Cyber Security in Medicine: It's Not Just HIPAA, Anymore

by F. Paul Greene, Esq.
fgreene@hselaw.com

Since at least 1996, medical professionals and practices have operated under a national regulatory framework designed to keep information concerning medical services both private and secure. That framework, the Health Insurance Portability and Accountability Act (known as "HIPAA"), is a uniform federal law that requires privacy and security of "protected health information" ("PHI"). PHI includes information that is either oral or recorded relating to an individual's past, present or future health or condition, health care provided, or payment for that health care. HIPAA regulates PHI that is stored, maintained or processed by a "covered entity," which is a health care provider, a health plan, or a health care clearinghouse.

To protect PHI, the United States Department of Health and Human Services issued regulations more commonly known as the Privacy Rule (originally published December 28, 2000) and the Security Rule (originally published February 20, 2003). The Privacy Rule generally prohibits disclosure of PHI without consent and grants individuals certain rights with respect to their PHI. The Security Rule, on the other hand, establishes security standards and practices for protected health information in electronic form ("ePHI").

Both Rules require that covered entities implement reasonable safeguards to avoid prohibited uses and disclosures of PHI, including ePHI. In this regard, HIPAA sets a flexible standard, inasmuch as the Rules contemplate that what is reasonable for a large hospital system may not be reasonable for a solo practitioner.

The Security Rule establishes substantive guidelines for keeping ePHI secure. These guidelines are categorized as either "required" or "addressable." A required guideline is mandatory, while an addressable guideline must only be implemented if, after a risk assessment, the covered entity determines that the guideline is reasonable and appropriate in light of the covered entity's risk management of ePHI. A key example of an addressable guideline is encryption. If, after an appropriate risk assessment, the covered entity determines that encryption is not reasonable and appropriate, it must document that determination and implement an equivalent reasonable and appropriate alternative measure.

If safeguards fail and a breach occurs, HIPAA requires notification of the breach. No element of harm is required to determine that a breach has occurred. Rather, a breach is presumed unless the covered entity can demonstrate that there is a low probability that ePHI has been compromised based on a risk assessment of at least four factors. These factors include the nature and extent of the ePHI involved; the person who accessed the ePHI or to whom the disclosure was made (e.g., an unauthorized employee inadvertently accessing an ePHI record versus a hacker stealing that record); whether the ePHI was actually acquired or viewed; and whether the risk to the ePHI has been mitigated.

If a HIPAA breach has occurred, a covered entity must provide notice of the breach to the affected individuals within 60 days of the breach. The covered entity also must provide notice of the breach to the Secretary of the Department of Health and Human Services. The timing of that notice depends on the scope of the breach. For smaller breaches, a covered entity can notify the Secretary annually. For breaches affecting 500 or more individuals, notice to the Secretary is required within 60 days of the breach, as is notice to the media in the relevant state or jurisdiction.

Complying with HIPAA, however, is not enough. Currently, 47 states (the only holdouts being Alabama, New Mexico, and South Dakota) have enacted at times overlapping and conflicting data breach notification requirements, with some states requiring substantive cyber security measures. For example, while HIPAA does not require encryption in all cases, some states do require encryption of "personal information" concerning their residents. Currently, New York does not require encryption.

Adding to this confusion, the various states have different deadlines for breach notification, which may be shorter or longer than those required under HIPAA. A common deadline, as adopted in the New York data breach notification statute is "in the most expedient time possible and without unreasonable delay." By definition, this is a subjective standard, and not as easily applicable as the 60-day deadline under HIPAA.

Continued on page 19

Reprinted with permission from The Bulletin - May/June 2016.
Published by Monroe County Medical Society. www.mcms.org

Cyber Security in Medicine

Continued from page 18

The state breach notification statutes further differ among themselves and differ with HIPAA on what constitutes a "breach." New York, for example, defines a "breach of the security of the system" as "unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business." Generally, the state statutes do not allow for the four-factor analysis as to whether a reportable breach has occurred provided under HIPAA, although other, state-specific factors may apply.

And the types of data protected by these state statutes is varied and increasing. Common protected data elements include an individual's name plus some more sensitive pieces of information, such as social security, driver's license number or bank account number. Some states go so far as to protect biometric data as well as e-mail addresses and passwords.

Adding to this complexity are the increasing efforts of the Federal Trade Commission ("FTC") to regulate cyber security, albeit without specific regulations. Rather, the FTC asserts authority under Section 5 of the federal FTC Act, which prohibits "unfair" and "deceptive" business practices that affect interstate commerce. The FTC has expanded its authority under the Act to create a de facto "reasonableness" standard, asserting that businesses, including covered entities otherwise regulated under HIPAA, must take reasonable measures to ensure that their customers' data is kept safe.

It is difficult to define, however, what this "reasonableness" standard entails. According to the FTC, it has provided relevant guidance in its speeches, business education, Congressional testimony, articles, blog entries, Commission materials, and settlements with businesses concerning cyber security. Given these numerous sources, it is impossible to distill a single clear standard for what the FTC would consider "reasonable" under all circumstances.

The FTC's powers in asserting this "reasonableness" standard are varied, ranging from a simple investigation (which itself can be both disrupting and costly) to a full blown civil action, seeking injunctive relief and penalties against the alleged offender. FTC action can result in a settlement under which a business agrees to 20 years of FTC cyber security monitoring, as well as substantial fines.

HIPAA compliance does not insulate against FTC investigation or enforcement. As an example, LabMD, a small cancer detection laboratory covered under HIPAA, found itself the target of an FTC investigation and enforcement proceeding in relation to an alleged breach. LabMD challenged the FTC's action and was eventually successful in asserting that the FTC had not shown the "substantial harm" necessary for enforcement under the FTC Act. That challenge, however, lasted approximately 6 years, and led to legal fees that ultimately shuttered LabMD's business. And the LabMD story is not over. The FTC has appealed the administrative ruling against it, which could lead to years of added cost for LabMD in its dispute with the FTC.

Hence, HIPAA marks the beginning of a covered entity's cyber security analysis. It's not just a question of whether ePHI is secure. Rather, medical professionals and practices must consider the state in which they practice and, potentially, whether their efforts to protect patient or even employee data would be found to be reasonable under an FTC analysis. This analysis becomes more complex as the threats posed by hackers and scammers become more widespread. A covered entity that ends its analysis with HIPAA does so at its peril.

Advanced Dermatology Associates

Stephen E. Presser, MD

MOHS Skin Cancer Surgery

General Dermatology

Dermatologic Surgery

Pediatric, Adult, and Geriatric Dermatology

Steven Altmayer, MD

joined our practice in August 2015.
Dr. Altmayer is a Brown University-trained MOHS Skin Cancer Surgeon.

Two Locations:

1815 South Clinton Ave., #530
Rochester, NY 14618
(585) 442-4310
Fax (585) 442-6750

114 Court St.
Geneseo NY, 14454
(585) 243-5990
Fax (585) 243-3256