eHealth: Where Are We Now?

Jennifer L. Rangel
Locke Lord LLP
600 Congress Avenue, Suite 2200
Austin, Texas 78701

I. HIPAA Update

In recent years, the scope of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and implementing regulations have expanded dramatically, presenting new privacy and information security challenges to certain types of businesses operating within the technology and healthcare industries. Not only does HIPAA present significant administrative responsibility for organizations regulated by HIPAA, but failure to implement the necessary safeguards to ensure HIPAA compliance can result in federal investigation and costly penalties.

Following passage of HIPAA, the U.S. Department of Health and Human Services (HHS) issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Security Standards (the Security Rule), and the HIPAA Enforcement Rule.[1] The intent of these regulations was and is to protect the privacy of individually identifiable health information that is maintained or transmitted in any form, whether electronic or not, and that relates to: (1) a past, present, or future physical or mental health condition; (2) provision of health care; or (3) past, present, or future payment for the provision of health care to an individual.[2] With some limited exceptions, this information is generally categorized as "protected health information" or "PHI."[3]

The Privacy Rule sets forth extensive regulations intended to protect individuals' PHI by requiring implementation of appropriate safeguards to ensure the privacy of PHI and regulating the uses and disclosures of PHI. The Privacy Rule also outlines specific rights that individuals have with respect to access, amendment, and communication relating to their PHI. The Security Rule sets forth technical and non-technical safeguards that HIPAA-subject entities must follow to secure individuals' "electronic protected health information," defined as any PHI produced, saved, transferred or received in an electronic form by covered entities or business associates.[4] According to the HHS, "a major goal of the Security Rule is to protect the privacy of individuals' health information while allowing HIPAA-subject entities to adopt new technologies to improve the quality and efficiency of patient care."[5]

On February 17, 2009, the Health Information Technology or Economic and Clinical Health Act, under Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, (HITECH Act) was signed into law and contained numerous provisions affecting the privacy and security of PHI. The final rule implementing most amendments mandated by the HITECH Act was issued on January 25, 2013 (the Omnibus Final Rule).[6] In addition to changes to the Privacy and Security Rules, the Omnibus Final Rule updated the penalty structure and enforcement scheme of HIPAA's Enforcement Rule and finalized breach notification

---

[1] 42 U.S.C. § 201 *et seq.* (HIPAA), 45 C.F.R. Part 160 and Subparts A and E of Part 164 (Privacy Rule); 45 C.F.R. Parts 160 and 164 subparts A and C (the "Security Rule"); 45 C.F.R. Part 160, Subparts C, D, and E (the "Enforcement Rule").
[2] 45 C.F.R. § 160.103.
[3] *Id.*
[4] 45 C.F.R. §§ 160.103; 164.302.
[5] U.S. Dept. of Health and Human Servs., *Security Law Summary of the HIPAA Security Rule*, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (last visited Apr. 24, 2016).
[6] 78 Fed. Reg. 5566 (Jan. 25, 2013).

requirements established by the HITECH Act (the HIPAA Breach Notification Rule).[7] The changes adopted through the Omnibus Final Rule are now in effect.

HIPAA and its implementing regulations apply to health plans, healthcare clearinghouses, and healthcare providers who engage in electronic data interchange using one or more of the "standard transactions," as defined by HIPAA regulations governing electronic data interchange (referred to as covered entities).[8] Pursuant to the HITECH Act and Final Omnibus Rule, "business associates" who perform functions or activities on behalf of covered entities and create, maintain, receive or transmit PHI in relation to such functions or activities are now directly regulated by the Security Rule and parts of the Privacy Rule.[9] HHS clarified in the Preamble to its Omnibus Final Rule that business associates include those who only maintain PHI on behalf of a covered entity, even if the entity does not view the PHI.[10] Consequently, cloud service providers and other software that store data for covered entities may be subject to HIPAA as a business associate.

A. *What Is a "Business Associate" Under HIPAA?*

In recent years, the definition of a "business associate" has expanded to clearly include businesses that, prior to passage of HITECH and the Final Omnibus Rule, took the position that they were not business associates. HIPAA currently defines a "business associate" as person or entity that:

> (i) On behalf of such covered entity…performs, or assists in the performance of:
>
> > (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
> >
> > (B) Any other function or activity regulated by this subchapter; or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.[11]

[7] 45 C.F.R. Part 164 subpart D (the "Breach Notification Rule").
[8] 45 C.F.R. § 160.103.
[9] *Id.*
[10] 78 Fed. Reg. 5572 (Jan. 25, 2013).
[11] 45 C.F.R. § 106.103.

UT LAW CLE THE UNIVERSITY OF TEXAS TEXASLAW

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the UT Law CLE eLibrary (utcle.org/elibrary)

Title search: eHealth: Where Are We Now?

Also available as part of the eCourse
2016 Technology Law eConference

First appeared as part of the conference materials for the
29th Annual Technology Law Conference session
"eHealth: Where Are We Now?"