3 OKLA. J. L. & TECH. 37 (2007)
www.okjolt.org

Abstract:

Robert Bond Malone is currently pursuing a J.D. at The University of Oklahoma College of Law as part of the Class of 2007. Below, Mr. Malone expands upon his previous publication, *Health Information Technology: Transforming the Healthcare Industry for the 21st Century*, in which he considered the effects such technology could have on the problems currently plaguing the industry. Refer to 3 Okla. J.L. & Tech. 36 for a full copy of *Health Information Technology*. Here, Mr. Malone considers whether this technology can co-exist with HIPAA and its concerns regarding privacy over sensitive health records. Mr. Malone concludes that the benefits of Health Information Technology outweigh any risks related to HIPAA, and that the technology could in fact aid HIPAA through better enforcement of its provisions.

HEALTH INFORMATION TECHNOLOGY AND HIPAA: CAN WE SATISFY SECURITY AND PRIVACY STANDARDS IN THE DIGITAL AGE?

I. Introduction

Health Information Technology (HIT), which the government hopes will create a unified system of medical histories and information to facilitate physicians in their handling of patients, has tremendous potential to revolutionize the healthcare industry. However, it is also fraught with the potential for fraud and abuse. Given the sensitive nature of the information involved, concerns about privacy and security breaches loom large.

In the second of this three part series about HIT, public concerns about how the Health Insurance Portability and Accountability Act (HIPAA) can be adapted to allow for HIT will be discussed, as well as the steps the government has taken to allow for the benefits of HIT without compromising the privacy and safety standards of HIPAA.

II. HIPAA: Background Information

HIPAA is a 1996 federal statute designed to address issues relating to how patients interface with the health care system.[1] Like its name would suggest, it ensures insurance portability and increases accountability for fraud and abuse.[2] It also requires all health plans and health care providers that transmit health information in an electronic form to implement very important and expensive computer systems and business methods.[3] It is these latter purposes that are most relevant to a discussion about HIT, and it is for these reasons HIT cannot be fully realized without first complying with HIPAA.

By the same token, HIPAA cannot be fully implemented without HIT. As a practical matter, the only real way to fully comply with HIPAA's privacy and security requirements is to employ encryption systems for transmission of personally identifiable electronic health records (EHR's).[4] It can therefore be argued that the primary purpose of HIPAA is to improve healthcare providers' ability to use and protect personally identifiable health care information, a goal which requires the use of HIT.[5]

The standards set by HIPAA correlate closely with the goals of HIT. HIPAA contains sets of requirements relating to the standardization, privacy, and security of health information transmitted electronically.[6] Also, HIPAA requires that the Secretary of the Department of Health and Human Services facilitate the efficiencies and cost savings that the increased use of electronic technology affords the health care industry by creating standards for health plans and health care providers who employ electronic

[1] Brenda T. Strama et al., Vinson & Elkins Symposium: Overview of HIPAA Security and Privacy Standards 2 (Apr. 26, 2000).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id. at 3.*
[6] *Id.*

health records.[7] Generally speaking, the United States Code section dealing with adoption of standards for health and welfare states that "any standard adopted … shall be consistent with the objective of reducing the administrative costs of providing and paying for health care."[8] These objectives mirror the goals of HIT set out by current Secretary of Health and Human Services Michael Leavitt in the first part of this series.

However, where HIPAA has the biggest impact on the process of implementing HIT is the second task required of the Secretary under HIPAA. That task, which is again arguably the primary purpose of HIPAA, is to develop standards to protect the security, confidentiality and integrity of this electronic health information.[9] It is this benchmark of security that HIPAA sets out that poses the biggest threat to the widespread adoption of HIT in the health care industry.

HIPAA's security standards and the risks to those standards posed by HIT is the focus of this brief.

III. HIPAA Security Standards

As mentioned, a cursory glance at HIPAA security standards shows that the HIT initiatives mentioned in the first brief in this series seem tailor made to facilitate the goals of HIPAA. To recap, the goals of HIT include lower overall health care costs, fewer medical errors, and general improvement in the quality of health care available. To this end, on August 12, 1998, the Department of Health and Human services issued a proposed rule that went a long way towards establishing security standards for health

[7] *Id.*
[8] 42 U.S.C. § 1320d-1(b) (2000).
[9] *See* Strama et al, *supra* note 1.

information maintained or transmitted in electronic form.[10] This federal regulation set out security standards that required affected entities to establish and maintain reasonable safeguards to guarantee both confidentiality and availability of health record information.[11] It is these twin aims of confidentiality and availability that HIT and HIPAA combine to strive for that will revolutionize the healthcare industry.

The security standards laid out in the above federal regulation establish "a national standard for protecting the security and integrity of medical records when they are kept in electronic form."[12] For this reason, HIPAA security standards will require significant systems implementation by healthcare providers.[13] The security standards were intended to protect sensitive health information against possible threats which could violate the integrity of such information, as well as protect the information from unauthorized disclosure or usage.[14] Implementation requirements related to HIPAA must be included to assure the security of electronic health information.[15] There is also a provision requiring healthcare providers to assess their own security needs and maintain appropriate security to address their own requirements.[16]

It is with regard to this last part that the goals of the proposed HIT initiatives mentioned in the first brief in this series could really benefit HIPAA. I feel that requiring healthcare providers to assess their own security needs and maintain security appropriate for their own requirements is a losing proposition. One of the main objectives of HIT is a

[10] Security and Electronic Signature Standards, 63 Fed. Reg. 43242 (proposed Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142).
[11] *Id.*
[12] *Id.*
[13] *See* Strama et al, *supra* note 1.
[14] *Id at 4.*
[15] *Id.*
[16] *Id.*

standardized system that is open, adaptable, and most importantly, interoperable. Having a unified system facilitates the efficient and secure exchanging of health information. If the Department of Health and Human Services can succeed in establishing a uniform system of electronic health records, everyone's sense of security will increase and the HIPAA goal of improved security standards to better protect an individual's legal right to security with regard to sensitive health information can be reached. I find it impossible to achieve this goal without Health Information Technology.

IV. HIPAA Privacy Standards

Under section 264 of HIPAA, the Department of Health and Human Services was ordered to develop suggestions to Congress for: "(1) the rights that individuals should have with respect to their own identifiable health information, (2) the procedures that should be used to exercise those rights, and (3) which uses and disclosure of that information should be authorized."[17] To meet these goals, the Department issued a proposed rule which established standards for individual privacy of identifiable health information.[18] The Department's regulation acknowledges the importance of confronting the issue of privacy with regard to HIT when they say: "The same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable."[19]

[17] Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,921 (Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160-164).

[18] *Id. at 59,918.*

[19] *Id. at 59,922.*

In issuing this rule, the Department expressed disappointment that HIPAA legislative authority is more limited in scope than its proposal, and there was concern that HIPAA lacked a private right of action for those whose privacy rights are violated.[20]

To better meet the privacy requirements necessitated by an electronic health record system, the Department of Health and Human Services made this rule, which applies to health information that is transmitted electronically.[21] All health information that can be individually identifiable is covered by the rule and given privacy protection.[22] The privacy standards set out by HIPAA and the Federal Regulation submitted by the Department require significant commitment by healthcare providers, and implementation of the privacy standards will require extensive preparation. This is where HIT comes in to facilitate the privacy standards which HIPAA aspires to achieve.

I believe that HIT can bridge the gap between the goal of privacy of health information laid out by HIPAA and the enormous cost and effort to implement those privacy standards. Legal issues surrounding the privacy of health information in electronic form can be conquered by a unified, interoperable and reliable HIT initiative that both protects individuals and reduces costs to individual healthcare providers.

V. Actions Underway To Reconcile HIPAA Fears With HIT

Of course, what it all comes down to is alleviating the fears of patients whose medical histories are to be so readily accessible through the use of electronic health records. The success of HIT ultimately depends on the public's acceptance of electronic health records as a sufficiently secure method of transmitting very sensitive and private

[20] *Id at 59,923.*
[21] *Id at 59,924, 59,927.*
[22] *Id at 59,936.*

information. HIPAA was designed to protect such information, and for HIT to achieve its full potential, the public must believe that HIPAA's principles will not be compromised.

Following the second HIT summit, held in Washington, D.C. on September 8, 2005, Dr. Alan F. Westin, Professor of Public Law and Government Emeritus at Columbia University and the Director of the Program on Information Technology, Health Records and Privacy, conducted a public opinion survey. In this survey he asked what the public thought about the administration of HIPAA in the face of emerging medical technology. The results plainly show the fears most people have about electronic health records. Respondents felt that health information, along with financial records, is the most sensitive information about a person and deserves the greatest protection.[23] Concerns about data security are high, given past incidents of identity theft which have plagued consumers in recent years.[24] Generally, the public is ambivalent about computer effects on privacy, but there appears to be strong public support for federal health privacy legislation and a desire to see the Department of Health and Human Services issue a strong privacy rule.[25]

One encouraging statistic from the poll is that most respondents feel that HIT will accomplish the objectives mentioned in the first brief in this series.[26] A majority of those polled felt that HIT can decrease the frequency of medical errors significantly, reduce

[23] Dr. Alan F. Westin, Slide Presentation: Public Attitudes Towards Privacy in HIPAA and HIT Programs (Sept. 8, 2005)*, available at* http://www.ehcca.com/presentations/hitsummit2/westin.pdf.
[24] *Id.*
[25] *Id.*
[26] *Id.*

healthcare costs and improve patient care, all of which are important goals.[27] However, a similar majority also felt that "the use of Electronic Medical Records makes it more difficult to ensure patients' privacy."[28] Concerns listed include fears that: Sensitive health data may be leaked, there may be inadequate data security, and HIPAA privacy rules will be reduced in the name of efficiency.[29] All of these fears are related to HIPAA, and could prevent HIT from becoming what the Department of Health and Human Services hopes will revolutionize the healthcare industry.

In order to overcome these fears, the Department has listed a series of "breakthroughs" that would shift public opinion in favor of widespread health information technology adoption. In Dr. Westin's survey, more than eight out of ten respondents rated "consumer empowerment" as important.[30] Allowing the electronic medical record system to arrange ways for consumers to track their own personal information and exercise privacy rights personally carried a lot of favor.[31] In response to information such as this, the Department lists "Consumer Empowerment" on its website's October 7, 2005 update as its first "breakthrough."[32] The Department names programs with titles like "My Personal Health Record" and "My Medical History" which it believes will help individuals manage their health care personally and decide for themselves when it comes to health care services.[33] Because most people are not experts in the medical field, and therefore are not aware of the specific medications and dosages they have been

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Office of the Nat'l Coordinator for Health Info. Tech. (ONCHIT), American Health Information Community, http://www.hhs.gov./healthit/ahic.html, *(last visited Oct. 7, 2005).*
[33] *Id.*

prescribed or the results of their past medical tests, these HIT programs will provide all current, salient information to be stored in one location.[34] This information would be available to both the individual and authorized healthcare providers.[35]

Ideas such as these demonstrate not only the benefits of HIT to the public, but also how HIT can be used not as a detriment to HIPAA security and privacy standards, but as an aid. Empowering consumers to be able to research their own medical history instead of relying on others increases privacy. Giving the public the right to make their own informed healthcare decisions is an important step towards bridging the gap between fears of HIPAA violations and the needed efficiencies of HIT.

VI. Conclusion

Health Information Technology decreases the frequency of medical errors, reduces healthcare costs and improves patient care, all of which are important for the future of the healthcare industry. These benefits outweigh any potential risks to HIPAA. However, that's not to say privacy and security standards established by HIPAA are not placed at risk through the use of electronic health records. I believe that empowering consumers to make their own healthcare decisions through the use of HIT will both ingratiate the technology to individuals and also help maintain the privacy and security benchmarks set in place by HIPAA.

[34] *Id.*
[35] *Id.*