

United States Regulatory Updates: The American Recovery and Reinvestment Act

Katheryn A. Andresen

Copyright © 2011

All Rights Reserved

Biographical Information

Title: Ms.

Name: Katheryn A. Andresen

Position or Title: Partner

Firm or Place of Business: Hellmuth & Johnson, PLLC

Address: 8050 West 78th Street, Edina, Minnesota 55439

Phone: 952-941-4005

Fax: 952-941-2337

E-Mail: kandresen@hjlawfirm.com

Primary Areas of Practice: Complex transactions, primarily in information technology and ecommerce law

Education: J.D. University of Minnesota Law School,
Certificate, Advanced International Law Studies
M.A. Boston University – International Relations

Recognition: Strathmore's Who's Who
Minnesota Lawyers Rising Star

Publications: Katheryn A. Andresen, THE LAW AND BUSINESS OF COMPUTER SOFTWARE (Thomson – West, 2007-2011); and
Katheryn A. Andresen, *Chapter 13 – Privacy Torts* in MINNESOTA BUSINESS TORTS DESKBOOK (Minnesota CLE 2008 – 2011)

Memberships: American Bar Association (Business Law Section and Cyber Law Committee); Minnesota State Bar Association (Computer Law Section, former Chair); International Law Technology Association; and Health Information and Management Systems Society.

**United States Regulatory Updates:
The American Recovery and Reinvestment Act¹**

INTRODUCTION

Health information technology creates both benefits and risk for all parties concerned. For example, the healthcare provider gains by efficiencies in technological processing, but is subject to technology development and maintenance costs and the inherent security risk of systems. The individual patient, also benefits from easier access and transferability of records, but is also at greater risk of losing his/her privacy rights if the data is so easily transmitted into or out of the system. The technology provider also benefits from a marketplace for its products, but it has increased security obligations due to the sensitive nature of the data. In the development of new technologies in the 1980's and 1990's, technology providers, or in some cases the healthcare providers through custom applications, developed unique data elements in a variety of technologies and computer coding languages. During this timeframe, the healthcare providers typically considered the data created to be owned by them. The technology provider typically created unique datasets and coding to incent the healthcare provider to maintain the system since the transition to another provider would be neither easy nor cost-effective. The individual generally had no say in the content or use of the data.

In the United States, the issues with interoperability, portability and privacy protections were addressed with the implementation of regulations issued under the Health Information Portability and Accountability Act ("HIPAA") of 1996. This was subsequently expanded to address obligations by business associates under the Health Information for Economic and Clinical Health Act ("HITECH Act") of 2009 part of the American Recovery and Reinvestment Act ("ARRA"). In the last two years, additional regulations have been passed to address the implementation of technology incentives for the adoption of meaningful use technologies by healthcare providers under the Medicare and Medicaid programs under ARRA.

HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT

In 1996, when the United States Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA),² the primary goal for the act was to protect the right of an individual to ensure health care coverage was portable between jobs. As noted in the purpose section of HIPAA, the Act was to "improve... the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."³ The law required the United States Congress enact privacy legislation in three years, or the Secretary of Health and Human Services was required to issue privacy regulations. In 1999, the Secretary issued a proposed rule and after public comments, the final Privacy Rule was issued in December 2000.⁴ The Privacy Rule was subsequently modified in 2002 after additional public comments.⁵ The following year, the related Security Rule was issued.⁶

An additional motive for HIPAA was administrative simplification with regards to the standards for electronic health records and the ability for an individual to ensure that his/her individually identifiable information was protected. The promotion of national standards for electronic health records had a fairly

¹ Ms. Katheryn ("Kate") A. Andresen is partner with the law firm of Hellmuth & Johnson, PLLC. Ms. Andresen is an experienced transactional attorney, with an emphasis in technology and intellectual property considerations. She is a frequent author and guest speaker on technology law related matters, both nationally and internationally. Ms. Andresen authored the second edition of *THE LAW AND BUSINESS OF COMPUTER SOFTWARE* (West Services, Inc., 2007-2011).

² Pub. L. 104-191.

³ Id. at Section F, § 261.

⁴ 65 FR 82462.

⁵ 45 CFR §§ 160.102, 160.103; See also § 164, Subparts A and E.

⁶ 68 FR 8334.

significant business impact on both healthcare providers, as well as those companies that provide health care systems. In 2000, the Office of the Secretary of Health and Human Services issued standards for eight electronic transactions and for code sets.⁷ As part of the background to this standards development, the Secretary clarified that:

“Electronic data interchange (EDI) is the electronic transfer of information, such as electronic media health claims, in a standard format between trading partners. EDI allows entities within the health care system to exchange medical, billing, and other information and to process transactions in a manner which is fast and cost effective.”⁸

The standards and the code sets developed were intended to ensure that an electronic health record (“EHR”) could be transmitted through an EDI to administratively simplify the healthcare process. As the EHR could contain individually identifiable information or “protected health information” (“PHI”) or its electronic counterpart (“E PHI”), these PHI in the standardized records had to be protected under the Privacy Rule and the electronic data had to be secured under the Security Rule.

The administrative benefits associated with HIPAA, were combined with individual protections as to privacy and an obligation for covered entities (i.e. those entities subject to the regulation like healthcare providers or clearinghouses) to secure PHI. The standards developed were expected to ease the transition of data exchange between a healthcare provider and the insurance company or claims processor which would process or pay for the claim. An additional impact of the standards implementation was that the various third party systems, which were used under license by healthcare providers, could be obligated to pass EHR or other data through to a competitive system.⁹ In response to a question on whether a standard had to be implemented that was not currently used, the Secretary stated:

“[W]hile we interpret HIPAA to mean that a health plan cannot refuse to conduct a transaction because it is a standard transaction, we do not believe that use of standard transactions can create a relationship or liability that does not exist. For example, a health plan cannot refuse to accept a claim from a health care provider because the health care provider electronically submits the standard transaction. However, the health plan is not required to pay the claim merely because the health care provider submitted it in standard format, if other business reasons exist for denying the claim (for example, the service for which the claim is being submitted is not covered).”¹⁰

In the comments and response section of the Federal Register regarding the final rule, the Secretary clarified that while not all technologies had to be standard (e.g., HTML interactions), the data content would have to be standard.¹¹

The Privacy Rule was issued by the Secretary to ensure that an individual’s privacy with regards to PHI was maintained, notwithstanding the standardization of the data and the ease of transmission through an EDI to administer healthcare claims processing. In particular, the Secretary acknowledged the complexity of implementing a Privacy regulation as there were competing interests between protections and the benefits and appropriateness of “use” of PHI, as well as a wide disparity between solo practitioners to multi-national health plans.¹² The Privacy Rule was intended to be a new baseline standard, not to preempt stronger privacy protections:

“It is important to understand this regulation as a new federal floor of privacy protections that does not disturb more protective rules or practices. Nor do we intend this regulation to describe a set of

⁷ 45 CFR §§ 160 and 162.

⁸ Id. at I.A.

⁹ Federal Register, Vol. 65, No. 160, p. 50315.

¹⁰ Id.

¹¹ Id.

¹² Federal Register, Vol. 65, No. 250, p. 82471.

a “best practices.” Rather, this regulation describes a set of basic consumer protections and a series of regulatory permissions for use and disclosure of health information. The protections are a mandatory floor, which other governments and any covered entity may exceed.”¹³

In particular, the Privacy Rule created the following standards: (i) uses of PHI not requiring consent (i.e. standard operations such as claims processing); (ii) uses of PHI requiring authorization (e.g. marketing or sharing with affiliate); (iii) uses or disclosures requiring an opportunity to object or agree and (iv) uses no longer deemed PHI (i.e. de-identification and statistical aggregation).¹⁴ The other components required the development of a Notice of Privacy Practices, the ability for an individual to review and request corrections to PHI, and obligations related to breaches of PHI.

As noted in the comments and responses section of the Federal Register publication of the Security Rule, the Secretary recognized that it was unreasonable to expect the same security measures to be taken by a solo practitioner which would be required by a multi-national health plan.¹⁵ The final Security Rule essentially identified a buffet of security options from which each covered entity could select those components appropriate and reasonable for such covered entity to implement based on scale of the system, control risks and the level of PHI stored or transmitted. In particular, the Security Rule focused on three types of security measures: (i) administrative; (ii) physical; and (iii) technical.¹⁶ The administrative shifted the responsibility of compliance to a covered entity’s management to ensure the covered entity appropriately developed security policies, implemented and verified compliance to such policies. The physical safeguards included restricting access to networks and facilities housing networks to those persons authorized. The technical safeguards are the typical array of industry standards for data protection: secure-socket-layer (“SSL”) transmission, encryption, user ID and password restrictions, etc.

Probably the most expensive element to implement for covered entities under HIPAA has been compliance with the breach notification rule for the privacy protections under the Privacy Rule.¹⁷ In the 2010 study issued in March 2011, the Ponemon researchers found “the average organizational cost for a data breach increased to \$7.2 million...”¹⁸ This is based on an average of \$214 per compromised record.¹⁹ The Secretary of Health and Human Services also requires a covered entity to report breaches of PHI under the Privacy Rule; breaches affecting 500 or more individuals are reported to the Secretary within 60 days of the breach (and are then kept in a database by the Secretary on the Health and Human Services website) and smaller breaches are reported in an annual report to the Secretary. The majority of the costs associated with these breaches were associated with lost revenue as those affected changed providers.²⁰

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

In 2009, the United States Congress implemented the American Recovery and Reinvestment Act which included a significant amendment to HIPAA under Title XIII the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”). The HITECH Act in large part extended the obligation to protect the privacy of secure data and report data breaches down to the sub-contractor level for a covered entity (i.e. a business associate). The shift of direct liability (both civil and criminal) to a business associate was intended to ensure all parties hosting, transmitting or storing PHI would be responsible for its privacy protection and other security protections.²¹ Although the business associate was contractually liable for its failure to secure the privacy of PHI under a business associate agreement, the HITECH Act

¹³ Id.

¹⁴ 45 C.F.R. § 164.

¹⁵ Federal Register, Vol. 65, No. 250, p. 82471.

¹⁶ Federal Register, Vol. 68, No. 34, p. 8376.

¹⁷ The 2010 Annual Study: U.S. Cost of a Data Breach by Ponemon, LLC sponsored by Symantec Corporation which may be found online at Symantec’s website: www.symantec.com.

¹⁸ Id. at p. 5.

¹⁹ Id.

²⁰ Id. at p. 6.

²¹ Federal Register, Vol. 74, No. 209, p. 56124.

codified this liability and extended the civil and criminal penalties associated with the covered entity to the business associate as well.

As a result of this direct regulation of the business associates, most covered entities now directly obligate such business associates to assume responsibility for costs associated with breaches. In particular, a business associate agreement may obligate the business associate to indemnify the covered entity for breaches due in whole or in part to a business associates actions or omissions. The definition typically ensures the business associate is responsible not only for its own employees, but also for any agents or sub-contractors as well. The business associate may try to limit this liability to breaches due solely to the business associate's negligent acts. The business associate agreement also needs to accurately reflect the reporting obligation as to breaches as both the covered entity and the business associate could now be found liable for failure to comply with the Secretary's regulations as to breach notification.

THE HITECH ACT MEANINGFUL USE CERTIFICATION INCENTIVE PROGRAM

One of the more positive impacts of the HITECH Act was its promotion of the adoption and meaningful use of healthcare technology.²² To incent covered entities in adopting such technologies, the HITECH Act was funded by a \$2,000,000,000 incentive program for which certified adopters of "meaningful use" technologies associated with Medicare and Medicaid services could receive incentive payments. Even large healthcare providers already using technology would be permitted to apply for incentive funds provided that the technology complied with the "meaningful use" standard and the provider was certified under the Certification Program for Health Information Technology.²³ There was a temporary certification program established under 45 CFR § 170, Subpart D which sunsets at the end of 2011. This was replaced with the final certification program as of January 2011.²⁴

The Certification Program for the adoption of meaningful use technologies has attempted to address both the business concerns of what is required and how to validate compliance, with the technology providers concerns of how to attain compliance verification and certification of specific EHR modules. For example, during the comment phase of the temporary certification program, the Secretary received numerous comments as to the need for healthcare providers to have a single source of verification as to whether a particular EHR module complied with the Certification Program's meaningful use requirement. The Secretary's response was to consent to maintain the Certified Health Information Technology Products List which would specify down to the version number, which provider and EHR module was certified to comply.²⁵ Each certified product would be assigned a unique identifier which the healthcare provider could then use to validate compliance for attestation purposes.²⁶ On the other hand, the Secretary did not mandate that each EHR-module integrate with any other EHR-module, "primarily because of the impracticalities pointed out by commenters (*sic*) related to the numerous combinations of EHR Modules that will likely exist and the associated technical, logistical, and financial costs of determining EHR Module-to-EHR Module integration."²⁷

In regulating the Certification Program, the Secretary was able to create not only standards for health information technology which was intended to improve the Medicare and Medicaid programs, but was also able to develop a framework in which the standards could be measured, certified and monitored. The National Institute of Standards and Technology accredits the organizations to test health information technology, in particular EHR technology. The Office of the National Coordinator ("ONC") approves the test tools and procedures to test EHR modules for certification. One organization will be named as the approved accreditor ("ONC-AA") every three years on a competitive basis. Each authorized certification

²² *Id.*

²³ See Secretary's website for health information technology and its certification programs at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_home/1204.

²⁴ Federal Register, Vol. 76, No. 5, p. 1262.

²⁵ *Id.* at p. 1277.

²⁶ *Id.* at pp. 1277-1278.

²⁷ *Id.* at p. 1273.

body (“ONC-ACB”), even those certified under the Temporary Certification Program (“ONC-ATCB”), will need to renew its status every three years.²⁸

The Centers for Medicare & Medicaid Services noted that expanding the meaningful use of certified EHR technology is “one piece of a broader Health Information Technology infrastructure needed to reform the health care system and improve health care quality, efficiency, and patient safety.”²⁹ The implementation of meaningful use is in stages. “The Stage 1 criteria for meaningful use focus on electronically capturing health information in a coded format, using that information to track key clinical conditions, communicating that information for care coordination purposes, and initiating the reporting of clinical quality measures and public health information.”³⁰ Stage 1 began in 2011 and includes 24-25 objectives/measures for eligible hospitals and eligible providers respectively. These measures are broken into core measures and they have the option to defer up to 5 remaining objectives/measures. Where it is impossible for an eligible provider or hospital to meet a specific measure, the eligible provider or hospital may be exempt for such measure. In order to “demonstrate Meaningful Use [the eligible provider, hospital or critical access hospital] are required to submit aggregate clinical quality measure numerator, denominator, and exclusion data” to the Centers for Medicare & Medicaid Services by attestation.³¹ By 2012, this data must be submitted through certified EHR technology.

CONCLUSION

The Certification Program is one step in promoting the concept of unified standards for health information technologies. The initial funding was based on federal incentives to standardize and promote efficiencies for the federal Medicare and Medicaid programs. The underlying motivation for implementing HIPAA, as subsequently modified by the HITECH Act was also the creation and implementation of standards for health information technologies. While most individuals associate HIPAA with an individual’s right to protect his/her privacy with respect to PHI, the legislative history and President Clinton’s remarks upon his signing it into law were the concept of standardization. The technology was intended to improve accuracy, time and other administrative simplification of our healthcare system. In particular, the individual would be able to easily port his/her related EHR from one provider to the next based on the standards. All of the standardization was intended to incent the use of technologies and EHR. While the effect of the Privacy Rule and the Security Rule may have been a financial and technical burden on covered entities, the long-term benefits of consistency and simplicity were expected to offset such upfront costs. Under ARRA, the United States decided to further incent the adoption of these standardized technologies through its Certification Program and the related incentives payments.

²⁸ See Secretary’s website for health information technology and frequently asked questions on the certification program.

²⁹ See the Centers for Medicare & Medicaid Services Fact Sheet on Meaningful Use on the CMS website at www.cms.gov.

³⁰ Id.

³¹ Id.