American Hospital Association

Regulatory Advisory

September 9, 2009

HHS' Breach Notification Obligations: The Interim Final Rule

At a Glance

The Issue:

The Department of Health and Human Services (HHS) published in the August 24 Federal Register its interim final rule implementing the *Information Technology for Economic and Clinical Health (HITECH) Act's* breach notification requirements. Under the rule, hospitals and other HIPAA-covered entities and their business associates must notify individuals when the privacy of their "unsecured" personal health information (PHI) is breached. It also updates HHS' guidance specifying technologies and methodologies for securing PHI that, while voluntary, would provide a "safe harbor" from HITECH's federal notice obligations for HIPAA-covered entities and business associates that adopt them.

The notice obligations are effective for breaches occurring on or after September 24. However, because covered entities may require time to implement compliance programs, HHS will use its "enforcement discretion to not impose sanctions for failure to provide [notices] for breaches that are discovered before 180 calendar days" from the rule's August 24 publication date.

Our Take:

We are pleased that HHS adopts a "risk of harm" trigger for the breach notification requirement. That is, an incident is not a breach for which notice is required if there is no reasonable likelihood of harm (e.g., identity theft). While we are disappointed that HHS declined to expand the list of technologies and methodologies that covered entities and their business associates can use to secure PHI and, thereby, create a "safe harbor" from the federal notice obligations, we believe that the "risk of harm" trigger may mitigate the impact of HHS' decision to limit the technologies and methodologies in the guidance to encryption and destruction. Hospitals that choose to follow the guidance nevertheless may have to comply with other legal obligations including state breach notice laws.

What You Can Do:

- ✓ Share this advisory with your senior management team, including your chief information officer, legal counsel, and security and privacy officers.
- ✓ Examine HHS' guidance to determine the extent to which your hospital is able to adopt its recommendations to secure PHI, thereby creating a safe harbor.
- ✓ Plan to participate in an upcoming AHA member conference call to discuss the rule's requirements and implementation. Watch your inbox for additional information about these calls, including dates and times.
- ✓ Consider submitting comments to HHS supporting its decision to adopt a risk-based definition of breach. Comments are due to HHS by October 23.

Further Questions:

Please contact Lawrence Hughes, assistant general counsel, advocacy and public policy, at (202) 626-2346 or lhughes@aha.org.

AHA's Regulatory Advisories are produced whenever there are significant regulatory developments that affect the job you do in your community. A 10-page, in-depth examination of this issue follows.

American Hospital Association

Regulatory Advisory

September 9, 2009

HHS' BREACH NOTIFICATION OBLIGATIONS: THE INTERIM FINAL RULE

BACKGROUND

The Department of Health and Human Services (HHS) released an interim final rule implementing the *Information Technology for Economic and Clinical Health (HITECH) Act's* breach notification requirements. The law requires hospitals and other HIPAA-covered entities and their business associates to notify individuals when the privacy of their "unsecured" personal health information (PHI) is breached. The rule also updates HHS guidance specifying technologies and methodologies for securing PHI that provide a "safe harbor" from the federal notice obligations.

The notice obligations are effective for breaches occurring on or after September 24. However, because covered entities may require time to implement compliance programs, HHS will use its "enforcement discretion to not impose sanctions for failure to provide [notices] for breaches that are discovered before 180 calendar days" from the rule's August 24 publication in the *Federal Register*. "During this time period," HHS warns, "we expect covered entities to comply … and will work with [them], through technical assistance and voluntary corrective action, to achieve compliance."

This advisory looks at the rule's major provisions and the significant changes to HHS' guidance document.

AT ISSUE

HHS' rule applies to HIPAA-covered entities and business associates

Hospitals and other organizations that are HIPAA-covered entities and their business associates are subject to the HHS rule on breach notification, not that of the Federal Trade Commission (FTC). As HHS explains in the interim final rule, "in those limited cases where an entity may be subject to both HHS' and the FTC's rules, such as a vendor that offers [personal health records] to customers of a HIPAA-covered entity as

a business associate and also offers [them] directly to the public, we worked with the FTC to ensure both sets of regulations were harmonized by including the same or similar requirements, with the constraints of the statutory language." HHS also clarifies that covered entities and their business associates will not be responsible for a breach by a third party to whom they have *permissibly* disclosed PHI; the third party will remain responsible for properly handling the information under applicable legal requirements.

HHS also clarifies that contrary state laws will be preempted by the HHS' breach notification requirements. The AHA had urged HHS to provide such clarification and to use the definition of "contrary" in the existing HIPAA regulations as the basis for determining whether a state law is preempted. In the interim final rule discussion, HHS explains that a state law is contrary to these regulations if, as the existing HIPAA regulations state, a covered entity "would find it impossible to comply with both the State law and federal requirements or if the State law stands as an obstacle to the accomplishment and execution of the full purpose and objectives of the breach notification provisions." Thus, **hospitals will need to analyze relevant state laws to understand and appropriately apply the preemption standard when implementing the HHS breach notification provisions.**

Despite receiving examples from the AHA and others of conflicts between state laws and the federal breach notification requirements, HHS believes that covered entities generally can comply with both. HHS also believes that in most cases a single notification will satisfy both federal and state requirements. As an example, HHS explains that where a state law requires that notice be provided within five days following a breach, a covered entity that complies with that state law requirement also will be in compliance with the federal rule's "without unreasonable delay" standard. HHS notes that a covered entity that does not have all the information required by the federal regulation within the five-day period specified in the state law can send an additional notice to the individual when it has gathered the appropriate information.

Likewise, HHS notes that there is no conflict between the federal requirements and a state law that specifies additional content requirements for the notice or requires that particular notice content be described in a certain way. According to HHS, the provisions of HITECH and the interim final rule do not prohibit additional content from being included in the notice and are flexible regarding how elements are to be described.

Rule's definition of "breach" is risk-based

In line with the recommendations of the AHA and others, HHS adopts a "risk of harm" trigger for the requirement to provide notice when a breach of unsecured PHI occurs. "Breach" is defined specifically to mean the "acquisition, access, use, or disclosure" of PHI in a manner not permitted by the HIPAA privacy rule which "compromises the security or privacy" of that information. "Compromises the security or privacy" of the information is defined to mean "poses a significant risk of financial, reputational, or other harm to the individual."

To decide whether a breach for which notification must be provided has occurred, one of the first steps is to determine whether a use or disclosure violates the HIPAA privacy rule. According to the HHS discussion, a use or disclosure of more than the minimum necessary information would violate the privacy rule and, therefore, qualify as a breach; but a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure where minimum necessary requirements are followed and reasonable safeguard are in place would not be a privacy rule violation and, consequently, would not be a breach. Additionally, the inadvertent or unauthorized use or disclosure of information that is de-identified in accordance with the requirements of the HIPAA privacy rule is not a breach because the definition of the term is limited specifically to PHI.

If a use or disclosure is found to violate the privacy rule, it must be determined if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. The discussion in the rule describes some of the factors or combination of factors to consider in the risk assessment. In a discussion footnote, HHS recommends that covered entities review OMB Memorandum M-07-17 for examples of factors to consider in this risk assessment. **The burden of demonstrating that no breach occurred because the impermissible use or disclosure did not pose a significant harm falls on covered entities and business associates and they must document and preserve their risk assessments in order to demonstrate compliance with the breach notification rule.**

The rule however explicitly states that a use or disclosure of PHI in the form of the *HIPAA-limited data set that also excludes dates of birth and zip codes* does not compromise the security or privacy of the information and, therefore, is not a breach under the rule. HHS decided to include directly in the interim final rule this more narrow exception to the definition of breach for a restricted version of the HIPAA-limited data set rather than designate the HIPAA-limited data set itself as one of the ways to secure PHI in a revision of its guidance document specifying the technologies and methodologies covered entities can use to create a safe harbor from the federal notice requirements. HHS emphasizes that the exception is to be construed narrowly, meaning that it would not apply if the information, for example, is stripped of birth dates but still contains zip codes. **Covered entities and business associates again will need to document that the information is a HIPAA-limited data set that also excludes dates of birth and zip codes in order to satisfy their burden of proof regarding compliance with the breach notification rule.**

HHS' decision to provide this explicit exception for the restricted version of the HIPAA-limited data set does not, however, prohibit a covered entity from performing a risk assessment to determine whether there is a significant risk of harm to the individual caused by an impermissible use or disclosure of PHI in the form of the HIPAA-limited data set itself. HHS notes that such a risk assessment should take into consideration the risk of reidentification of the information in the HIPAA-limited data set that is impermissibly used or disclosed.

The definition of breach in the rule also excludes certain circumstances to comply with HITECH's explicit statutory exemption relating to whether a recipient of the information would "reasonably have been able to retain" the information:

- Any unintentional acquisition, access, use of PHI by an workforce member (or person acting under the covered entity's or business associate's authority), if it was made in good faith and within the scope of authority and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA privacy rule.
- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person who is authorized to access PHI at the same facility or business associate (or organized health care arrangement in which the covered entity participates) and the information received is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA privacy rule.
- A disclosure of PHI where a covered entity or business associate has a good faith belief that unauthorized person who receives the information would not reasonably have been able to retain such information.

The covered entity or business associate again bears the burden of demonstrating that any of the above exceptions apply and must document precisely why the impermissible use or disclosure falls within the specific exception.

Breach discovered when impermissible use or disclosure is known

Under the rule, a breach is discovered on the first day it is known, or by exercising reasonable diligence would have been known, to the covered entity or the business associate. Reasonable diligence refers to the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." The covered entity or business associate is deemed to have knowledge of a breach if any workforce member or agent (applying the federal common law of agency) of the covered entity or the business associate, other than the individual committing the breach, knows or, by exercising reasonable diligence should know of, the breach.

The rule imputes directly to a covered entity a business associate's discovery of a breach in circumstances where a business associate is acting as an agent, not as an independent contractor, of the covered entity. In this circumstance, the timeliness of the required notice is tied to the business associate's discovery of the breach. On the other hand, where a business associate is an independent contractor of the covered entity, the timing of the required notice is based on when the business associate notifies the covered entity of the breach.

Both covered entities and business associates will need to implement reasonable processes for discovery of breaches. Because the rule attributes knowledge of a workforce member or other agent, including certain business associates, directly to the covered entity and, thereby starts the clock for timely provision of the notice, **it also is essential for covered entities to ensure that workforce members** (which includes

employees, volunteers, trainees and other persons whose conduct is under the direct control of the covered entity without regard to whether they are paid by the covered entity) **and other agents are appropriately trained and aware of the importance of timely reporting of security and privacy incidents. Covered entities also may want to address notification timing issues in their business associate agreements.**

Covered entities must notify affected individuals, media and HHS

Under the rule, a covered entity that discovers a breach of unsecured PHI must notify each individual whose PHI "has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed" because of the breach. The notification must be provided *without unreasonable delay* and no later than 60 days after the discovery of the breach, unless the notice must be delayed because a law enforcement official has requested delay to prevent impeding a criminal investigation or harm to national security. The covered entity bears the burden of showing that the required notices were provided, including that any delay was necessary.

HHS expects that a covered entity generally will provide the required notifications as soon as reasonably possible. The rule permits the covered entity to investigate the circumstances surrounding the breach to collect information it is required to include in the notification. Where a covered entity promptly investigates a reported breach and can swiftly conclude that there was no breach (e.g., an employee reports a stolen laptop but it is discovered in another secure office of the covered entity the next day), the covered entity does not need to send out any breach notification. The rule also permits the covered entity to provide the information required in the notice in multiple mailings as the information becomes available provided however that the required information is given within the timeframes set by the statute and the rule.

Because of these timeliness requirements, the investigation cannot take an unreasonable amount of time. For example, an unreasonable delay would occur where a covered entity learns of a breach but unreasonably allows the investigation to lag for 30 days. Further, because HHS considers the 60 days to be the outer limit, in certain cases it may be an unreasonable delay if a covered entity waits until the 60th day to provide notification. Where a covered entity, for example, has by the 10th day collected the necessary information required to be in the notice but waits until day 60 to send the notice, an unreasonable delay results.

A covered entity nevertheless may be required to delay temporarily notification if requested to do so by a law enforcement official. The rule adopts the definition of law enforcement official from the HIPAA privacy rule. If the law enforcement official makes a written request that specifies the time that is required for the delay, the covered entity must delay notification for that period. Where the request is made orally, the covered entity may delay the notification for not longer than 30 days, unless during this period the covered entity receives a written request that specifies the time required for the delay. In the case of oral request, the covered entity must document the law enforcement official's statement and the identity of the official making the request for the delay.

The rule requires the content of the notice follow the statutory provisions, requiring inclusion to the extent possible of:

- A brief description of what happened, including the date of the breach and its discovery, if known;
- A description of the type, not an itemized list, of the unsecured PHI breached (e.g., whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other general types of information were involved);
- A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individuals whose information was breached, and safeguard against further breaches;
- Any steps individuals should take to protect themselves from the potential harm of the breach; and
- Contact information, which must include a toll-free telephone number, e-mail address, Web site or postal address, so that affected individuals can ask questions or receive additional information.

Although there is no page limit, notices must be written in plain language, meaning that a covered entity should use clear language and syntax, avoid any extraneous materials that might diminish the message, and write at an appropriate reading level. Additionally, HHS cautions that some covered entities may have other legal obligations that affect how they communicate with affected individuals, including responsibilities to ensure meaningful access for persons with limited English proficiency (e.g., by translating the notice into frequently encountered languages) or with disabilities (e.g., by providing the notice in Braille, large print, audio or other formats).

The rule requires that notices must be sent directly to affected individuals, and in certain circumstances to prominent media outlets, as well as to the Secretary of HHS:

Notice to Affected Individuals*.* The covered entity must provide written notice to each affected individual by first-class mail to the last known address of the individual (or, if indicated as a preference by the individual and the individual has not withdrawn that preference, by electronic mail). Where the affected individual is a minor or otherwise lacks legal capacity, notice to the parent or the personal representative will satisfy the requirement. If the covered entity knows that the affected individual is deceased and has appropriate address information, notice to the next of kin or to the personal representative (as defined in the HIPAA privacy rule) is sufficient to satisfy the requirement.

Notice in Urgent Situations*.* In any case that the covered entity determines is urgent because the possibility of misuse of the unsecured information is imminent, the covered entity may contact affected individuals by telephone or other appropriate means. The rule clarifies that such notification is in addition to, not in lieu of, direct written notification to the affected individuals as described above.

Substitute Notice When Contact Information is Insufficient or Outdated. When individual contact information is insufficient or so out of date and therefore precludes direct written notification to affected individuals, a substitute form of notice is permitted by the rule. Substitute notice must be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals. However in the case of a deceased individual who is affected by the breach, the covered entity is not required to provide substitute notice to the next of kin or the personal representative if the covered entity either does not have contact information or has out-of-date contact information for the next of kin or the personal representative. Substitute notice must include all of the content required in the direct written notice to individuals.

The form of the substitute notice must be reasonably calculated to reach the individuals for whom it is being provided. When less than 10 individuals are involved, a covered entity may notify them by telephone or through an alternative form of written communication such as email, even if the individuals have not agreed to that form of contact. HHS cautions that covered entities should be sensitive to not unnecessarily disclosing PHI in the process. Alternatively, posting to the covered entity's Web site or at another location may be appropriate if the covered entity lack any current contact information, as long as the posting is reasonably calculated to reach the individuals.

In the case where there are 10 or more individuals for whom the covered entity has insufficient or out-of-date contact information, the covered entity is required by the rule to use a conspicuous posting for 90 days on the home page of its Web site or in major print or broadcast media in the geographic area where the individuals affected by the breach likely reside. The Web posting or media notice must include a toll-free telephone number where an individual can learn whether his or her PHI is included in the breach.

Notice to the Media. If the breach involves the unsecured PHI of more than 500 residents in a specific state or jurisdiction, the covered entity also must notify prominent media outlets serving that state or jurisdiction. The notice to the media must include the same information required in the direct written notice to affected individuals and be provided within the same timeframe required for the individual notices. HHS expects that most covered entities will use a press release for the notice to the media.

"Prominent" media outlet is not specifically defined in the rule because it will differ depending upon the state or jurisdiction affected. For a breach affecting more than 500 individuals throughout the state, a major, general-interest newspaper with a state-wide daily circulation would qualify as a prominent media outlet while a newspaper serving a single town in the state or a daily newspaper of specialized interests (e.g., sports or politics) would not. When the breach affects only individuals in a specific city, a major general interest newspaper with a daily circulation in the city alone, even if it does not serve the whole state, would qualify as an appropriate media outlet.

Notice to the Secretary of HHS. If the breach involves more than a total of 500 individuals, regardless of their residency, the covered entity also must notify the

Secretary of HHS concurrently with the required notification sent to the affected individuals. For all other breaches, the covered entity may maintain a log documenting the breaches that occur during the year and submit that log to HHS no later than 60 days after the end of each calendar year. The rule states that information provided to the Secretary is to be provided in the manner specified on the HHS Web site and HHS expects to provide these instructions shortly. The rule also requires the Secretary to post on the HHS Web site a list identifying each covered entity involved in a breach where the unsecured PHI of more than 500 individual is acquired or disclosed.

Business associates must notify covered entities

When a business associate discovers a breach of unsecured PHI by the business associate, the rule requires the business associate to notify the covered entity of the breach so the covered entity can notify the affected individuals. The rule clarifies that a business associate who maintains PHI for multiple covered entities need notify only the covered entity to which the breached information relates. However, if it is unclear to which covered entity the information relates, a business associate may be required to notify all potentially affected covered entities. The rule leaves the decision about how the required reporting from business associate to covered entity should be handled so as not to disrupt existing communication channels between the covered entity and its business associates.

Notification by the business associate is subject to the same timeliness constraints the rule imposes on notification by covered entity. Similarly, a delay in the business associate's provision of notice may be required to satisfied law enforcement considerations. The business associate bears the burden of showing that the proper notification was provided, including that any delay was necessary.

In its notice to the covered entity, the business associate must identify to the extent possible the affected individuals (i.e., those whose PHI has been, or is reasonably believed to have been, breached). Depending on the circumstances, the business associate may immediately notify the covered entity of the breach and, later follow up with any additional required information in a timely manner. HHS recognizes that in some situations a business associate may not be aware of the identity of affected individuals (e.g., when a record storage company that holds hundreds of boxes of paper records discovers that several boxes are missing but is unable to identify the specific individuals whose records were stored in the missing boxes). The language of the rule therefore is not intended to delay the business associate's notification to the covered entity when the covered entity may be in a better position to identify the affected individuals.

HHS also recognizes that a business associate may be in a better position to gather the information that the covered entity is required to include in its notice to affected individuals. As a consequence, the rule requires a business associate provide to the covered entity any such available information, either at the time the business associate notifies the covered entity of the breach or promptly thereafter as the information becomes available. HHS notes that the business associate should provide this information even if it becomes available after the covered entity sends the individual

notices or after the 60-day time period has elapsed. However, HHS cautions that a business associate should not delay in notifying the covered entity of a breach in order to collect information needed for the individual notice.

Additional administrative requirements apply

Covered entities and business associates must develop policies and procedures for complying with the breach notification requirements in the rule and train workforce members on and have sanctions for violations of those policies and procedures. They also must permit individuals to file complaints regarding the policies and procedures and the failure to comply with them. Additionally, the rule prohibits covered entities from requiring individuals to waive their rights under the breach notification provisions as a condition of receiving treatment, payment, and enrollment in a health plan or eligibility for benefits. Covered entities also are prohibited from engaging in intimidating or retaliatory acts against individuals who exercise their rights under the breach notification provision, including the filing of a complaint.

No additional technologies/methodologies specified in HHS' guidance

Unfortunately, the HHS' guidance continues to list *only* encryption and destruction as the technologies and methodologies that covered entities and their business associates can use to render PHI unusable, unreadable or indecipherable to unauthorized individuals, and, therefore, create a "safe harbor" from the federal breach notification requirements. HHS specifically declined to include access controls in the guidance, pointing out that such controls, as well as other security methods such as firewalls, do not "meet the statutory standard of rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals." HHS also declined to include, as the AHA recommended, redaction of paper records as an alternative to destruction because redaction "is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable or indecipherable."

HHS nevertheless emphasizes the benefit of implementing strong access controls to help prevent breaches from occurring. HHS also points out that a loss or theft of information that has been properly redacted may not require notification as required by the rule if the redaction creates information that is no longer PHI (i.e., it meets the HIPAA definition of "de-identified") or would not compromise the security or privacy of the information and, therefore, would not constitute a breach under the rule.

Although it did not substantively modify the guidance, HHS clarified that the guidance "does nothing to modify a covered entity's responsibilities with respect to the [HIPAA] security rule nor does it impose any new requirements upon covered entities to encrypt all protected health information." The AHA had urged HHS to resist requests to convert a voluntary element of HITECH's breach notification provisions into a uniform mandate to encrypt all PHI that would materially and inappropriately alter compliance obligations under the security rule. Thus, if a covered entity decides to use an encryption method or algorithm not specified in the HHS guidance, it may be in compliance with the HIPAA security rule; but it may need to provide the required federal breach notification if a breach of PHI occurs. On the other hand, if a covered entity chooses to follow the HHS

guidance to comply with the HIPAA security rule, it would not need to provide notice if a breach occurs.

HHS' also includes several other clarifications in the guidance related to the forms of information addressed in the National Institute of Standards and Technology (NIST) publications which are referenced in the guidance:

- "Data in motion" includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange.
- "Data at rest" includes data that resides in databases, file systems, flash drives, memory and any other structured storage method.
- "Data in use" includes data in the process of being created, retrieved, updated or deleted.
- "Data disposed" includes discarded paper records or recycled electronic media.

HHS also clarifies that covered entities and business associates should keep encryption keys on a separate device from the data that they encrypt or decrypt to ensure that the keys themselves are not breached.

Finally, HHS adds that NIST plans to include the development of security guidelines for enterprise-level storage devices, such as RAID (redundant array of inexpensive disks) or SAN (storage-attached network) systems, and such guidelines, when available, will be considered future updates to the HHS guidance. HHS anticipates that the first annual update to the guidance will be issued in April 2010.

Hospitals and their business associates will want to examine the revised guidance, including the referenced NIST publications that are available at http://www.csrc.nist.gov/, and determine the extent to which they can adopt the identified technologies and methodologies to secure their PHI and, thereby, create a safe harbor from the federal breach notification requirements. They nevertheless will be required to comply with all other applicable legal requirements, including the federal HIPAA requirement to mitigate, to the extent practicable, any harmful effect of the breach and any state-specific breach notification requirements. **Hospitals and their business associates also will want to implement a process for examining annual updates to HHS' guidance, including assigning specific responsibility for doing so to appropriately knowledgeable staff.**

NEXT STEPS

In the coming weeks, the AHA will hold member conference calls to discuss the rule's requirements and implementation. Watch your inbox for additional information about these calls, including dates and times. We also welcome input from members on the administrative and operational difficulties of implementing the federal breach notification requirements in anticipation of submitting our comments on the interim final rule before the HHS' October 23 deadline. You may direct any comments or questions about the rule's requirements to Lawrence Hughes, AHA assistant general counsel, at lhughes@aha.org or (202) 626-2346. Finally, we encourage members to submit a comment letter to HHS supporting its decision to adopt a risk-based definition of breach.