THE ABA HEALTH LAW SECTION

THE HEALTH LAWYER

## IN THIS ISSUE



**Volume 22, Number 1**
**October 2009**

# THE HITECH BREACH NOTIFICATION RULES: UNDERSTANDING THE NEW OBLIGATIONS

Andrew B. Wachler, Esq.
Amy K. Fehn, Esq.
Wachler & Associates, P.C.
Royal Oak, MI

On August 19, 2009, the Department of Health and Human Services ("HHS") issued an interim final rule with request for comments on the Breach Notification for Unsecured Protected Health Information (the "Interim Final Rule").[1] The Interim Final Rule was mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as part of the American Recovery and Reinvestment Act of 2009 ("ARRA"),[2] which was enacted on February 17, 2009.

The Interim Final Rule sets forth the regulatory requirements for determining when a breach of "unsecured" protected health information has occurred and dictates how, when and to whom such a breach must be reported. The Interim Final Rule also addresses comments and clarifies certain provisions contained in the Guidance and Request for Information issued by HHS on April 17, 2009[3] related to technologies and methods available to "secure" protected health information. While the Interim Final Rule sets forth the obligations for covered entities and business associates of covered entities that are subject to HIPAA,[4] the Federal Trade Commission ("FTC") also issued a final rule imposing similar notification requirements on vendors of personal health records ("PHR"s) and entities that contract with such vendors.

The Interim Final Rule became effective on September 23, 2009. However, HHS has stated that it will not impose sanctions for failure to provide notification of breaches discovered before 180 days from the publication of the rule, i.e., February 22, 2010.[5] HHS has requested additional comments which are due October 23, 2009 and could result in further modifications of the Interim Final Rule in the future.

## Definition of Breach

The Interim Final Rule defines a "breach" as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E of this part [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information."[6] By definition, a use or disclosure that violates the HIPAA Privacy Rule[7] is a prerequisite to the finding of a "breach" pursuant to the Interim Final Rule.[8] So, for example, a

*continued on page 3*

*continued from page 1*

disclosure of information that occurs despite the implementation of reasonable safeguards would not be considered a "breach" for purposes of the Interim Final Rule because there would not be a violation of the Privacy Rule.[9]

**The "Harm Threshold"**

HHS agreed with commenters who urged that the language "compromises the security or privacy of the protected health information" should be viewed as requiring a "harm threshold" before an unauthorized use or disclosure would be considered a "breach" for purposes of the Interim Final Rule.[10] Thus, although a violation of the Privacy Rule is a prerequisite to the finding of a "breach," some uses or disclosures that do violate the Privacy Rule will not be considered a "breach" if the use or disclosure does not "pose a significant risk of financial, reputational, or other harm to the individual."[11] HHS stated that the inclusion of this "harm threshold" better aligned the Interim Final Rule with state breach notification laws and the obligations set forth in the Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, M-07-16 ("OMB M-07-16"), which applies to federal executive departments and agencies.[12]

To determine whether the "harm threshold" has been met, the Interim Final Rule requires covered entities and business associates to conduct and document a fact-specific "risk assessment" whenever an unauthorized use or disclosure occurs.[13] HHS identified the following factors that should be considered when performing the risk assessment:

(1) *The identity of the entity or individual that impermissibly used the information or to whom the information was impermissibly disclosed.* For example, an impermissible disclosure to another entity that has obligations pursuant to the HIPAA Privacy Rule may not pose as great of a threat as a disclosure to a person or entity that does not have the same obligations.[14]

(2) *The steps that were taken to mitigate harm and the immediacy with which such steps were taken.* For example, the covered entity may mitigate harm by taking immediate steps to obtain satisfactory assurances that the information will not be used or further disclosed, such as through confidentiality agreements or agreements to destroy the information.[15]

(3) *Whether the information was returned before being accessed.* For example, if a laptop was stolen, but later returned and it is determined based on forensic analysis that it was not accessed, the "harm threshold" would likely not be met. HHS noted, however, that covered entities and business associates should not delay notification in the hope that a lost or stolen computer may be recovered.[16]

(4) *The type and amount of information disclosed.* For example, the unauthorized disclosure of a name and general statement that the individual received services at a certain hospital might not be deemed to meet the "harm threshold." However, information regarding specific services received, admission to a specialized facility, or information that could increase the risk of identity theft creates a greater likelihood of harm. HHS urged that many forms of health information, not just those related to mental health or sexually transmitted diseases, could pose a risk of employment discrimination and should also be considered "sensitive."[17]

With regard to whether the "harm threshold" has been met, HHS also suggested that covered entities review the examples set forth in OMB M-07-16.[18] As part of the Identity Theft Task Force,[19] OMB M-07-16 requires federal agencies to develop and implement breach notification policies. Examples of "possible harms" discussed in OMB M-07-16 include: the potential for blackmail; the disclosure of private facts; mental pain and emotional distress; the disclosure of address information of victims of abuse; the potential for secondary uses of the information that could result in fear or uncertainty; or unwarranted exposure leading to humiliation or loss of self-esteem.[20] OMB M-07-16 also provides examples of the types of data that would most likely pose a risk of identity theft, such as social security numbers, account numbers, dates of birth, passwords, and mother's maiden names.[21]

**Special Treatment of Limited Data Sets**

The Interim Final Rule provides that an unauthorized use or disclosure of information in a limited data set will not meet the "harm threshold," so long as dates of birth and zip codes are removed. If dates of birth and zip codes are not removed, a covered entity or business associate would need to complete a fact-specific risk assessment, but might still determine that the "harm threshold" is not met because the risk of re-identification is low.

To create a limited data set that falls within this narrow exception, the sixteen identifiers contained in 45 CFR 164.514(e)(2)[22] must be removed, as well as the birth dates and zip codes. Although the HIPAA Privacy Rule only permits disclosure of information in limited data sets for healthcare operations, research or public health activities and requires that a limited data set can only be shared pursuant to a data use agreement, a covered entity does not need to meet these requirements to take advantage of the above exception to the definition of "breach." In other words, a covered entity that impermissibly discloses information that has been stripped of the 16 direct identifiers as well as zip codes and dates of birth will not have to report the disclosure as a breach, regardless of the purpose for which the information was used or disclosed and regardless of whether a data use agreement was in place.[23]

**Exceptions**

The HITECH Act contained three statutory exceptions to the "breach" definition, all of which are generally mirrored in the Interim Final Rule.

*continued on page 4*

*continued from page 3*

The first exception to the "breach" definition applies to certain uses or disclosures by a covered entity's "workforce"[24] members, i.e., persons acting under the authority of the covered entity or business associate. Specifically, the exception applies when the use or disclosure was made in good faith, was within the scope of the disclosing individual's authority and does not result in further violation of the Privacy Rule.[25] While the HITECH Act used the term "employee," the Interim Final Rule expands this exception to all "workforce" members in order to encompass additional individuals working under the covered entity's control, such as trainees and volunteers.[26]

HHS provided two contrasting examples to illustrate when this exception may apply. The first example is a billing employee who receives and opens a misdirected e-mail containing protected health information from a nurse within the same entity. The billing employee immediately deletes the e-mail and alerts the nurse of the error. In this example, the billing employee is acting in good faith, is acting within his or her scope of authority and does not make any further use or disclosure of the protected health information in violation of the Privacy Rule. Thus, the exception would apply. In contrast, a receptionist who is not authorized to view protected health information, but accesses such information in order to learn about a friend's treatment is an example of an individual who is not acting in good faith or within the scope of authority and to whom the exception would not apply.[27]

The second exception to the "breach" definition applies to inadvertent disclosures from one person who is authorized to access protected health information to another person who is also authorized to access protected health information within the same covered entity, business associate, or organized healthcare system.[28] While the HITECH Act originally limited this exception to persons who were "similarly situated," commenters sought clarification and HHS responded by focusing on whether the individuals are authorized to access protected health information, regardless of whether the type or degree of access is the same.[29] For example, an inadvertent disclosure to a billing person with limited access to protected health information from a physician with more expansive access to protected health information would meet the exception.[30] The HITECH Act also limited this exception to disclosures within the same "facility."[31] However, in response to concerns that the exception was too narrow and to "more clearly capture the intent of the statute," the Interim Final Rule changes "same facility" to "same covered entity, business associate, or organized health care arrangement."[32] Because an organized health care arrangement may include a hospital and its staff physicians, this exception may, for example, apply to an inadvertent disclosure from a hospital nurse to a physician with staff privileges at the hospital.[33]

The third exception to the "breach" definition applies to "a disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information."[34] The Interim Final Rule's language generally mirrors that of the HITECH Act, except that it adds "good faith belief."[35]

For clarification, HHS included two examples in which this exception would apply. The first example is where a covered entity, due to a lack of reasonable safeguards, inadvertently sends explanations of benefits ("EOB"s) to the wrong individuals. If some of the EOBs are returned by the post office unopened, the covered entity could conclude in good faith that the addressees could not possibly have retained the information. The second example involves a nurse who mistakenly gives discharge papers to the wrong patient. If the nurse can conclude in good faith that the patient who received the wrong discharge papers could not have reasonably read and retained the information, this exception would apply.[36]

#### Burden of Proof

For each of these three exceptions, or for a determination that the "harm threshold" has not been met, the covered entity or business associate has the burden of showing that a breach notification is not required.[37] HHS contemplates that for any violation of the Privacy Rule, a business associate or covered entity must first determine whether the "harm threshold" is met, i.e., whether there is a significant risk of financial, reputational, or other harm to the individual. The covered entity or business associate must then determine whether any of the three exceptions discussed above are applicable.[38] Such determinations must be documented, retained for six years and made available to HHS upon request.[39] Additionally, covered entities and business associates will need to make this determination quickly. As discussed in more detail below, timeframes related to the notification requirements are calculated from the date that the incident is known or reasonably should have been discovered, not from the date that the determination is made regarding whether the Privacy Rule violation rises to the level of a "breach."[40]

## Determining When a "Breach" Triggers Notification Obligations

#### "Unsecured" Protected Health Information

Not all uses and disclosures that meet the "breach" definition set forth above trigger notification obligations. Rather, breach notification obligations apply only to breaches of "unsecured" protected health information.[41] "Unsecured" protected health informa-

tion is defined as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary."[42] "Unsecured" protected health information can be in any form or medium, including electronic, paper or oral communications.[43]

Guidance specifying technologies and methodologies that can be used to render protected health information "unusable, unreadable, or indecipherable" was originally published on April 17, 2009.[44] The Interim Final Rule updates this guidance based, in part, on comments received in response to the April publication. HHS' commentary in the Interim Final Rule clarifies that the guidance does not create new responsibilities for covered entities pursuant to the Security Rule. Rather, the guidance provides a mechanism by which a covered entity can secure protected health information to avoid the breach notification requirements in the event that the protected health information falls into the hands of an unauthorized person.[45]

One way that protected health information can be rendered "unusable, unreadable, or indecipherable" is through the use of encryption, so long as the confidentiality of the decryption process or key has not been breached.[46] In order to determine whether an encryption process meets the standard set forth in the guidance, the Interim Final Rule incorporates by reference the processes developed by the National Institute of Standards and Technology ("NIST"), including NIST guides for "data at rest" and "data in motion."[47] HHS clarifies that "data at rest" includes data that resides in structured storage methods, such as databases, file systems, flash drives and memory. "Data in motion" includes data that is moving through a network, including a wireless network, such as data moving through e-mail or structured electronic interchanges.[48]

Protected health information can also be rendered "unusable, unreadable, or indecipherable" by destroying the media on which the protected health information is stored.[49] Hard copy media such as paper and film can be destroyed by shredding or destroying the media in a manner that renders it unreadable and not subject to reconstruction.[50] With regard to electronic media, the media must be cleared, purged or destroyed consistent with NIST Guidelines and in such a manner that it cannot be retrieved.[51]

Although commenters urged HHS to consider redaction as an acceptable method for rendering paper records "unusable, unreadable, or indecipherable," HHS declined to do so.[52] HHS did note, however, that redacting paper documents might be considered a valid method of creating "de-identified"[53] information, thus removing the information from the definition of protected health information or creating a limited data set that may meet the narrow exception discussed more fully above. In addition, HHS noted that the use of redaction might be sufficient to reduce the risk of harm to the individual so as to fall below the "harm threshold" discussed above.[54]

## Notification Requirements

Once the covered entity or business associate has determined that there has been a "breach" and that the protected health information at issue was "unsecured," the covered entity or business associate must determine what notification requirements apply to the situation. Documentation of all notifications must be retained for six years pursuant to the administrative requirements in the HIPAA Privacy Rule[55] and must be made available to HHS upon request.[56] Covered entities and business associates have the burden of proof to demonstrate that all notifications were made in a timely manner and in accordance with the requirements of the Interim Final Rule.[57]

### Notification to Individuals

When a covered entity has a reasonable belief that an individual's protected health information has been involved in a breach, the covered entity has an obligation to notify each affected individual personally.[58] The notice must be provided by first class mail to the individual's last known address unless the individual agreed to receive it electronically.[59] The notification can be provided in multiple mailings if all information is not available at the time of the initial notice.[60] For minors or incapacitated individuals, notice can be provided to the "personal representative" as defined by the HIPAA Privacy Rule.[61] If the covered entity knows that the affected individual is deceased, the notice should be sent to either the individual's next of kin or personal representative if the covered entity has the next of kin or personal representative's contact information.[62]

To the extent that the information is available, the notification to an affected individual must include the following elements:[63]

(1) *A brief description of what happened.* The covered entity should include the date of the breach and the date of discovery of the breach, if known.[64]

(2) *A description of the types of unsecured information that were involved in the breach.*[65] Examples of the types of information that should be listed, if involved in the breach, include full name, social security number, date of birth, home address, account number, diagnosis, and disability code.[66] Actual protected health information should not be included. For example, the notice should state that the individual's social security number was involved in the breach, but should not list the actual social security number. In addition, covered entities should avoid including any sensitive information in the notification.[67]

(3) *Any steps individuals should take to protect themselves from potential harm resulting from the breach.*[68] For example, in situations in which credit card information is involved, the notice should recommend that affected individuals contact credit card companies or may

*continued on page 6*

*continued from page 5*

include information on how to contact credit bureaus or obtain credit monitoring services.[69]

(4) *A brief description of what the covered entity involved is doing to investigate, mitigate harm to individuals, and protect against further breaches.*[70] For example, if a theft of unsecured information is suspected, the fact that the covered entity has filed a police report should be included in the notification. Any disciplinary actions against employees involved in the incident should also be included.[71] It is important to note that HHS chose to use the term "mitigate harm to individuals" in the Interim Final Rule, rather than "mitigate losses" as used in the HITECH Act. This was done to clarify that steps should be taken to protect the individual from all types of harm, not just economic loss.[72]

(5) *Contact procedures for individuals to ask questions or learn additional information, including either a toll-free telephone number, e-mail address, website or postal address.*[73]

The Interim Final Rule also requires that the notification be "written in plain language."[74] In order to satisfy this requirement, covered entities should write the notice at a proper reading level, use clear language and syntax, and not include extraneous material that might "diminish the message."[75] While some commenters recommended imposing a page limit in order to ensure that the notice is not overly technical or complex, HHS stated that it did not wish to hinder a covered entity's ability to include all information that it believes would be helpful to the individual.[76] HHS also noted that certain covered entities may be subject to additional laws that would require the notice to be interpreted into different languages or made accessible to individuals with sight impairment or other disabilities.[77]

Subject to exceptions for delays requested by law enforcement, which are more fully discussed below, the Interim Final Rule requires a covered entity to send notification of a breach to an affected individual without "unreasonable delay" and no later than sixty calendar days from the date that the covered entity discovers the incident that is ultimately determined to constitute a breach.[78] As discussed above, when an incident is discovered, a covered entity may be uncertain as to whether it rises to the level of a breach. However, any risk assessment must also be completed without "unreasonable delay."[79] In order to avoid reporting obligations, an investigation and risk assessment must be conducted swiftly. An example of a situation that would not trigger reporting requirements is a laptop that was reported as stolen but discovered the next day in another secure office within the covered entity.[80] However, as discussed previously, HHS makes it clear that covered entities cannot delay notification based on the hope of finding lost or stolen information.[81]

Likewise, while investigation of a breach may be necessary in order to gather the required information for the notice to the individual, such investigation also must be completed without "unreasonable delay."[82] In comments to the Interim Final Rule, HHS emphasized that 60 calendar days is an outer limit. For example, when a covered entity has compiled all of the information necessary to provide notification to affected individuals on the 10th day following a breach but waits until the 60th day to actually provide notification, this would be considered an "unreasonable delay."[83]

**Urgent Situations**

In certain situations, a covered entity may determine that misuse of protected health information is imminent. In these situations, the covered entity may make additional notice via telephone or other means.[84] In comments to the Interim Final Rule, HHS emphasized that this "urgent notice" is in addition to, and not in lieu of, the written notice requirement.[85] It should also be noted that such urgent notice is permissive, rather than required by the regulations. However, it might be considered necessary by the HIPAA Privacy Rule's requirement to mitigate harm.[86]

**Substitute Notice**

If a covered entity does not have sufficient contact information or has out-of-date contact information for some or all of the individuals affected by a breach, the covered entity must provide a "substitute notice," which is an alternate form of notice that is "reasonably calculated to reach the individual."[87] When substitute notice is required, it should be provided as soon as reasonably possible after the covered entity determines that it has insufficient or out-of-date contact information.[88] However, in cases in which affected individuals are known to be deceased and the covered entity does not have sufficient contact information for the personal representative or the next of kin, the covered entity will not be required to supply substitute notice.[89]

If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be accomplished with an alternative form of written notice, telephone notice or notice by other means.[90] By way of example, HHS stated that it would be acceptable to contact an individual by e-mail if the individual's postal address was out-of-date, even if the individual had not given prior permission to be contacted by e-mail.[91] Similarly, the individual could be contacted by telephone. HHS cautioned, however, that covered entities should be cautious as to the amount and sensitivity of information shared when providing substitute notice. For example, messages on answering machines should be limited to a statement that the covered entity has a very important message for the individual.[92]

Where there are greater than 10 individuals for which there is insufficient

or out-of-date contact information, the covered entity must provide substitute notice by posting a conspicuous notice on the covered entity's web site home page or in a print or broadcast medium that is a "major media outlet" in the geographic areas where individuals likely reside. The notice must include a toll-free telephone number that will remain active for at least 90 days from the time of the posting so that an individual can call to find out whether his or her protected health information was affected by the breach.[93]

If the covered entity chooses to include the notice on its home page, the notice must be conspicuous and must remain posted for 90 days. "Home page" means either the home page of the covered entity's web site or a landing or login page for individuals who have set up accounts with the covered entity. If some of the information required by the notice must be accessed via a hyperlink, the hyperlink must be prominent and noticeable and worded to convey the nature and importance of the information.[94]

The determination as to whether a broadcast or print medium is a "major media outlet" for the geographic area is fact-specific and depends on the geographic area where the affected individuals are likely to reside as well as whether the selected media outlet is reasonably calculated to reach such individuals. For example, if affected individuals are likely to reside in a rural area, a local major newspaper might be reasonably calculated to reach those individuals. However, if the affected individuals are likely to live in a major metropolitan area, a publication that serves the entire metropolitan area or the entire state might be more likely to reach the affected individuals. In some circumstances, the use of multiple media outlets might be required, especially where affected individuals are likely to reside in multiple states.[95]

In response to commenters' concerns regarding the potential burden of fielding calls from the toll-free number that is required to be provided by the substitute notice, HHS noted that covered entities may limit the volume of calls by including sufficient information in the notice itself or on a web site which would allow individuals to determine whether their information was included in the breach.[96] Although HHS did not elaborate on this suggestion, the covered entity must also comply with the HIPAA Privacy Rule when posting such information. Thus, information such as names or medical records would not be a permissible means for listing impacted individuals. The covered entity could, however, state that the breach involved individuals with last names beginning with certain letters or individuals who received care at the covered entity between a range of dates.

HHS also suggested that it may be less costly and onerous in some circumstances for covered entities to attempt to update the affected individuals' contact information rather than providing substitute notice.[97] If the information can be updated to the extent that less than 10 individuals with out-of-date or insufficient information remain, the requirement for substitute notice via web site or media may be avoided and other, less burdensome, forms of substitute notice could be used.

**Notification to Media**

In situations in which the protected health information of more than 500 individuals within a state or jurisdiction is affected, the covered entity must provide notice to a prominent media outlet within that state or jurisdiction.[98] The term "state" includes the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.[99] HHS clarified that "jurisdiction" is defined as a geographic area smaller than a state, such as a county, city or town.[100] This notification is in addition to, and not a substitute for, the individual notice or substitute notice discussed above and should include the same content as the individual notice.[101]

HHS clarified that the number of individuals from a single state or jurisdiction will be the determining factor, even if the aggregate number of affected individuals spread across multiple states is greater than 500. For example, if a breach impacts 600 individuals, with 200 individuals residing in Virginia, 200 residing in the District of Columbia and 200 residing in Maryland, media notification would not be required. However, in this scenario, individual notification would still be required, as well as notice to the Secretary of HHS, as more fully discussed below.[102]

As with the publication of substitute notice, the determination of what constitutes a "prominent media outlet" is fact-specific and depends on the state or jurisdiction affected. For example, if all of the affected individuals reside in a particular city, then the notification should be provided to a prominent media outlet serving that city. On the other hand, if the affected individuals are from across the state and not from any particular city or county, the notice should be published in a media outlet serving the entire state.[103]

Where media notification is required, it must be provided within the same timeframe as notice to the individual, i.e., "without unreasonable delay" and no more than sixty calendar days from the discovery of the incident that is determined to be a breach.[104]

**Notification to the Secretary**

Covered entities are also required to report all breaches to the Secretary of HHS.[105] If a covered entity discovers a breach of unsecured protected health information involving more than 500 individuals, the entity must report the breach to the Secretary "immediately" and in accordance with instructions that will be posted on the HHS website.[106] Unlike media notification, there is no requirement that the 500 individuals reside in the same state or jurisdiction. A list of covered entities that report breaches involving greater than 500 individuals will be posted on the HHS website.[107]

Breaches involving less than 500 individuals must be tracked, even if they

*continued on page 8*

*continued from page 7*

involve only a single individual, but are to be kept in a log and reported to the Secretary annually no more than 60 days after the end of the calendar year.[108] HHS will also post instructions for the submission of annual reports on its website.[109] For calendar year 2009, only breaches occurring after September 23, 2009 (the effective date of the Interim Final Rule) must be reported.[110]

### Notification by Business Associate to Covered Entity

A business associate that discovers a breach of unsecured protected health information must notify the covered entity "without unreasonable delay" and no later than 60 days from the discovery of the breach.[111] The notification to the covered entity must include, to the extent possible, the identification of each individual whose information was affected, as well as any other information that the covered entity is required to include in its notification to the individual.[112]

HHS included the language "to the extent possible" to address situations in which the business associate might not know the identification of the individuals. For example, if a record storage facility discovers that certain boxes are missing, the covered entity might be in the better position than the storage facility to determine the identity of the individuals whose records were contained in the box.[113]

HHS also noted that nothing in the Interim Final Rule is intended to interfere with the ability of covered entities and business associates to contractually establish their respective obligations. For example, the parties may determine that the business associate is in the best position to provide notification to individuals, and may require this via contract. HHS does, however, encourage the parties to ensure that the individual does not receive notice from both the covered entity and the business associate.[114] If a covered entity decides to give a business associate the individual notification reporting obligation, the covered entity should retain the responsibility for conducting the "risk assessment" to determine if notification is needed.

## Factors Impacting Timeliness of Notification

### Discovery: Starting the Clock

The "discovery" of a breach "starts the clock" for purposes of determining timeliness of notification by a covered entity or a business associate.[115] A breach is not treated as discovered until the date that the incident is actually discovered by the covered entity or business associate or the date that it would have been known to the covered entity or business associate through the exercise of "reasonable diligence."[116] Thus, covered entities and business associates should have reasonable systems in place to aid in the discovery of breaches.[117] "Reasonable diligence" is defined by the HIPAA Enforcement Rule as the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."[118] The Interim Final Rule further clarifies that in situations involving discovery by workforce members and business associates, the federal common law of agency will apply to determine whether such discovery should be imputed to the covered entity.[119] Because knowledge of a breach by certain workforce members and business associates may therefore be imputed to a covered entity, it is very important that covered entities adequately train these individuals and entities as to their reporting obligations.[120]

Where business associates are considered to be independent contractors rather than agents, the covered entity is not deemed to have knowledge of the breach until the business associate notifies the covered entity.[121] Thus, covered entities may wish to analyze their relationships with business associates to determine whether such business associates would be considered "agents" of the covered entity in accordance with the federal common law of agency. However, as noted above, the Interim Final Rule grants discretion to covered entities and business associates to delineate by contract how the notification requirements will be implemented. Thus a business associate's obligations regarding breach notification should be set forth clearly in the business associate agreement.[122] Even if business associate agreements contain general language providing for automatic revision in the event of changes in the HIPAA regulations, covered entities should consider revising the existing agreements to more fully address each party's notification obligations, including the timing of such notifications and the consequences for failing to notify.[123]

With regard to media notices or immediate notification to the Secretary, HHS noted that there may be situations where a breach of unsecured protected health information occurring at a business associate will involve the records of multiple covered entities. In these situations, if there are less than 500 affected individuals from any single covered entity, no notification is required to the media or immediate notification to the Secretary. The covered entity would, however, need to track these breaches for inclusion in its annual report to the Secretary. In addition, where the business associate cannot determine which covered entity's information has been breached, the covered entities may consider having the business associate provide notification to the media on behalf of all covered entities.[124]

### Law Enforcement Delay

The Interim Final Rule allows for a temporary delay of notification if a law enforcement official states orally that a notification would impede a criminal investigation. The covered entity or business associate must document the oral statement and identity of the official, and may only delay notification for

no more than 30 days. If, however, the law enforcement officer formally states in writing that a delay is necessary so as not to impede a criminal investigation or cause damage to national security, otherwise required notifications can be delayed for the time specified by the law enforcement official.[125] HHS retained the definition of "law enforcement official" contained in the HIPAA Privacy Rule, but moved the definition to 45 CFR §164.103 so that it will be also be applicable to the Interim Final Rule.[126]

## Preemption of State Law

HHS noted that the general HIPAA preemption provision found at 45 CFR §160.203 will apply to the breach notification regulations and that none of the exceptions contained in that section will be applicable to the Interim Final Rule.[127] 45 CFR §160.203 generally provides that any HIPAA requirement that is "contrary to" state law will preempt the state law. A state law is considered "contrary" if a covered entity finds it impossible to comply with both HIPAA and the state law or if the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the breach notification provisions."[128]

HHS also noted that, in general, it believes covered entities will not have a problem complying with both state law and the Interim Final Rule. For example, if a state breach notification rule requires notification to the individual within five days following a breach, that notification would comply with the time frame of the Interim Final Rule as well. If all of the information required by the Interim Final Rule was not available at the time that the state required notification was made, the information could be provided in multiple mailings as permitted by the Interim Final Rule.[129]

Likewise, if a state breach notification rule requires inclusion of elements not required by the Interim Final Rule, the inclusion of these additional elements would not violate the Interim Final Rule. The Interim Final Rule does not preclude the use of additional elements and is flexible as far as how the elements can be described.[130]

## Relationship with FTC Health Breach Notification Rule

ARRA also required the FTC to issue regulations governing breach notification for vendors of PHRs and other non-HIPAA covered entities.[131] These regulations ("the FTC Rule") were issued on August 18, 2009[132] and apply to vendors of PHRs,[133] PHR related entities,[134] and third party service providers.[135] The FTC Rule breach notification requirements are similar, but not identical, to those of the Interim Final Rule. For example, a breach involving greater than 500 individuals must be reported to the FTC within ten business days.[136] In contrast, the Interim Final Rule requires a report to the Secretary of HHS concurrently with notification to the individual, up to 60 days from the discovery of the breach.[137]

In the Interim Final Rule, HHS noted that there may be circumstances where a PHR vendor is covered by both the Interim Final Rule and the FTC Rule. Specifically, the vendor will be considered in compliance with the FTC Rule when appropriate notifications are made pursuant to the Interim Final Rule in the following limited circumstances:

(1) The PHR vendor provides notice to individuals on behalf of a HIPAA-covered entity;

(2) The PHR vendor has dealt directly with these individuals in managing their PHR accounts; or

(3) The PHR vendor provides notice to all of its customers at the same time (regardless of whether the customers are HIPAA-covered entities or non-HIPAA-covered entities).[138]

The FTC offered several examples to illustrate situations where the FTC Rule and the Interim Final Rule may overlap and indicated an expectation that the notification response should be coordinated so that consumers receive only one notification per breach.[139] In the first example, a PHR vendor provides PHRs to the public through its own web site and also to a HIPAA-covered entity as a business associate of the covered entity. With regard to patients of the HIPAA-covered entity, the vendor would only be required to notify the covered entity, rather than notifying the individuals directly. However, the vendor would be required to provide individual notice to its private clients pursuant to the FTC Rule. Because the PHR vendor has a direct relationship with all of the affected individuals, it could contract with the covered entity to provide the individual notice required by the Interim Final Rule. The FTC encourages such contractual relationships so that the individuals receive only one notice, both entities fulfill their obligations and the process is simplified.[140]

Another example illustrates the problems that occur when a PHR vendor does not properly maintain and update lists that separate individuals that it enrolls privately from those that it enrolls as a business associate of a covered entity. If a patient disaffiliates with the covered entity but remains a customer of the PHR vendor, there may be confusion as to which entity is obligated to send notice, resulting in failure to provide notice at all or providing multiple notices for one breach. This illustrates another situation in which an agreement obligating the business associate to directly send all notices would simplify the process.[141]

The FTC further elaborated on the relationship between the FTC Rule and the Interim Final Rule with regard to HIPAA-covered entities. Although HIPAA-covered entities are specifically excluded from the definition of a PHR vendor, the FTC refused to specifically exclude doctors from the FTC rule. The FTC described an example of a limited situation in which a doctor may be subject to the FTC Rule. Where a non-practicing doctor creates or offers PHRs

*continued on page 10*

*continued from page 9*

to the public as part of a start-up venture separate from his or her medical practice, he or she would be required to comply with the FTC Rule. On the other hand, a practicing physician who offers PHRs to his or her patients would be a HIPAA-covered entity and would be governed by the Interim Final Rule rather than the FTC Rule.[142]

Like the Interim Final Rule, the FTC Rule is effective 30 days from the date of publication, i.e., September 24, 2009. However, like HHS, the FTC will not enforce the rule for the first 180 days following publication, i.e., February 22, 2010.

## Sanctions

Violation of the Interim Final Rule, as with any violation of HIPAA, could result in the imposition of penalties pursuant to Section 13410 of the HITECH Act, which increased HIPAA penalties effective February 17, 2009.[143] Currently, violations of any provision of HIPAA, including the breach notification requirements, due to "willful neglect", are punishable by at least $10,000 per violation and up to $50,000 per violation, with an annual maximum of at least $250,000 and no greater than $1,500,000.[144] Thus, choosing to ignore the breach notification requirements could be very costly for covered entities and business associates, even though, as discussed below, compliance with the notification requirements is essentially an admission of a Privacy Rule violation which also may lead to sanctions and potential liability under state law.

In addition, because of the expanded authority given to state attorneys general through the HITECH Act, the Interim Final Rule, as with all provisions of HIPAA, can be enforced by the attorney general of a state or the Office of Civil Rights of HHS.[145]

## Conclusion

The Interim Final Rule creates significant obligations for covered entities and their business associates. Covered entities and business associates should immediately begin drafting policies and procedures to ensure that internal reporting mechanisms are in place to report breaches and to ensure that employees and other workforce members are properly trained. Policies and procedures setting forth the specific requirements and timeframes for the various notification obligations should also be implemented.

Covered entities and business associates should include counsel in decisions related to conducting and documenting the "risk assessment" to determine whether the "harm threshold" has been reached. Because this will dictate whether the breach needs to be reported, many considerations will need to be carefully weighed, including the covered entity's duty to mitigate harm pursuant to the Privacy Rule, state law requirements, and the liability exposure resulting from notifications to individuals, the media and the Secretary of HHS. Because such notifications are admissions of violations of the Privacy Rule, they will significantly increase liability exposure for covered entities, not only because of the heightened penalties found in the HITECH Act, but also because the notifications will alert individuals and attorneys to potential claims based on breach of privacy or medical malpractice.

Now, more than ever, covered entities should be focused on bolstering HIPAA compliance efforts, including reviewing policies and re-educating staff on all of the requirements of the HIPAA Privacy Rule.

Because the HITECH Act creates direct liability for business associates who violate HIPAA provisions, business associates should not rely solely on covered entities to define their responsibilities. Companies and individuals who do business with covered entities should analyze their relationships to determine whether they will be considered a business associate pursuant to the HIPAA regulations and to determine their corresponding obligations, including those associated with the Interim Final Rule.

Covered entities should also analyze business associate agreements to determine whether the business associate could be considered an "agent" of the covered entity pursuant to the federal common law of agency. Because it is undesirable to have a business associate's knowledge of a breach imputed to the covered entity, covered entities may wish to include language in business associate agreements or underlying agreements specifying that the agreement is not intended to establish an agency relationship.

Covered entities may also wish to add language to business associate agreements imposing reporting obligations that are more stringent than those required by the Interim Final Rule. For example, if a business associate is determined to be an agent of the covered entity and its knowledge of the breach is imputed to the covered entity, the covered entity would want the business associate to be contractually obligated to report breaches to the covered entity immediately, rather than within the 60 day timeframe set forth in the Interim Final Rule, so that the covered entity has time to fulfill its reporting obligations. In addition, the covered entity may wish to seek indemnification from the business associate for breaches or failure to notify the covered entity of such breaches.

Finally, entities that provide PHRs or affiliate with vendors of PHRs should carefully determine their obligations under both the Interim Final Rule and the FTC Rule.

**Andrew B. Wachler** is the principal of Wachler & Associates, P.C. He graduated Cum Laude from the University of Michigan and Cum Laude from Wayne State University Law School.

Mr. Wachler has been practicing healthcare and business law for over 25 years. Mr. Wachler counsels healthcare providers and organizations nationwide in a variety of legal matters. He writes and speaks nationally to professional organizations and other entities on a variety of healthcare legal topics.

Mr. Wachler is a member of the State Bar of Michigan, Health Care Law Section, American Bar Association, Health Law Section and American Health Lawyers Association. He is also a Member of *The Health Lawyer's* Editorial Board.

He may be reached at *awachler@wachler.com*.

**Amy K. Fehn** is an attorney at Wachler & Associates, P.C. Ms. Fehn graduated Summa Cum Laude from Kent State University and Summa Cum Laude from the University of Akron School of Law.

Ms. Fehn is a former registered nurse who has been counseling healthcare providers for the past eleven years on regulatory and compliance matters. Ms. Fehn is a member of the American Health Lawyers Association, as well as the State Bar of Michigan, Health Care Law Section, where she served as a member of the HIPAA Task Force. She also co-authored workbooks on both HIPAA Privacy and Security and has presented on HIPAA issues to local and national organizations.

She may be reached at *afehn@wachler.com*.

## *Endnotes*

1 74 Fed. Reg. 42740 (August 24, 2009) available on the internet at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

2 Pub. L. 111-5. The HITECH Act is Title XIII of Division A and Title IV of Division B of ARRA.

3 See 74 Fed. Reg. 19006 (April 27, 2009), Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information.

4 Health Insurance Portability and Accountability Act of 1996, P. L. 104-191. Note that this was the first amendment to the HIPAA regulations since they were enacted in 1996.

5 74 Fed. Reg. 42757.

6 45 CFR §164.402.

7 The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164. For the Final Privacy Rule with comments, see 65 Fed. Reg. 82462 (December 28, 2000), accessible on the internet at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf. For the Final Modifications to the Privacy Rule, see 67 Fed. Reg. 5312 (August 14, 2002), accessible on the internet at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulepd.pdf.

8 74 Fed. Reg. 42743.

9 74 Fed. Reg. 42744.

10 *Id.* HHS noted that the requirement for a "harm threshold" would also align the Final Interim Rule more closely with state breach notification statutes.

11 45 CFR §164.402(1). In comments to the Interim Final Rule, HHS also noted that the Security Rule, while providing for administrative, physical and technical safeguards of protected health information, does not govern "uses and disclosures." Therefore, a violation of the Security Rule does not constitute a "breach" as defined by the Interim Final Rule unless there is an associated improper "use or disclosure" which violates the Privacy Rule. See 74 Fed. Reg. 42744.

12 OMB Memorandum M-07-16, available on the internet at: http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf (last accessed September 8, 2009).

13 74 Fed. Reg. 42744.

14 74 Fed. Reg. 42745.

15 74 Fed. Reg. 42745.

16 *Id.*

17 *Id.*

18 Office of Management and Budget Memorandum M-07-16, available on the internet at: http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf (last accessed September 8, 2009).

19 The Identity Theft Task Force was established by Executive Order 13402 and was charged with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions that can be taken by public and private sectors. See OMB M-07-16 at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf and the Task Force's report at http://www.idtheft.gov/reports/IDTReport2008.pdf.

20 OMB Memorandum M-07-16, available on the internet at: http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf (last accessed September 8, 2009) at p. 15.

21 *Id.*

22 45 CFR 164.514(e)(2) requires removal of all of the following in order to create a limited data set: names, postal address information other than town or city, state and zip code, telephone and fax numbers, email addresses, social security numbers, medical records numbers, beneficiary numbers, account numbers, certificate/license numbers, VIN and serial numbers, license plate numbers, device identifier and serial numbers, URLs, IP addresses, biometric identifiers (such as voice and finger prints), full face and comparable photographic images.

23 74 Fed. Reg. 42746.

24 "Workforce" is defined in 45 CFR §160.103 as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

25 45 CFR §164.402(2)(i).

26 74 Fed. Reg. 42747.

27 74 Fed. Reg. 42747.

28 45 CFR §164.402(2)(ii).

29 74 Fed. Reg. 42747.

30 *Id.*

31 *Id.*

32 *Id.*

33 74 Fed. Reg. 42748. *See* 45 CFR §164.103 for definition of "organized health care arrangement".

34 45 CFR §164.402(2)(iii).

35 74 Fed. Reg. 42748.

36 74 Fed. Reg. 42748.

37 45 CFR §164.414(b).

38 74 Fed. Reg. 42748.

39 45 CFR §164.414(a).

40 74 Fed. Reg. 42748-42749.

41 45 CFR §164.404(a).

42 45 CFR §164.402.

43 74 Fed. Reg. 42748.

44 74 Fed. Reg. 19006 (published April 27, 2009).

45 74 Fed. Reg. 42741.

46 74 Fed. Reg. 42742. The definition of "encryption" for purposes of the Guidance mirrors the definition set forth in the HIPAA Security Rule at 45 CFR §164.304 which defines encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." The Guidance notes that, in order to protect the

*continued on page 12*

*continued from page 11*

confidentiality of the process or key, the decryption tools should be stored on a separate device or at a separate location.

47 74 Fed. Reg. 42742. Encryption Processes identified for "data at rest" must be consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*. Encryption processes identified for "data in motion" must be consistent with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, 800-77 *Guide to IPsec VPNs*, or 800-113 *Guide to SSL VPNs* or others which are Federal Information Processing Standards (FIPS) 140-2 validated. These guides are available at http://www.csrc.nist.gov/.

48 74 Fed. Reg. 42742.

49 74 Fed. Reg. 42743.

50 74 Fed. Reg. 42743.

51 Specifically, destruction must be consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, available at http://www.csrc.nist.gov/.

52 74 Fed. Reg. 42742.

53 "De-identification" is defined in 45 CFR §164.514(a) and the implementation specifications are contained in 45 CFR §164.514(b). De-identification can generally be accomplished by analysis by a professional statistician or by removing all of the following identifiers: names, geographic subdivisions smaller than a state, elements of dates, telephone and fax numbers, email addresses, social security numbers, medical records numbers, beneficiary numbers, account numbers, certificate/license numbers, VIN and serial numbers, license plate numbers, device identifier and serial numbers, URLs, IP addresses, biometric identifiers (such as voice and finger prints), full face and comparable photographic images, and any other unique identifying number, characteristic, or code.

54 74 Fed. Reg. 42742.

55 45 CFR §164.530(j).

56 45 CFR §160.310.

57 45 CFR §164.414 (b).

58 45 CFR §164.404(a).

59 74 Fed. Reg. 42750. Although the Interim Final Rule does not specify, permission to provide notice electronically would presumably be provided prior to the breach, possibly as part of a request by the patient to receive all correspondence electronically.

60 45 CFR §164.404(d)(1).

61 "Personal Representative" is defined by the Privacy Rule in 45 CFR §164.502(g).

62 While the HITECH Act language would only have required notice to the individual's "next of kin", HHS noted that covered entities may have contact information for the personal representative rather than the "next of kin". See 74 Fed Reg. 42750; 45 CFR §164.404(d)(1)(ii).

63 45 CFR §164.404(c)(1).

64 45 CFR §164.404(c)(1)(A).

65 45 CFR §164.404(c)(1)(B).

66 *Id.*

67 74 Fed. Reg. 42750.

68 45 CFR §164.404(c)(1)(C)

69 74 Fed. Reg. 42750.

70 45 CFR §164.404(c)(1)(D).

71 74 Fed. Reg. 42750.

72 74 Fed. Reg. 42768.

73 45 CFR §164.404(c)(1)E).

74 45 CFR §164.404(c)(2).

75 74 Fed. Reg. 42750.

76 *Id.*

77 *Id.* Examples of specific laws that some covered entities may be required to comply with include Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act of 1990.

78 45 CFR §164.404(b).

79 74 Fed. Reg. 42749.

80 74 Fed. Reg. 42749-42750.

81 74 Fed. Reg. 42745.

82 74 Fed. Reg. 42749.

83 *Id.*

84 45 CFR §164.404(d)(3).

85 74 Fed. Reg. 42752.

86 45 CFR §164.530(f) provides: "A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate."

87 45 CFR §164.404 (d)(2).

88 74 Fed. Reg. 42751.

89 45 CFR §164.404 (d)(2).

90 45 CFR §164.404(d)(2)(i).

91 74 Fed. Reg. 42751.

92 *Id.*

93 45 CFR §164.404(d)(2)(ii).

94 74 Fed. Reg. 42751.

95 74 Fed. Reg. 42751.

96 74 Fed. Reg. 42752.

97 74 Fed. Reg. 42751.

98 45 CFR §164.406(a).

99 45 CFR §160.103; 45 CFR §164.406(a).

100 74 Fed. Reg. 42752.

101 45 CFR §164.406(c).

102 74 Fed. Reg. 42752.

103 *Id.*

104 45 CFR §164.406(b); 74 Fed. Reg. 42752.

105 45 CFR §164.408(a).

106 45 CFR §164.408(b); 72 Fed. Reg. 42753.

107 72 Fed. Reg. 42753.

108 45 CFR §164.408(c); 74 Fed. Reg. 42753.

109 74 Fed. Reg. 42753.

110 *Id.*

111 45 CFR §164.410. Note also that, pursuant to Section 13401(b) of the HITECH Act, civil and criminal penalties apply to business associates in the same manner as covered entities.

112 45 CFR §164.410(c).

113 74 Fed. Reg. 42754.

114 74 Fed. Reg. 42755.

115 74 Fed. Reg. 42749 (covered entities); 74 Fed. Reg. 42754 (business associates).

116 45 CFR §164.404(a)(2); 45 CFR §164.410(a)(2).

117 74 Fed. Reg. 42749.

118 45 CFR §160.410.

119 45 CFR §164.410 (a)(2).

120 74 Fed. Reg. 42749.

121 74 Fed. Reg. 42754.

122 *Id.*

123 *See* 74 Fed. Reg. 42754.

124 74 Fed. Reg. 42752.

125 74 Fed. Reg. 42755; 45 CFR §164.412.

126 "Law enforcement official" for the purposes of the Interim Final Rule is "an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian Tribe, who is empowered by law to (1) Investigate or conduct an official inquiry into a potential violation of law; or (2) Prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law."

127 74 Fed. Reg. 42755. Exceptions are contained in 45 CFR §160.203 and generally relate to state fraud and abuse laws and public health reporting laws.

128 74 Fed. Reg. 42756.

129 74 Fed. Reg. 42756.

130 *Id.*

131 Pub. L. 111-5; Sec. 13407

132 74 Fed. Reg. 42962 (published August 25, 2009).

133 A "vendor of personal health records" is defined as "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered, that offers or maintains a personal health record." 16 CFR §318.2(j).

134 A "PHR related entity" is defined as "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) Offers products or services

through the Web site of a vendor of personal health records; (2) Offers products or services through the Web sites of HIPAA-Covered entities that offer individuals personal health records; or (3) Accesses information in a personal health record or sends information to a personal health record." 16 CFR §318.2(f).

[135] A "third party service provider" is defined as "an entity that (1) provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services."

[136] 16 CFR §318.5(c).

[137] *See* discussion *supra* at Section III of this article.

[138] 74 Fed. Reg. 42755.

[139] 74 Fed. Reg. 42964.

[140] 74 Fed. Reg. 42965.

[141] 74 Fed. Reg. 42964.

[142] 74 Fed. Reg. 42964.

[143] Pub. L. No. 111-5, §13410(d)(1).

[144] Note that Section 13410(a)(2) of the HITECH Act, which allows violations of the HITECH Act to be enforced pursuant to Sections 1176 and 1177 of the Social Security Act does not become effective until February 18, 2010, which is an additional reason that HHS decided not to impose sanctions immediately upon the effective date of the Interim Final Rule.

[145] Damages that can be collected by a state attorney general include damages of $100 per violation, not to exceed $25,000 for identical violations in a calendar year. These sanctions are in addition to those imposed by the federal government, but cannot be obtained when a federal action is pending. Pub. L. No. 111-5, §13410(e).