Results: Summer 2006 (2006) Retrieved March 24, 2009 from http://himss.org/content/files/SummerSurvey2006.pdf.
19. Washkuch, F. Update: CD with personal information of 75,000 Empire Blue Cross members found. (2007). Retrieved April 4, 2009 from http://www.scmagazineus.com/Update-CD-with-personal-information-of-75000-Empire-Blue-Cross-members-found/article/34755/
20. Unpublished paper submitted to the author as a class assignment, November 2007.