Illinois Association of Defense Trial Counsel
Springfield, Illinois | www.iadtc.org | 800-232-0169
IDC Quarterly | Volume 23, Number 3 (23.3.11)

Health Law Update

By: Roger R. Clayton, Gregory J. Rastatter, and J. Matthew Thompson
Heyl, Royster, Voelker & Allen, P.C., Peoria

HHS Releases HIPAA Final Rule to Implement Statutory Amendments under HITECH Act and GINA

On January 25, 2013, the United States Department of Health and Human Services (HHS) issued its final rule ("Final Rule"), 78 Fed. Reg. 5566 (Jan. 25, 2013), to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 115, and the Genetic Information Non-Discrimination Act of 2008 ("GINA"), Pub. L. No. 110-233, 122 Stat. 881. In the Final Rule, HHS seeks to finalize the modifications to the Privacy, Security and Enforcement Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936, modify the HIPAA Breach Notification Rule, and finalize the modifications to certain sections of the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Subparts A and E of Part 164, to strengthen privacy protections for genetic information. This column describes several of the key provisions implemented by the Final Rule, but practitioners should be aware that it does not provide an exhaustive list of all the provisions. The effective date of the Final Rule was March 26, 2013, and covered entities and business associates of all sizes have until September 23, 2013 (180 days) to come into compliance.

Modifications to Privacy, Security, and Enforcement Rules

1. Direct Applicability to Business Associates

The Final Rule implements changes to Section 164.500 and 164.502 of the HIPAA Privacy Rule, 45 C.F.R. §§ 164.500; 164.502, which previously limited the enforcement of HIPAA's rules to covered entities. The HITECH Act established direct liability for impermissible uses and disclosures of protected health information by a business associate of a covered entity "that obtains or creates" protected health information "pursuant to a written contract or other arrangements," and for compliance with other privacy provisions in the HITECH Act. 42 U.S.C. § 17934. Under the Final Rule, a business associate is *directly liable* under the Privacy Rule for uses and disclosures of protected health information that are not in accord with its business associate agreement or the Privacy Rule. 45 C.F.R. § 164.502(a)(3). Direct liability also may be imposed upon a business associate for failing to disclose protected health information to a covered entity, an individual, or an individual's designee, as necessary to satisfy the covered entity's obligations with respect to an individual's request for an electronic copy of protected health information. *Id.* § 164.502(a)(4). Further, a business associate is directly liable for failing to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *Id.* § 164.502(b).

2. Definition of "Marketing"

The Privacy Rule requires covered entities to obtain valid authorization from individuals before using or disclosing protected health information to market a product or service to them. 45 C.F.R. § 164.508(a)(3). Section 164.501 of the Privacy Rule defines "marketing" as "mak[ing] a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." *Id.* § 164.501. The Privacy Rule contains exceptions for "treatment" or "health care operations" communications, and a concern arose that the exceptions allowed a third party to pay a covered entity to send health-related communications to an individual about the third party's products or services. See 42 U.S.C. § 300jj-12(b)(2)(B)(iv). The Final Rule clarifies that the exceptions are intended to curtail a covered entity's ability to use the exceptions to the definition of "marketing" to send communications to an individual that are motivated more by commercial gain than for the purpose of the individual's health care, despite the communication being about health-related products or services. Under the Final Rule, an authorization from the patient is required for *all* treatment and health care operations communications where the covered entity receives financial remuneration, directly or indirectly, for making the communications from a third party whose product or service is being marketed. 45 C.F.R. § 164.501.

3. Notice of Privacy Practices

The Final Rule requires certain modifications to the notice of privacy practices required under the Privacy Rule. Covered entities must edit and distribute a new notice containing additional disclosures, including a description of the uses and disclosures of protected health information that require an authorization under Sections 164.508(a)(2) through (a)(4), 45 C.F.R. §§ 164.508(a)(2)-(a)(4), (psychotherapy notes, and marketing and sales of protected health information). 45 C.F.R. § 164.520(b)(1)(ii)(E). Further, if a covered entity intends to contact the individual for fundraising purposes, that contact must be disclosed, along with a statement that the individual may opt out of those communications. *Id.* § 164.520(b)(1)(iii)(A). Finally, the notice must include a statement that individuals have a right to be notified following a breach of unsecured protected health information. *Id.* § 164.520(b)(1)(v)(A).

4. Access of Individuals to Protected Health Information

Section 164.524 of the Privacy Rule already requires covered entities to provide a copy of an individual's protected health information to the individual upon request. The Final Rule expands this obligation by requiring the covered entity to provide a copy in electronic form if the covered entity does in fact maintain an electronic copy. 45 C.F.R. § 164.524(c)(2)(ii); 78 Fed. Reg. 5566. According to the comments, the covered entity is expected to provide the copy in a "machine readable" format, such as Word, Excel, text, HTML, or text-based PDF documents. 78 Fed. Reg. 5566-01 cmt.

Breach Notification Rule

Section 164.402 of the interim rule defined a "breach" to mean generally "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information." 74 Fed. Reg. 42767 (Aug. 24, 2009). The phrase "compromises the security or privacy of the protected health information" was defined to mean that it "poses a

significant risk of financial, reputational, or other harm to the individual." *Id.* This definition had become known as the "harm standard." When a covered entity or business associate was faced with the question of whether a "breach" had occurred, it could either treat the use or disclosure as a breach, or perform a risk assessment to determine whether the harm standard had been met such that the issue rose to the level of a breach. If there was no breach, then the breach notification requirements were not triggered (that is, "no harm, no foul").

The Final Rule does away with the harm standard and replaces it with a more objective analysis. A covered entity or business associate still may either treat the item as a breach or perform a risk assessment, but now the question to be answered is whether "there is a low probability that the protected health information has been compromised." 78 Fed. Reg. 5566-01. This standard is more objective, and the HHS anticipates it will lead to a more uniform assessment of the definition of what constitutes a breach. 45 C.F.R. § 164.402. The risk assessment must analyze, at a minimum, the following factors:

> (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
>
> (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
>
> (iii) Whether the protected health information was actually acquired or viewed; and
>
> (iv) The extent to which the risk to the protected health information has been mitigated.

Id. § 164.402(2).

Conclusion

Overall, the Final Rule serves to significantly expand the reach of HIPAA's administrative simplification rules, most importantly the Privacy Rule and the Breach Notification Rule. This column emphasizes several of those requirements, but care should be taken to examine the Final Rule in its entirety. The preamble provides important background information that can serve to supplement the rule's language and to assist in implementing these changes with your clients. See Final Rule, 78 Fed. Reg. 5566.

About the Authors

Roger R. Clayton is a partner in the Peoria office of *Heyl, Royster, Voelker & Allen, P.C.*, where he chairs the firm's healthcare practice group. He also regularly defends physicians and hospitals in medical malpractice litigation. Mr. Clayton is a frequent national speaker on healthcare issues, medical malpractice and risk prevention. He received his undergraduate degree from Bradley University and law degree from Southern Illinois University in 1978. He is a member of the Illinois Association of Defense Trial Counsel (IDC), the Illinois State Bar Association, past president of the Abraham Lincoln Inn of Court, president and board member of the Illinois Association of Healthcare Attorneys, and past president and board member of the Illinois Society of Healthcare Risk Management. He co-authored the Chapter on Trials in the IICLE Medical Malpractice Handbook.

Gregory J. Rastatter is an associate in the Peoria office of *Heyl, Royster, Voelker & Allen, P.C.*, where he is a member of the firm's healthcare practice group. Greg's practice involves representing and advising hospitals on compliance issues, including drafting and analysis of hospital and medical staff bylaws, physician and allied health professional contracts, and other aspects of health law for compliance with state and federal law and Joint Commission standards. He received his undergraduate degree from Bradley University and a law degree from the University of Illinois College of Law in 2003. Greg is a member of the Peoria County Bar Association, the Illinois State Bar Association, and the American Bar Association.

J. Matthew Thompson is an associate in the Peoria office of *Heyl, Royster, Voelker & Allen, P.C.*. He practices primarily in the area of general tort defense. He received his B.S. in Accounting from Culver-Stockton College in 2005 and his J.D. *cum laude* from Southern Illinois University School of Law in 2008.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at **www.iadtc.org**.

IDC Quarterly, Volume 23, Number 3.

Illinois Association of Defense Trial Counsel, PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, idc@iadtc.org