FOLEY HOAG LLP

Key Elements of the New "Omnibus" HIPAA Privacy and Security Regulations

COLIN ZICK
Partner
Boston
617 832 1275 direct
czick@foleyhoag.com

On January 18, 2013, nearly four years after the passage of the HITECH Act and its amendments to HIPAA, and nearly three years after it proposed regulatory amendments, the U.S. Department of Health and Human Services ("HHS") has finally issued major "omnibus" revisions to HIPAA's privacy and security regulations.

In the 563 pages of the regulations and related regulatory comments, there are many substantive and technical changes. However, we distilled two major themes in these revisions:

- Extension of HIPAA generally, and in particular the direct extension of HIPAA to business associates and their subcontractors, so that now the entire food chain that deals with Protected Health Information ("PHI") falls under HIPAA's privacy and security regulations; and
- Ramping up the regulations on data breach, including shifting of the burden on breach notification, so that it squarely now sits on the covered entity/business associate to prove a "low probability" that PHI will be compromised.

Also notable is what these regulations did not do: they did not raise the cap on HIPAA civil monetary penalties. It remains at $1.5 million, which is somewhat surprising, in light of the increasing frequency and scope of breaches involving PHI, and the increasingly large penalties the Office of Civil Rights has imposed for HIPAA privacy and security violations.

The final rule is effective on March 26, 2013 and the compliance date is 180 days thereafter (September 22, 2013). Covered entities and business associates will have up to one year after the 180-day compliance date to modify existing contracts in order to comply with these revised rules.

- HIPAA's privacy and security requirements will now directly apply to business associates: "Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate." 45 C.F.R. § 160.102. This change includes subjecting both covered entities and business associates to compliance reviews. 45 C.F.R. § 160.308.
- The definition of "business associate" itself has been expanded to include:
  - (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data trans-mission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
  - (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on be-half of the business associate. 45 C.F.R. § 160.103.

- Subcontractors of business associates will automatically become business associates themselves, and business associates will be required to obtain "satisfactory assurances" that the subcontractors are complying with HIPAA. 45 C.F.R. § 164.308(b)(2).
- Business associates may also be liable for the increased penalties for noncompliance based on the level of culpability, up to a maximum penalty of $1.5 million. In addition, the factors that are taken into account for imposing civil penalties have been revised to include:
  - "The number of individuals affected";
  - "The time period during which the violation occurred";
  - "financial harm" to the affected individuals;
  - "harm to an [affected] individual's reputation";
  - "hinder[ing] an [affected] individual's ability to obtain health care".

In other words, breaches that impact more people over a longer time with resulting harm will be punished more severely. A history of previous "indications of non-compliance" also will be factored into this HIPAA civil penalty analysis. 45 C.F.R. § 160.408.

- The definition of breach is changed, with the burden now on the covered entity to prove there was not a breach. In particular, an impermissible use or disclosure of PHI is **presumed** to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised based on the following factors:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health in-formation was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated. 45 C.F.R. § 164.402(2).
- There are new limits on how information is used and disclosed for marketing and fund-raising purposes. Marketing is now defined to exclude the following:
  - Refill reminders; and
  - "For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment." 45 C.F.R. § 164.501.
- For fundraising, however, some elements of PHI can be used without patient authorization:
  - Name;
  - Address;
  - Contact information;
  - Date of birth;
  - Dates of care;
  - Treating physician;
  - Outcome information; and
  - Health insurance status.

As a condition of this use, however, patients must be given the chance to opt-out of fundraising contacts. 45 C.F.R. § 164.502(f)(1)

- The sale of an individual's health information without permission is prohibited. The rules also clarify that the prohibitions on the sale of health information do not apply to public health or research purposes, or treatment, or sale of an entity, or to a business associate. 45 C.F.R. § 164.502(a)(5)(ii).
- HIPAA won't protect the information of individuals who have been deceased for over 50 years, as the definition of PHI has been changed to exclude such information. 45 C.F.R. § 164.502(f).

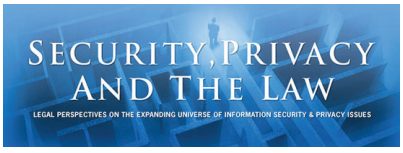
There are several provisions that make patient interactions with the health care system simpler and easier:

- The definition of "family member" is given greater specificity and breadth. It also should be easier for family members to access records of a deceased, if they were involved in the care of that period before death. 55 C.F.R. § 164.510(b)(5).
- When individuals pay for their care themselves, they can instruct their provider not to share information about their treatment with their health plan. 45 C.F.R. § 164.522(a)(1)(vi)(B);
- Patients can request a copy of their electronic medical record in an electronic format; 45 C.F.R. § 164.524(c)(3).
- An individuals' ability to authorize the use of his/her health information for research purposes will be streamlined. 45 C.F.R. § 164.508(b)(3)(i);
- It will be easier for parents and others to give permission to share proof of a child's immunization with a school; 45 C.F.R. § 164.512(b)(1)(vi).

Strangely, these regulations also include an expansion of very specific genetic privacy protections (which have no basis in the 1996 HIPAA statute). In particular, the definition of "health information" now includes "genetic information" and the final rule prohibits using or disclosing protected health information that is genetic information for underwriting purposes by all health plans that are covered entities under the HIPAA Privacy Rule, including those to which GINA does not expressly apply, except with regard to issuers of long term care policies. 45 C.F.R. § 164.502(a)(5)(i).

There are several other, less notable provisions, which will nevertheless impact HIPAA notices of privacy practices, business associate agreements and authorization for release of information and which will need to be included in any modifications to your policies, procedures and forms. We will be preparing model forms that incorporate all the changes found in this omnibus rule.

For the latest developments on this and other related topics, follow our blog.



FOLEY HOAG LLP

FOLEY HOAG LLP
Seaport West
155 Seaport Boulevard
Boston, MA 02210-2600
617 832 1000 main
617 832 7000 fax