Employee Benefits and Executive Compensation | Health Law Advisory: HHS Issues Rules Relating to Breach Notification and Related Items under the HITECH Act

8/26/2009

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a comprehensive set of rules regulating, among other things, the privacy and security of medical information. As originally adopted, HIPAA directly regulated only "covered entities," *i.e.,* health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with covered transactions. The HIPAA privacy rule established a set of patient rights, including the right of access to one's medical information, and placed certain limitations on when and how health plans and health care providers may use and disclose protected health information (PHI). The HIPAA security rule specifies a series of administrative, technical, and physical security procedures for providers and plans to use to ensure the confidentiality of electronic health information. HIPAA did not regulate vendors to covered entities—or "business associates," in the parlance of the final privacy and security rules. Covered entities are, however, required to enter into written agreements with "business associate covenants" in order to share PHI.

The HITECH Act

The original HIPAA regulatory scheme did not require covered entities or business associates to inform individuals in the event of security breaches involving their PHI. This omission changed with the recently enacted American Reinvestment and Recovery Act (ARRA, or the Act). The Act adds new breach notification requirements, along with certain new substantive privacy rights. In addition, the Act makes business associates directly responsible for complying with certain of the HIPAA privacy rules and all the HIPAA security rules. These provisions and others are contained in ARRA Title XIII, which is referred to as the "Health Information Technology for Economic and Clinical Health" (or HITECH) Act. HITECH is generally effective as of February 17, 2009, although most of the substantive HITECH provisions have delayed effective dates.

The HITECH Act requires covered entities to provide notification to affected individuals and to the Secretary of the U.S. Department of Health and Human Services (HHS) following the discovery of a breach of unsecured PHI. In some instances, HITECH also requires covered entities to provide notification to the media. Where the breach involves a business associate, the business associate must notify the covered entity of the breach. A "breach" for this purpose means "the unauthorized acquisition, access, use, or disclosure of protected health information,

which compromises the security or privacy of such information." To this general rule, there are exceptions for:

- instances in which the recipient of the information would not reasonably have been able to retain the information;
- certain unintentional acquisition, access, or use of information by employees or persons acting under the authority of a covered entity or business associate;and
- certain inadvertent disclosures among persons similarly authorized to access PHI at a business associate or covered entity.

"Unsecured PHI" is PHI that is not secured through use of a technology or methodology identified by HHS as rendering the information unusable, unreadable, or indecipherable to unauthorized persons.

As required by the Act, HHS issued guidance on technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable on April 17, 2009. That guidance described encryption and destruction as the two acceptable technologies. The Act also directed HHS to issue regulations, no later than August 16, 2009, addressing the Act's breach notice requirements as they apply to HIPAA covered entities and business associates. These rules are applied to breaches discovered on or after 30 days following the issuance of regulations.

The HHS Interim Final Rule

HHS issued an interim final rule on August 19, 2009, establishing standards for notification of breaches of unsecured PHI under the privacy and security rules. The rule clarifies certain key definitions and concepts, generally in a manner that is favorable to covered entities and business associates, while remaining true to the Act and the intent of Congress. The interim final rule also makes minor modifications to, and formally adopts, its April 17, 2009 proposal relating to which technologies and methodologies will render PHI unusable, unreadable, or indecipherable to unauthorized individuals (and, as a consequence, exempt from the Act's breach notice requirements). HHS has also clarified that the requirements of the HITECH Act are in addition to those of the security rule. Thus, while the security rule does not require encryption in all instances, encryption is necessary to avoid the HITECH breach notice rules.

The bulk of the interim final rule implements the breach notification provisions of the Act as they apply to HIPAA covered entities and their business associates.

Breach

Breach is defined to mean "the acquisition, access, use, or disclosure of protected health information…which compromises the security or privacy of the protected health information." The interim final rule makes clear that the definition of "breach" is limited to PHI. In determining whether notification is required under the Act, therefore, one must first determine whether a use or disclosure violates the privacy rule. This means, among other things, that the breach notice rules do not apply to employment records, which are not PHI. (Notification

requirements under other laws may still apply to employment records.) Similarly, breach notice rules do not apply to de-identified health information, again, because it is not PHI and because its disclosure does not violate the privacy rule.

A "breach" must relate to a use or disclosure that "compromises the security or privacy" of PHI. Once it is established that a use or disclosure violates the privacy rule, the covered entity must determine whether the violation compromises the security or privacy of the PHI. Here, HHS determined that the breach must "[pose] a significant risk of financial, reputational, or other harm to the individual" to trigger the obligation to provide notice. This will require covered entities and business associates to perform a risk assessment and use their discretion to determine if there is a *significant* risk of harm to the individual as a result of the impermissible use or disclosure. Covered entities and business associates are also instructed to consider who impermissibly used the information, or to whom the information was impermissibly disclosed, when evaluating the risk of harm to individuals. For example, if PHI is impermissibly disclosed to another covered entity, the chance of significant harm may be more remote, since the recipient is already obligated to protect PHI. Covered entities and business associates should also consider the type and amount of PHI involved in the impermissible use or disclosure. The disclosure of sensitive health information, such as mental health or infectious disease related information, is more likely to create a significant risk of harm.

Exceptions to Breach

The interim final rule includes the following three exceptions to the definition of "breach":

1. Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate.

   Example: A billing employee receives and opens an e-mail containing PHI about a patient, which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it. Because the billing employee's use of the information was done in good faith and within the scope of his authority, the disclosure does not constitute a breach.
2. Inadvertent disclosure of PHI from one person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.

   Example: A physician in a group practice has authority to use or disclose PHI at a hospital by virtue of participating in an "organized health care arrangement" (*e.g.,* hospital/group health practice). The physician mistakenly provides the wrong patient file to a nurse at the hospital. There is no breach in this instance.
3. Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

   Example: A covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. The covered entity can conclude that the improper

addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable and that the covered entity knows were sent to the wrong individuals, however, should be treated as potential breaches.

Unauthorized Acquisition, Access, Use, or Disclosure

The interim final rule defines the phrase "unauthorized acquisition, access, use, or disclosure of protected health information" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted" by the Act. In this regard, HHS helpfully reminds us that, while the HIPAA security rule provides for administrative, physical, and technical safeguards and organizational requirements for electronic PHI, it does not govern uses and disclosures of PHI. Therefore, a violation of the security rule does not itself constitute a potential breach under the Act's breach notice rules. Such a violation may, however, lead to a use or disclosure of PHI that is not permitted under the privacy rule and, thus, may violate the Act's breach notice rules.

Limited Data Sets

The interim final rule contains special rules related to "limited data sets." A limited data set is created by stripping from PHI 16 direct "identifiers" set out in the privacy rule. These identifiers include the name, address, social security number, and account number of an individual or the individual's relative, employer, or household member, but not birth dates and zip codes. Because HHS was concerned that birth dates and zip codes increase the potential for re-identification, it was unwilling to provide a blanket exemption from the Act's breach notice rule for limited data sets. Instead, the interim final rule establishes an exemption for limited data sets where zip codes or dates of birth have been removed. In addition, HHS recognized that there may be instances (based on a risk analysis) that the risk of identifying a particular individual is so small that the use or disclosure of a limited data set poses no significant risk of harm to any individuals. Note that even if a covered entity is able to avoid breach notice rules through the use of a limited data set, it may still have state law notification obligations.

Notice requirements

The interim final rule tracks closely the requirements of the Act. Notice of a breach must be provided without unreasonable delay and within 60 days after "discovery." A breach is "discovered" as of the first day that it is known (or reasonably should have been known) to the covered entity or the business associate. (A business associate that discovers a breach is required to notify the covered entity.) A covered entity or business associate is treated as having knowledge of a breach on the day that any employee, officer, or other agent has such knowledge or should have had such knowledge (except for the individual who committed the breach).

The notice of breach must, at a minimum, contain the following:

- a brief description of the breach, including dates
- a description of types of unsecured PHI involved
- the steps the individual should take to protect against potential harm

- a brief description of steps the covered entity or business associate has taken to investigate the incident, mitigate harm, and protect against further breaches
- contact information.

The interim final rule requires that the notices be written in plain language and that they not include the actual PHI that was the subject of the breach (*e.g.,* social security numbers). Notices must also tell the individual how to mitigate harm (*e.g.,* by notifying his or her credit card company if the breach included related financial information).

Additional notice requirements include the following:

- Written notice must be provided to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual). Notices to minors, incapacitated persons, and deceased persons may be made to their personal representatives.
- Where there is insufficient or out-of-date contact information, or in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the Web site of the covered entity or notice in major print or broadcast media is required. Where there is a possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the methods described above. Substitute notice for breaches involving fewer than 10 people may include alternative forms of written notice, telephone, email, or other means. Where the substitute notice covers more than 10 individuals, a toll-free telephone number must be provided for at least 90 days.
- Notice is required to be provided to prominent media outlets within the state or jurisdiction if a breach of unsecured PHI affects, or is reasonably believed to affect, more than 500 residents of that state or jurisdiction.
- What constitutes a prominent local media outlet depends on the circumstances. In the case of a small town, an appropriate media outlet may be the local newspaper. In other cases, a prominent local media outlet may be a major general interest newspaper with state-wide circulation. Notices to the media are required, in addition to individual notices.
- Notice must be furnished to HHS by covered entities immediately for breaches involving more than 500 individuals and annually for all other breaches.

The guidance contains helpful rules where a breach involves residents in multiple states or jurisdictions. For example, if a covered entity discovers a breach of 600 individuals, 200 of whom reside in Virginia, 200 of whom reside in Maryland, and 200 of whom reside in the District of Columbia, such a breach did not affect more than 500 residents of any one state or jurisdiction. As such, notification is not required to be provided to the media. But if a covered entity discovered a breach of unsecured PHI involving 600 residents within the state of Maryland and 600 residents of the District of Columbia, notification must be provided to a prominent media outlet serving the state of Maryland and to a prominent media outlet serving the District of Columbia.

It is also possible that a breach may occur at a business associate and involve PHI of multiple covered entities. There, a covered entity would only be required to provide notification to the media if the information breached included the PHI of 500 or more individuals located in any

one State or jurisdiction. But where the entities are unable to determine which entity's PHI was involved, the covered entities may require the business associate to provide notification to the media on behalf of all of the covered entities.

Timeliness

Generally, covered entities must send the required notification without unreasonable delay, and in no case later than 60 calendar days after the date the breach was "discovered." Covered entities may take reasonable time to investigate the circumstances surrounding the breach, however, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule. Importantly, 60 days is an outer limit. In some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification.

Conclusion

The HITECH breach notice requirements will go live in about a month, so there is little time to waste. While covered entities are accustomed to living with HIPAA's requirements, they must now be ready for an entirely new set of substantive requirements. The learning curve for business associates is steeper still, since they were previously regulated indirectly. There are other requirements of the HITECH Act intended to encourage HHS to step up its audit activities. Also, fines and sanctions have been increased, and state attorneys general have been given concurrent jurisdiction over the HITECH mandates. As a consequence, the compliance bar has been raised significantly.

Covered entities and business associates should take steps to secure their PHI so as to avoid having to provide breach notifications. The preamble to the interim final rule places a premium both on workforce training and on adopting and routinely revisiting policies and procedures regarding securing PHI. Policies and procedures also should be put in place to accommodate breach notifications, including guidelines for performing risk assessments and determining whether a breach that requires notice has occurred. Business associate agreements should also be revised to include specific references to the breach notice requirements.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Employee Benefits and Executive Compensation

BOSTON

Alden Bianchi
(617) 348-3057
AJBianchi@mintz.com

Tom Greene
(617) 348-1886
TMGreene@mintz.com

Addy Press
(617) 348-1659
ACPress@mintz.com

Patricia Moran
(617) 348-3085
PAMoran@mintz.com

NEW YORK

David R. Lagasse
(212) 692-6743
DRLagasse@mintz.com

Gregory R. Bennett
(212) 692-6842
GBennett@mintz.com

Jessica Catlow
(212) 692-6843
JCatlow@mintz.com

Health

BOSTON

Stephen M. Weiner
Chair, Health Law Practice
(617) 348-1757
SWeiner@mintz.com

Dianne J. Bourque
(617) 348-1614
DBourque@mintz.com

Thomas S. Crane
(617) 348-1676
TSCrane@mintz.com

Deborah A. Daccord
(617) 348-4716
DADaccord@mintz.com

Brian P. Dunphy
(617) 348-1810
BDunphy@mintz.com

Garrett G. Gillespie
(617) 348-4499
GGGillespie@mintz.com

Rachel M. Irving
(617) 348-4454
RMIrving@mintz.com

Ellen L. Janos
(617) 348-1662
EJanos@mintz.com

Krietta Bowens Jones
(617) 348-3042
KBowensJones@mintz.com

M. Daria Niewenhous
(617) 348-4865
DNiewenhous@mintz.com

Andrea P. Testa
(617) 348-4407
ATesta@mintz.com

Melissa O'Neill Thatcher
(617) 348-3015
MOThatcher@mintz.com

NEW YORK

Stephen C. Curley
(212) 692-6217
SCCurley@mintz.com

Andrew B. Roth
(212) 692-6889
ARoth@mintz.com

Nili S. Yolin
(212) 692-6799
NSYolin@mintz.com

WASHINGTON

Susan W. Berson
Managing Member,
Washington, D.C. Office
(202) 661-8715
SBerson@mintz.com

Karen S. Lovitch
Managing Member, Health Law Practice
(202) 434-7324
KSLovitch@mintz.com

Michael D. Bell
(202) 434-7481
MDBell@mintz.com

Stephen R. Bentfield
(202) 585-3515
SRBentfield@mintz.com

Theresa C. Carnegie
(202) 661-8710
TCCarnegie@mintz.com

Robert D. Clark
(202) 434-7402
RDClark@mintz.com

Hope S. Foster
(202) 661-8758
HSFoster@mintz.com

Lauren N. Haley
(202) 434-7386
LNHaley@mintz.com

Sarah A. Kaput
(202) 434-7423
SAKaput@mintz.com

Katina W. Lee
(202) 661-8729
KLee@mintz.com

Carrie A. Roll
(202) 434-7350
CARoll@mintz.com

Tara E. Swenson
(202) 585-3504
TESwenson@mintz.com

Heather L. Westphal
(202) 585-3538
HLWestphal@mintz.com

Jennifer E. Williams
(202) 585-3542
JEWilliams@mintz.com