Bloomberg BNA

BNA's
Health Law Reporter™

Data Breaches

Protected Health Information

A trend toward increased enforcement should prompt every company that interacts with protected health information to develop and maintain a plan to respond to breaches of PHI. This article focuses on three key steps affected entities should take: (1) determining whether a breach has occurred, (2) notifying the relevant parties, and (3) remediating the breach and preparing for a civil investigation.

HITECH Breaches: A How-To Guide



BY LISA J. SOTTO, AARON P. SIMPSON AND RYAN P. LOGAN

Virtually every business, well beyond those in the health care sector, comes into contact with protected health information, or PHI, which is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Most organizations interact with PHI through company-sponsored health plans. Others may serve as business associates or subcontractors to HIPAA-covered entities. Many of these organizations are not aware that they are subject to the breach notification requirements of the Health Information Technology for Clinical and Economic Health ("HITECH") Act.

Lisa J. Sotto is a partner in the New York office of Hunton & Williams LLP where she heads the Privacy and Data Security Practice. Aaron P. Simpson, a partner, and Ryan P. Logan, an associate, are based in New York on the Privacy and Data Security team.

Among other issues that can result in a breach, the widespread use of portable electronic devices to store PHI can leave an organization vulnerable to a potential breach of that PHI. According to statistics from the Health and Human Services Department's Office for Civil Rights (OCR), there have been over 530 reports since 2009 of large breaches of PHI involving more than 500 individuals, and thousands more involving fewer than 500 individuals.

The growing number of breaches of PHI has been met with increased enforcement by federal and state regulators. For example, in January 2013, OCR announced that it had entered into a resolution agreement and $50,000 settlement with the Hospice of North Idaho for a breach that affected 441 individuals. This marked OCR's first enforcement action relating to a breach in-

 ISSN 1064-2137

volving fewer than 500 affected individuals. In March 2012, OCR levied its first civil penalty resulting from a breach of unsecured PHI. BlueCross Blue Shield of Tennessee agreed to pay $1.5 million to settle potential HIPAA violations related to the October 2009 theft of 57 unencrypted hard drives containing the PHI of its members. At the state level, Minnesota Attorney General Lori Swanson entered into a $2.5 million settlement with Accretive Health in July 2012 for a security breach that compromised patient data.

The trend toward increased enforcement should prompt every company that interacts with PHI to develop and maintain a plan to respond to breaches of PHI. This article focuses on the three key steps affected entities should take: (1) determining whether a breach has occurred; (2) notifying the relevant parties; and (3) remediating the breach and preparing for a civil investigation.

Determining Whether a Breach of PHI Has Occurred

In 2009, the HITECH Act established a statutory requirement for breach notification. The Breach Notification Rule, issued in January 2013, implements the HITECH Act's requirements and defines a breach as ''the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.'' The phrase ''compromises the security or privacy of the protected health information'' was defined in the August 2009 Interim Breach Notification Rule to mean ''poses a significant risk of financial, reputational, or other harm to the individual.'' This harm threshold will remain in place until Sept. 23, 2013.

On Jan. 17, 2013, HHS announced the Final Omnibus HIPAA Rule, which modified the Interim Breach Notification Rule. The final rule replaced the harm threshold, which had imposed a notification requirement only where there was a ''significant risk'' of harm to an individual, with a presumption that any acquisition, access, use, or disclosure of PHI not permitted under the Privacy Rule would be considered a breach unless the covered entity or business associate could demonstrate that ''there is a low probability that the [PHI] has been compromised based on a risk assessment.''

The risk assessment to be made under this section must include consideration of four factors: (1) whether the acquisition, access, use, or disclosure of the PHI violates the HIPAA Privacy Rule; (2) whether the PHI involved was ''unsecured,'' (3) whether an exception to the definition of ''breach'' may apply; and (4) whether there was a low probability that the PHI has been compromised.

The first criterion to establish the existence of a breach of PHI is that the acquisition, access, use, or disclosure of PHI must violate the HIPAA Privacy Rule. Accordingly, any acquisition, access, use, or disclosure that is not permitted by the HIPAA Privacy Rule could equate to a potential breach of PHI. For example, a covered entity or business associate that uses or discloses more than the minimum amount of PHI necessary to serve the purpose of the use or disclosure potentially has violated the requirements of the Privacy Rule. The remaining three criteria also must be established.

With respect to the criterion requiring that the incident involve ''unsecured'' PHI, HHS has provided a definition of the relevant term. ''Unsecured'' PHI is any PHI that is ''not rendered unusable, unreadable, or indecipherable'' through the use of certain technologies (*i.e.*, encryption) or methodologies (*i.e.*, shredding paper records or purging electronic hard drives) specified by HHS. Accordingly, if PHI is not either encrypted or securely destroyed, it may be the subject of a breach if the PHI is compromised.

The third criterion addresses exceptions to the definition of ''breach.'' The Breach Notification Rule indicates that a ''breach'' does not include: (1) any unintentional acquisition, access, or use of PHI by a workforce member or authorized person, if made in good faith and within the scope of authority, and if there is no further impermissible use or disclosure; (2) any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same organization (or organized health care arrangement in which the covered entity participates), and the PHI is not further impermissibly used or disclosed; and (3) a disclosure of PHI where a covered entity or business associate has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information.

The final step (and fourth criterion) in establishing whether a breach has occurred is to conduct a risk assessment to determine whether there is a ''low probability'' that the PHI has been compromised. The risk assessment must include consideration of the following four factors:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;

(2) the unauthorized person who used the PHI or to whom the disclosure was made;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk to the PHI has been mitigated.

For the first factor, organizations should consider whether any PHI involved in a potential breach is ''of a more sensitive nature.'' For example, Social Security numbers and detailed clinical information would be considered more sensitive than a list of patient treatment dates because, as HHS indicated, such sensitive data ''could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests.''

With respect to the second factor, disclosures to another HIPAA-regulated entity or to a federal agency, for example, may result in a ''lower probability that the [PHI] has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.''

The third factor typically would involve a forensic analysis or investigation. For example, an entity that recovers a lost or stolen laptop would examine it to determine whether the PHI on the laptop actually was viewed or accessed.

The fourth factor might involve reaching out to the unauthorized recipient of the PHI and obtaining from that recipient ''satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.'' HHS noted in the Final Omnibus Rule that

   ISSN 1064-2137

it will issue future guidance on risk assessments associated with breaches, hopefully before Sept. 23, 2013, when the new risk assessment requirement for breaches becomes effective.

Notifying the Relevant Parties

Once the criteria for a breach of PHI has been established, the relevant parties must be notified. Covered entities, which include health care providers, group health plans, and health care clearinghouses, must notify affected individuals, HHS and, in certain cases, the media. These entities have a tight timeline in which to notify affected individuals—the notice must be provided without unreasonable delay and in no case later than 60 calendar days following discovery of the breach. HHS has indicated that the 60-day period is ''an outer limit and therefore, in some cases, it may be an 'unreasonable delay' to wait until the 60th day to provide notification.''

If a breach occurs while the PHI is in the possession of a business associate (*i.e.*, a service provider to the covered entity), the business associate must notify the covered entity following discovery of the breach. In turn, the covered entity typically will notify the affected individuals, HHS, and the media, although it is permissible for a covered entity to have its business associate provide the requisite notices. As a result of these requirements, covered entities should (1) ensure that their business associates have robust breach notification plans and (2) contractually obligate those business associates to notify them immediately following the discovery of a breach.

Covered entities generally are required to send breach notification letters to the last known address of the affected individuals. Notices also may be sent by email if the individual previously agreed to electronic notification. If contact information is not available for 10 or more affected individuals, a covered entity must provide ''substitute notice,'' which typically means a conspicuous posting on the entity's website for 90 days or a notice in a newspaper where the affected individuals likely reside. For deceased individuals, an entity is only required to send notification letters if it has the contact information of the individuals' next of kin or personal representatives.

The notice to individuals must include specific content such as: (1) a brief description of what happened, including the date of the breach and the date of discovery of the breach, if known; (2) a description of the types of unsecured PHI involved in the breach; (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (5) contact information for individuals to ask questions or learn additional information.

Regardless of the size of the breach, an affected entity must notify OCR. For large breaches impacting 500 or more individuals, a covered entity must notify OCR at the same time it notifies affected individuals by submitting a report that will be posted to OCR's website. For breaches involving fewer than 500 individuals, an entity must submit the report to OCR within 60 days after the end of the calendar year in which the breach occurred (*e.g.*, by March 1, 2013, for breaches occurring in 2012). The relevant OCR form requires a description of the breach and provides drop-down menus to more precisely describe the type of breach (*e.g.*, theft, loss or improper disposal) and other details.

Finally, for large breaches involving more than 500 residents of a state or territory, the covered entity must notify prominent media outlets. This is typically accomplished by taking out newspaper ads in journals circulating in large metropolitan areas of the jurisdiction.

Remediating the Breach and Preparing for a Civil Investigation

Following the discovery of a breach, a covered entity can take numerous steps to remediate the effects of the breach. For starters, it might offer credit monitoring to affected individuals in the event that Social Security numbers or financial account data are involved in the breach. The covered entity also might set up a call center to address the questions of affected individuals regarding the breach. Depending on the circumstances of the breach, the covered entity should consider: (1) revising its HIPAA privacy and security procedures, including its incident response plan; (2) training its workforce on how to safeguard PHI; (3) encrypting portable media that contain PHI; (4) requiring employees to change their passwords; and (5) increasing physical security through the use of biometric locks or other devices. Finally, a covered entity should sanction any member of the workforce whose conduct led to the breach. The relevant sanction could range from a written report placed in the employee's personnel file to termination in egregious cases.

OCR has indicated that it will review all breaches affecting more than 500 individuals. A covered entity that suffers a breach should prepare for a civil investigation by ensuring that it has comprehensive, written HIPAA privacy and security policies and procedures. OCR typically requests these in civil investigations. OCR also frequently requests evidence of sanctions taken against employees responsible for the breach, and proof that workforce members attended HIPAA training and received and acknowledged the organization's HIPAA policies and procedures. Finally, OCR typically requests the covered entity's prior risk assessments. Following a breach, it is critical that the covered entity focus on identifying any gaps in compliance that led to the breach and closing those gaps to ensure that another similar breach will not occur.

Lessons Learned

Breaches of PHI are inevitable. Although they are bound to occur, proactive planning can help mitigate the harmful effects of a breach. Breach prevention should be the focus for every organization. Data security requires the ongoing attention of senior executives and should not be the exclusive jurisdiction of the IT team. In addition, systems and safeguards should be reassessed frequently to ensure that vulnerabilities are identified and addressed in a timely manner. Most importantly, given the current ubiquity of breaches, every entity is well advised to integrate the concern for data security as a core value of the organization.