Health Lawyers Weekly

August 28, 2009 Vol. VII Issue 34

HHS Issues Interim Final Rule Governing Security Breach Notification

*By Lisa J. Acevedo, Shirley P. Morrigan, M. Leeann Habte, and Aaron K. Tantleff, Foley & Lardner LLP**

On August 19, 2009, HHS issued highly anticipated regulations (Regulations) to implement the new security breach notification requirements legislated pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act of 2009 (ARRA). Security breach notification is one of the key measures of the HITECH Act designed to further the adoption of electronic health records systems by providing more stringent protections for patient information.

The new Regulations were issued as an interim final rule with request for comments and will become effective 30 days after publication in the *Federal Register*, with comments due 60 days after such publication date. Given that the Regulations have been issued as "interim final" and that HHS has provided the 60-day comment period, they may be subject to further modifications.

The Regulations further delineate the new security breach notification requirements first outlined in the HITECH Act, and subsequently expanded upon in the HHS issuance, *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (*Guidance). HIPAA-covered entities (CEs) (healthcare providers, health plans, healthcare clearinghouses) and their business associates (BAs) must report security breaches in compliance with the Regulations. Under the Regulations, CEs must timely notify affected individuals if their unsecured protected health information (PHI) was the subject of a security breach. In doing so, CEs also must report such breaches to HHS (either concurrently or annually) and, in certain circumstances, the media. BAs must timely

notify their CEs of reportable security breaches such that the CEs can make reports to affected individuals and others as required by the Regulations.

The scope of the reporting obligations under the Regulations is highly dependent upon the definitions of critical terms such as "breach" and "unsecured." The Regulations attempt to clarify key definitions and provide guidance in interpreting the notification requirements outlined in the HITECH Act. The following summarizes key provisions of the Regulations.

Provisions Impacting the Obligation to Notify

The Regulations both clarify and provide interpretive guidance on occurrences considered to constitute reportable breaches as well as exceptions that may apply to relieve CEs and BAs from providing notification of otherwise reportable breaches.

Clarifications Regarding Definition of "Unsecured PHI"

The notification obligations under the Regulations only apply to breaches involving unsecured PHI, defined in the HITECH Act as PHI that is not secured with a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. On April 27, 2009, HHS published guidance to further define methods to create "secure" PHI not subject to the notification requirements. The Guidance specified encryption and destruction as the technologies and methods for securing PHI. The Guidance specified that encryption must be an algorithmic process with a confidential process or encryption key. With regard to destruction, the Guidance specified that paper copies of PHI must be shredded or destroyed and electronic media copies of PHI must be cleared, purged, or destroyed. The Guidance also described the National Institute of Standards and Technology (NIST) standards for valid encryption processes for data at rest and data in motion and for media sanitization.

The Guidance raised many further questions. The Regulations attempt to address those questions by providing additional clarification to the provisions of the Guidance as follows:

- When PHI is secured by means of encryption, the encryption key must be kept on a separate device from the encrypted data to ensure that the key is not itself breached.
- Redaction does not satisfy the requirements for destruction. As a result, redacted data might be considered unsecured PHI. However, redaction is an acceptable method for de-identification of PHI. As discussed below, de-identified information is not PHI and thus is not subject to the breach notification requirements.
- The Regulations also include a note that references NIST guidance on the development of security guidelines for enterprise-level storage devices such as

redundant array of inexpensive disks (RAID), or storage-attached network (SAN) systems.

Guidance on Definition of "Breach"

The HITECH Act defines "breach" as the "unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." The Regulations provide important interpretive guidance on what constitutes a breach under HIPAA.

What Is a Breach?

The Regulations provide two important points of clarification. First, according to the Regulations, "unauthorized acquisition, access, use, or disclosure" means that the acquisition, access, use, or disclosure is *impermissible* under the HIPAA Privacy Rule. Second, the Regulations clarify that such an unauthorized activity "compromises the privacy or security of PHI" if it *poses a significant risk for financial, reputational, or other harm to the individual*. According to HHS, this clarification addresses commentary requesting a harm threshold to trigger notification obligations.

Therefore, pursuant to the Regulations, not every impermissible use or disclosure of PHI constitutes a reportable breach. Significantly, this narrowing of the definition of a breach limits the number of breaches that CEs and BAs will be required to report. Conversely, it creates additional administrative burden because it requires CEs and BAs to conduct a risk assessment for each occurrence that otherwise fits within the definition of a "breach." The determination of whether an impermissible acquisition, access, use, or disclosure of PHI constitutes a breach hinges on whether there is a significant risk of harm to the individual as a result of the impermissible activity.

In conducting the risk assessment, the Regulations instruct CEs and BAs to consider the following factors:

- Who impermissibly used or to whom the information was impermissibly disclosed (e.g., if disclosed to another CE, there may be less risk because that entity is bound by HIPAA to protect the information).
- Whether immediate steps to mitigate the harm render the risk to the individual to be less than "significant," (e.g., recipient signs a confidentiality agreement assuring that it will not use or further disclose the PHI).
- Whether impermissibly disclosed PHI was returned prior to it being accessed for an improper purpose (e.g., a stolen laptop is recovered and forensic analysis establishes that the PHI was not opened, altered, transferred, or compromised).
- The type and amount of PHI involved in the impermissible use or disclosure (e.g., if the PHI at issue only includes patient name and fact that healthcare services

were received from a hospital, without more information, then there may not be a significant risk of financial or reputational harm).

Breaches Involving Limited Data Sets; Other Clarification

The Regulations clarify that limited data sets (except those that have been stripped of zip code and date of birth) are subject to the breach reporting requirements. In considering whether a reportable breach of a limited data set has occurred, the CE or BA must consider the risk of re-identification of the PHI, given the geographic area and related factors. Importantly, the Regulations clarify that CEs and BAs are not responsible for the breaches of limited data set recipients unless that recipient received the limited data set in the role as an agent for the CE or BA.

The Regulations also clarify that uses or disclosures that impermissibly involve more than the minimum necessary information also may qualify as reportable breaches.

What Is Not a Breach?

- Violations of the HIPAA Security Rule and certain violations of the HIPAA Privacy Rule are not considered reportable breaches in and of themselves although they may lead to an impermissible use or disclosure, which would be considered a breach and trigger notification obligations.
- The Regulations confirm that use or disclosure of de-identified information is not subject to the breach notification requirements because such information is not considered to be PHI. Use or disclosure of limited data sets where zip code and date of birth have been stripped also is not subject to the breach notification rules.
- The Regulations affirm that impermissible use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures does not qualify as a breach.

Exceptions to the Breach Notification Requirements

- **Unintentional** acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a CE or BA does not trigger notification obligations if such unintentional activity was done in good faith, within the course and scope of employment or other professional relationship, and does not result in further use or disclosure not permitted by the HIPAA Privacy Rule.
- **Inadvertent** disclosure of PHI from one person with authority to access PHI at a CE or a BA to another person who also has authority to access PHI does not trigger notification obligations if such inadvertent recipient is part of the same CE, BA, or Organized Health Care Arrangement as the individual who made the inadvertent disclosure, and provided the recipient does not further disclose the information in violation of the HIPAA Privacy Rule. The Regulations modify and expand the version of this exception in the HITECH Act, which had required the recipient to be within the same "facility" as the disclosing individual.
- **Unauthorized** disclosures in which the person to whom PHI is disclosed would not reasonably have been able to retain the information do not trigger notification obligations. This exception can be applied when the disclosing individual has a

good faith belief that the unauthorized recipient is unable to retain the information.

In determining whether a reportable breach has occurred, the Regulations advise CEs and BAs to take the following steps. First, the CE or BA must determine whether there has been an impermissible acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule. Second, the CE or BA must conduct a risk assessment to determine whether the impermissible activity compromised the security or privacy of the PHI. The results of that risk assessment and determination must be documented. Lastly, the CE or BA must evaluate whether the incident falls under one of the exceptions to the notification obligations described above.

Providing Notification Under the Regulations

Once a CE or BA has determined that a reportable security breach has occurred, the CE or BA must provide notification in compliance with the Regulations. The Regulations expand upon and clarify the requirements for providing notification of security breaches under the HITECH Act.

Notification Requirements Following a Breach

In general, the notification requirements provide that:

- CEs timely notify individuals when their unsecured PHI is breached.
- CEs timely notify the media if 500 or more individuals had their unsecured PHI breached in a given state or jurisdiction.
- CEs concurrently notify the HHS Secretary of any breach if it involves 500 or more individuals, regardless of location, and provide an annual log of breaches that involved fewer than 500 individuals.
- BAs timely notify CEs when an individual's unsecured PHI is breached.

Notification Requirements for Individuals

Upon the *discovery* of a reportable breach, CEs are required to provide notice to affected individuals without unreasonable delay, but in no case later than 60 calendar days from the time the CE discovered the breach or should have discovered the breach using reasonable diligence. The Regulations provide that CEs will not be liable for failure to provide notice of breaches in circumstances where the CE did not know, nor had reason to know, of the breach.

What Is the Effect of the "Discovered" Standard and the Requirement to Exercise Reasonable Diligence?

To successfully comply with the notification provisions of the Regulations, the notices must be sent within the required deadlines. The clock begins when a breach is

"discovered" or "should have been discovered" in the exercise of reasonable diligence. As a result, the Regulations advise that it is imperative that CEs and BAs implement reasonable systems to detect and discover potential breaches. The Regulations also advise that it is important to properly train and educate workforce members on the importance of timely reporting of any potential breaches and the consequences for failing to do so.

In response to comments, the Regulations also clarify that the clock begins when an incident is discovered, even if it is initially "unclear whether the incident constitutes a breach" subject to the notification requirements.

Timeliness of Notification — CEs

Except when a law enforcement delay, as discussed below, is applicable, the Regulations require CEs to provide notice of a breach of unsecured PHI without unreasonable delay, and in no case more than 60 calendar days from the date of discovery. The Regulations state that CEs may take reasonable time to perform an investigation to collect the required information to provide notice to an individual. However, as noted above, this investigation does not extend the time in which the CE must provide notice.

Content of Notification

The Regulations require notifications to individuals to be written in plain language and at an appropriate reading level so they can be easily understood. The Regulations do not impose a page limitation. The notifications must contain the following information, to the extent possible:

- A brief description of what happened, including the date of the breach and the date of discovery.
- A description of the type of unsecured PHI that was involved (e.g., name, Social Security Number, procedure, diagnosis, treatment, and so forth).
- The steps the CE is recommending that the individual should take to protect himself or herself.
- A brief description of what the CE is doing to investigate, mitigate harm, and protect against future similar breaches (this might include information regarding an investigation, police report, or what the CE is doing to retrieve the unsecured PHI).
- Contact information so the individual can communicate with the CE for additional information regarding his or her specific breach (the contact information must include at least one of the following: a toll-free number; e-mail, Web site, or postal address).
- Any sanctions the CE imposed on any workforce members involved with the breach

The Regulations note that CEs may need to take reasonable steps to ensure meaningful access to and effective communication of the notice under the Rehabilitation Act of 1973,

Americans with Disabilities Act of 1990, and to Limited English Proficient Persons under the Civil Rights Act of 1964, including, but not limited to, providing the notification in different languages, Braille, large print, or by audio means.

Methods of Notification

The Regulations adopt the HITECH Act's provisions for "actual" notification and "substitute" notification.

Actual Notification

A CE is required to provide actual written notice via first-class mail at the last known address of any individual whose unsecured PHI has been breached. The Regulations permit written notice to be sent via e-mail if the individual earlier consented to being contacted in this manner. If the individual is a minor or otherwise not capable of receiving or understanding the notice, the notice should be sent to the parent or legal guardian, as authorized under applicable law.

In urgent cases, where there is a fear of possible imminent misuse of an individual's PHI, the Regulations authorize a CE to use alternative methods to contact the individual, for example, by telephone. However, the Regulations emphasize that this method of notification is not a substitute for actual, written notification.

If the CE knows the individual is deceased, the notification should be provided to the deceased's next-of-kin or personal representative. However, the Regulations clarify that if contact information for the next-of-kin or personal representative was not previously provided by the individual, the CE is not obligated to seek it. The Regulations also clarify that if the CE is not aware the individual is deceased, the CE is not obligated to contact such individual's next-of-kin or personal representative.

Substitute Notification

If an affected individual's last known contact information is out-of-date or incomplete and cannot be used to contact the individual, or if notifications are returned because they are undeliverable, the CE can provide a substitute notice in lieu of an actual written notice. However, the substitute notice must be reasonably calculated to reach the particular individuals to whom the CE could not provide actual written notice.

The Regulations provide that the substitute notice requirement can be satisfied by the following methods, so long as the substitute method does not unnecessarily disclose PHI:

- If there are less than 10 individuals at issue, an alternate written form, telephone call, or other means may satisfy this requirement, even if the individuals had not previously consented to such alternative forms of notice.
- Where 10 or more individuals are at issue, the CE can satisfy the notification requirement by posting a conspicuous notice on the home page of its website for 90 days, or placing a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals reside.
- The substitute notice must be reasonably calculated to reach those affected individuals and must include a toll-free number for those individuals to use to contact the CE for additional information. This toll-free phone number must remain active for at least 90 days.

Notification to Media

If a reportable breach affects 500 or more residents of a state or jurisdiction, the Regulations require the CE to notify a prominent media outlet serving that state or jurisdiction. The Regulations declined to define a "prominent media outlet" because such definition will differ depending on the state or jurisdiction at issue. However, the Regulations provide some guidance by indicating that if the breach affects individuals across a particular state, then a "prominent media outlet" could be a major newspaper with a state-wide daily circulation. If the breach affects individuals in a particular city, then a "prominent media outlet" could be a major newspaper with city-wide, but not state-wide, daily circulation.

The Regulations provide that the notification to the media is in addition to the actual written notice, and not in lieu of it. However, this notice can serve as the substitute notice in the event actual notice is not possible if the notification to the media also meets all of the requirements for substitute notice (e.g., the notice includes a toll-free number and is reasonably calculated to reach those individuals to whom the CE could not provide actual written notice).

Timeliness of Media Notification

The Regulations clarify that the notice to the media must be provided without unreasonable delay, but no later than 60 calendar days from discovery. This notice must contain the same information as what is included in the actual written notice to the individuals. The Regulations anticipate that most CEs will issue notice in the form of press releases.

Clarification as to Circumstances Where Media Notification Is Not Required

The Regulations clarify that notification of the media is not required in the following circumstances, notwithstanding that a breach involves 500 or more affected individuals:

- Where the affected individuals are spread out over several states and no single state has 500 or more affected individuals.
- Where the breach occurred at a BA and implicated several CEs, but no individual CE had 500 or more affected individuals in a particular state or jurisdiction. However, if the BA cannot determine which CEs' unsecured PHI was involved, the Regulations advise that it may be wise for the BA to provide media notification on behalf of all the affected CEs.

Notification to HHS Secretary

CEs are required to provide notice of any breach to the HHS Secretary. For breaches involving fewer than 500 individuals, the CE is only required to maintain a log and submit it annually to the HHS Secretary. However, under the HITECH Act, if the breach involves 500 or more individuals, regardless of geography, "immediate" notice to the HHS Secretary is required. The Regulations interpret "immediate" notice to mean that notice to the HHS Secretary must be sent concurrently with the notifications sent to the affected individuals.

The Regulations provide that the HHS Secretary will post instructions on its website for submitting the concurrent notifications as well as the annual log.

The HHS Secretary also will post on its website a listing of all CEs who submit reports of breaches involving 500 or more individuals. The Regulations clarify that the state or jurisdiction in which such individuals reside is irrelevant to the requirement to provide concurrent notice to HHS.

Notification by BAs

BAs must notify CEs of reportable breaches in order for the CEs to notify the affected individuals. The Regulations require BAs to provide notice to CEs without unreasonable delay, and no later than 60 days from the date that the BA discovers the breach or should have discovered it using reasonable diligence. BAs, to the extent possible, must identify each affected individual and provide such information to the CE.

When Discovery by a BA Will Be Imputed to the CE

The Regulations clarify that where the BA is an agent of the CE, the date the BA discovers (or should have discovered) the breach will be imputed to the CE. As a result, it will be important that the business associate agreement between the parties clearly addresses the fact that the BA must provide the CE with notification of the breach as soon as it is discovered. However, the Regulations also clarify that where the BA is an independent contractor, and not an agent, of the CE, the CE is not considered to have discovered the breach until it is notified by the BA of the breach.

Interplay Between the Regulations and the FTC Regulations

In certain circumstances, BAs could be subject to both the Federal Trade Commission (FTC) Security Breach Notification Regulations (FTC Regulations) (*See* Foley's August 19, 2009 Legal News Alert: http://www.foley.com/publications/pub_detail.aspx?pubid=6332) and the Regulations in circumstances where BAs provide personal health records (PHRs) both to customers of a CE through a business associate agreement and also directly to the public. The Regulations address this by providing that, in certain circumstances, the BA will be deemed to have complied with the FTC Regulations where the BA complies with certain provisions of the Regulations and also complies with the other provisions of the FTC Regulations, including notifying the FTC within 10 days of discovering a breach.

Law Enforcement Delay

The timeframe for providing notification under the Regulations may be temporarily delayed if a law enforcement official determines that notification of the breach would impede a criminal investigation. The Regulations provide that CEs must delay notification upon receiving a statement from a law enforcement official that sets forth the timeframe for the delay. If the request is given orally by a law enforcement official, the CE must document the statement and the identity of the official. A request for a delay given by an oral statement may only delay the notification deadline by 30 days unless, before such time, a written statement is provided.

State Security Breach Notification Laws and Preemption Under the Regulations

With the increasing number of state breach notification laws, many CEs and BAs will be required to analyze state law preemption issues to determine their reporting obligations. For purposes of the HITECH Act security breach notification requirements, contrary state laws are preempted. The Regulations clarify that a law is "contrary" if a CE would find it impossible to comply with both the state and federal requirements or if the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the HIPAA breach notification provisions. The Regulations clarify that certain exceptions to the preemption of state law set forth at 45 CFR 160.203 do not apply to security breach notification requirements, but solicit comments in this regard.

While some of the state breach notification laws for medical information use the degree of harm as a factor in determining whether a reportable breach occurred (as does HIPAA), others take an alternative approach. For example, California law requires that discovered breaches (unauthorized access, use, or disclosures) be reported in five calendar days. Degree of harm associated with the unauthorized access, use, or disclosure is not a factor.

The Regulations state that "in general, we believe that covered entities can comply with both the applicable State laws and this regulation." Accordingly, from a practical perspective, CEs will most likely have to comply with both state and federal law.

* **Lisa J. Acevedo** is a partner with Foley & Lardner LLP and a member of its Health Care Industry Team and Privacy, Security & Information Management Practice. Ms. Acevedo provides regulatory advice to clients representing virtually all aspects of health care, and in particular focuses on federal and state data privacy and security laws. Ms. Acevedo can be reached at lacevedo@foley.com.

Shirley P. Morrigan is a partner with Foley & Lardner LLP, a member of its Health Care Industry Team and Privacy, Security & Information Management Practice, and co-leader of the Health Care Industry Team Regulatory and Strategic Counseling Work Group. She represents healthcare providers in matters relating to privacy, security, and confidentiality of medical information. Ms. Morrigan can be reached at smorrigan@foley.com.

M. Leeann Habte is an associate with Foley & Lardner LLP and a member of its Health Care Industry Team and Privacy, Security & Information Management Practice. She is a Certified Information Privacy Professional with management experience developing and implementing data privacy and security policies. Ms. Habte can be reached at lhabte@foley.com.

Aaron K. Tantleff is an associate with Foley & Lardner LLP and a member of its Information Technology & Outsourcing Practice and Health Care Industry Team. His practice includes information technology, outsourcing, licensing, transactional intellectual property and technology transactions. Mr. Tantleff can be reached at atantleff@foley.com.

Peter F. McLaughlin (pmclaughlin@foley.com), Michael Scarano (mscarano@foley.com), and Andrew B. Serwin (aserwin@foley.com) also contributed to this article.

Suite 600, 1025 Connecticut Avenue NW
Washington, DC 20036-5405
Phone: 202-833-1100 Fax: 202-833-1105