Healthcare Information Privacy, Security & Technology Bulletin

August 24, 2009

HHS Releases HITECH Act Breach Notification Rule: Rule Effective Thirty Days After Publication But HHS Sanctions Will Not Apply for 180 Days

Jim Wieland
jbwieland@ober.com

On Wednesday August 19, the Office for Civil Rights of the Department of Health and Human Services (the "OCR") posted a copy of its Interim Final Rule for Breach Notification for Unsecured Protected Health Information (the "Interim Rule"), implementing Section 13402 of the HITECH Act (the "Act"). Publication in the Federal Register is expected on Monday August 24.[1] As an Interim Final Rule, there is a sixty day comment period after publication in the Federal Register. Comments may result in further changes or clarifications.

This Alert covers the highlights of the Interim Rule and is focused on the comments and analysis of the OCR that accompanied the Interim Rule. For a more complete overview of the Act itself, including the statutory provisions governing breach notification, see "Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements in the Stimulus Bill" (2/19/09).[2]

The HITECH Act requires notification to individuals in the event of a breach of the security or the privacy of unsecured protected health information. Unsecured protected health information is defined in the Act as protected health information that is not secured through a technology or methodology specified by the Secretary of Health and

[1] Citations in this Alert are to the Interim Final Rule as posted by the Secretary, not to the official version published in the Federal Register.

[2] This review of the Interim Final Rule for Breach Notification for Unsecured Protected Health Information is for the purpose of information and to alert entities and their advisors that are potentially affected by the Interim Rule to its general content. It covers the points deemed by the author to be of the most interest, not every point raised in the Interim Rule. This Alert does not constitute legal advice to any specific entity or as to any individual situation.

Human Services in guidance. This guidance was published in the Federal Register on April 27, 2009 and is supplemented in a companion portion of the Interim Final Rule. According to the guidance, electronic protected health information can be secured by encryption. Paper protected health information can be secured by destruction. No means are described for securing oral protected health information within the meaning of the Act.

Under the act, business associates are required to provide notification of a breach to covered entities and covered entities are required to provide the notification to the individuals and to the Secretary of Health and Human Services.

Effective Date and Delay of Sanctions

Summary
Under the Act, the breach notification requirements become effective thirty days after publication in the Federal Register. The OCR followed the letter of Act in this respect: ". . . compliance is required for breaches occurring on or after 30 days from the publication of this rule." (Interim Rule, page 69). However, referring to the concerns of covered entities and business associates about the difficulty of achieving compliance within the mandated thirty days and citing some ambiguity within the Act, the OCR went on to state: " . . we will use our enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from publication of this rule . . . During this initial time period – after this rule has taken effect but before we are imposing sanctions – we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance." (Interim Rule, page 69).

Comment
Realistically, this suspension of the imposition of sanctions gives covered entities and business associates some welcome breathing room to complete putting the protocols for compliance into effect. However, covered entities and business associates must still provide notification of breaches, starting thirty days after publication of the Interim Rule. The OCR specifically noted that covered entities and business associates should already have breach notification procedures in place to comply with state consumer protection laws requiring notification to individuals of the compromise of the security of identity theft related information including, in California, medical information. Further, as discussed below, the OCR takes a firm line in the Interim Rule as to when a breach is deemed discovered for the purpose of the notification requirement. Covered entities and business associates who fail to determine the date of deemed discovery of a breach, especially towards the end of the interim period, may be vulnerable to sanctions.

Unauthorized Acquisition, Access, Use or Disclosure

Summary

A breach under the Act is the "unauthorized acquisition, access, use, or disclosure of protected health information." The Interim Rule clarifies that an unauthorized access or use is one that is not permitted under the HIPAA Privacy Rule. Significantly, this leads the OCR to note that "uses of disclosures that impermissibly involve more than the minimum necessary information . . .may qualify as breaches." (Interim Rule, page18) Covered entities and business associates are reminded in a subsequent section of the Interim Rule that the breach notification requirement applies to protected health information in written, electronic or oral form. (Interim Rule, page 37)

Comment

This is one of several indications in the Interim Rule of the significance of guidance that will be issued in accordance with Section 13405 (b) of the Act dealing with the "minimum necessary" requirements of the Privacy Rule. Covered entities must use and disclose only the minimum necessary amount of protected health information needed for a particular situation, subject to exceptions for treatment related disclosures and several other purposes. Pending issuance of minimum necessary guidance, Section 13405 (b) of the Act mandated use of a limited data set "to the extent practicable." While predicting the content of future guidance is not possible, covered entities and business associates should consider the suitability of the limited data set for non-treatment related disclosures of protected health information. The minimum necessary guidance is due not later than eighteen months after enactment of the Act, that is on or before August 17, 2010. The limited data set and its role under the breach notification provisions of the Act is discussed further below.

Compromises of the Security or Privacy of Protected Health Information

Summary

While the Act simply states that a breach is a use or disclosure which "compromises the security or privacy" of protected health information, the Interim Rule provides important clarification that will help covered entities and business associates make notification decisions by articulating a "harm threshold" for a determination that security or privacy has been compromised. For there to have been a compromise requiring notification of subject individuals, a breach must be one that "poses a significant risk of financial, reputational, or other harm to the individual." (Interim Rule, page 20) Covered entities and business associates are advised to perform a risk assessment, and the OCR makes it clear that documentation of that risk assessment will be a key if notification is not given.

In discussing the risk assessment, the OCR articulates five factors to be considered.

- The first factor is the regulatory status of the person or entity that impermissibly used protected health information or to whom the protected health information was impermissibly disclosed. The OCR indicates that disclosure to a HIPAA covered entity or to an agency that is governed by another federal privacy law may not pass the harm threshold, since the recipient is obligated to protect the information. (Interim Rule, page 21)

- The second factor is the nature of the mitigation efforts that were undertaken. The OCR indicates that immediate and effective steps, such as promptly obtaining assurance from the recipient that the information will not be further used or disclosed (such as through a confidentiality agreement) or will be destroyed may make the possibility of harm less than significant. (Interim Rule, page 21).

- For the third factor, the OCR states that if impermissibly disclosed protected health information is promptly returned without being accessed for an improper purpose, the possibility of harm may not be significant. The example given is of a lost or stolen laptop, which is recovered with a forensic analysis showing that information was not opened, transferred, or otherwise compromised. (Interim Rule, page 22)
- The fourth factor identified by the OCR is the type and amount of protected health information involved in the impermissible use or disclosure. The name of an individual and the fact that the individual received services from a hospital may not pass the significant risk threshold; the name of the individual and the fact that the individual received services that may be associated with a particular medical condition (cancer is the example given) or from a specialized type of provider (a substance abuse program is the example given) may. (Interim Rule, page 22)

- Finally, if the breach involves a limited data set, the OCR provides a fifth factor to be considered. Under the Privacy Rule, a limited data set is protected health information from which all sixteen direct identifiers (e.g. name and address) have been removed. However, the limited data set is still protected health information since it is capable of re-association with the subject individual through use of other data. The OCR stated that, in assessing the harm threshold for a breach involving a limited data set, the likelihood of re-association with the individual is a factor to be considered. In addition, the OCR enacted a specific exception from the breach notification requirements for a limited data set that, in addition to excluding the 16 direct identifiers, also excludes date of birth and zip code of the subject individual. This factor applies regardless of whether the limited data set was assembled for the one of the purposes permitted under the Privacy Rule, such as research. (Interim Rule, page 25-26) The OCR specifically invites comments on this limited exception during the sixty day comment period on the Interim Rule.

Comment
Taken together, the OCR's examples provide clarity and some comfort, for covered entities and business associates dealing with a number of recurring situations. A medical bill sent to the wrong address but promptly returned unopened; a laptop left at a meeting which was promptly recovered with an event log that shows that it was not powered up during the time it was missing; a patient file mistakenly sent to the wrong physician's office – each of these may fail to meet the OCR's harm threshold and not require notification of subject individuals. The specific examples also provide a useful basis for judging analogous situations.

The specific exemption afforded by the OCR for a limited data set which also lacks date of birth and zip code information, the latter two being data that is useful for probabilistic matching, a common technique for re-identification of a limited data set through comparison with other available data, may have significance in connection with the August 2010 minimum necessary guidance. This type of "enhanced limited data set" may represent one potential standard for minimum necessary uses and disclosures, at least certain purposes.

Exceptions to Breach

Summary
The Act contains three statutory exceptions to the definition of a breach. In the Interim Rule, the OCR provides examples to flesh out each of these exceptions.

- As to the first exception, unintentional, good faith acquisition, access or use by an employee or other individual acting under the covered entity's or business associate's authority when there is no further use or disclosure, the OCR expands the term "employee" to include members of the covered entity's or business associate's "work-force", a term defined in the Privacy Rule to include, for example, unpaid volunteers working in a covered entity. The OCR illustrates its interpretation of this exception with the example of a billing employee opening an email transmitted to him in error, who notices the error, alerts the sender and deletes the email. By contrast, the OCR cites a work-force member who looks through patient records for information about a friend's treatment, as a violation. (Interim Rule, page 29-32)

- The second statutory exception covers inadvertent disclosures by one individual authorized to access protected health information to another individual within the same facility who is also authorized to access protected health information, if the information is not further disclosed. Here, the OCR expands the definition of "facility" to specifically include covered entities established under HIPAA as an organized health care arrangement (such a hospital and members of its medical staff,

of they collectively meet the standards for an OHCA set forth in the Privacy Rule) and "similarly situated individuals" to mean individuals within the same organization who are authorized to access protected health information, even if the two individuals do not have the same type or scope of rights to access protected health information. Finally, the OCR states that the "same facility" includes all the facilities of a covered entity, such as a hospital system with multiple locations. (Interim Rule, page 32-33)

- The third and broadest exception set forth in the Act applies to an unauthorized disclosure of protected health information to a person who would not reasonably have been able to retain the information. The OCR gives the example of a covered entity sending a number of Explanation of Benefits to the wrong addresses "due to a lack of reasonable safeguards." Those EOBs that are returned unopened as undeliverable do not constitute a breach of the privacy or security of the EOB information. A nurse, mistakenly handing discharge papers to the wrong patient and promptly recovering them, who forms a reasonable conclusion that the recipient could not have read or otherwise retained the protected health information in the papers, also does not cause a breach, according to the OCR. (Interim Rule, page 34)

Comment
The examples provided by the OCR are useful and deal, directly or by analogy, with many recurring situations that covered entities and business associates feared would require breach notification, based on the plain language of the Act. Covered entities with large scale or geographically distributed operations may wish to develop protocols for taking advantage of the clarity these examples provide, as appropriate to the covered entity or business associate own situation, so that "minor" incidents can be quickly documented, if not actually resolved, at the local level, limiting the demands on the organization's privacy officer or other responsible individual as to recurring situations that, given the OCR's examples, do not require notice. The burden of proof is, of course, on the covered entity or business associate. Clear and detailed documentation prepared at or near the time of the incident will be important.

Notification to Individuals

Summary
The Act provides that the time period for notification of individuals starts when the covered entity, in the exercise of reasonable diligence, should have known of the breach. Notice can be imputed to the covered entity from variety of its representatives, including employees (other than the employee causing the breach) and from agents.

Notification must be provided without unreasonable delay and in no event later that sixty calendar days after the breach is known or deemed known by attribution. The OCR

defines "reasonable diligence" as "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." (Interim Rule, page 38). The OCR's comments make it clear that the sixty day period is not tolled by the time spent in analysis or investigation: "Thus, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule."

While the Act requires business associates to notify the covered entity of a breach, the OCR states that the knowledge of a business associate can be imputed to the covered entity, without the mandated notice, if the business associate is an agent of the covered entity. (Interim Rule, page 39) The OCR also explicitly affirms what is implicit in the Act, that the sixty day period is the outside limit and circumstances may well make waiting the full sixty days unreasonable and a violation of the law. (Interim Rule, page 40).

In discussing the content of the notice to individuals, the OCR specifies that the notice should not include protected health information or other sensitive information. The OCR states that, rather than describing steps to "mitigate loss" (the term used in the Act), the notice must describe the steps being taken to "mitigate harm to the individual. In an aside, the OCR adds that the harm to be mitigated "is not limited to economic loss." (Interim Rule, page 42)

Plain language should be utilized in the notice. The OCR states that other statutory accommodations under laws such as the Americans with Disabilities Act (Braille, large print, or audit) must be available. The Interim Rule contains extensive discussion of the mechanics of notice to minors or to representatives of deceased individuals as well as of the use of substitute notice where current mailing (or email, if the individual has consented to email notice) addresses are not available. In certain circumstances, telephone notice to an individual may be left on an answering machine, according to the OCR; however, that notice should be limited to the covered entity's name, contact phone number and the fact that the covered entity has "a very important message" for the individual. (Interim Rule, page 46) The Interim Rule also includes discussion of media notice, web posting and notification to the Secretary, as required in specific circumstances described in the Act.

Comment

This section of the Interim Rule contains useful and detailed discussion of the mechanics and nuances of providing the various types of notification required by the Act. It also provides guidance to covered entities and business associates about avoiding duplicate notices to individuals arising from the same event, a clearly articulated goal of the OCR.

Notification by a Business Associate

Summary
The OCR states that if the protected health information subject to a business associate's breach cannot be attributed to a single covered entity or set of covered entities for which the business associate provides a function or activity, then all potentially affected covered entities must be notified, presumably so that some means of attribution can then be devised by the parties. Covered entities and business associates are free, according to the OCR, to determine who should receive the notice within the covered entity's management structure.

One of the most significant provisions in the OCR's discussion of business associate's role in the breach detection and notification process concerns the circumstances in which the business associate will be deemed an "agent" of the covered entity, and therefore within the language of the Act for purposes of imputing the business associate's knowledge of a breach to a covered entity. The OCR applies the "federal common law of agency" to the determination of a business associate's status. If a business associate is an agent, knowledge will be imputed to the covered entity; if a business associate is an independent contractor, knowledge will not be imputed (at least not automatically). (Interim Rule, page 59)

The Act obligates the business associate to provide certain information to the covered entity that is necessary for the notice. The OCR modifies this in the Interim Rule, by adding the qualifier "to the extent possible" to the language describing the business associate's obligation. The OCR makes it clear that notice to the covered entity should be provided as soon as the business associate is aware of the breach, even if the business associate's investigation is continuing. An example provided by the OCR indicates that some of the burden may, in appropriate circumstances, shift to the covered entity; a record storage company holding "hundreds of boxes" of medical records discovers several boxes are missing and cannot identify the individuals whose records were in the boxes. In this situation, the OCR states: "It is not our intent that the business associate delay notification of the breach to the covered entity, when the covered entity may be better able to indentify the individuals affected." (Interim Rule, page 60) The Interim Rule provides that the business associate must provide the covered entity with any other information that the covered entity is required to include in the notice, either at the time the business associate provides notice to the covered entity or later.

The OCR concludes its discussion of the HIPAA requirements as to breach notification as between covered entities and business associates with a paragraph that stresses the freedom of the parties to contractually allocate responsibilities, so long as the requirements of the Interim Rule are met. This flexibility includes not only when the notification from the business associate is required but also which party will provide notice to individuals. The OCR stated that "We encourage the parties to consider which

entity is in the best position to provide notice to the individual, which may depend on the circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual." (Interim Rule, page 61) The parties are also encouraged to ensure that the individual receives only a single notification of the breach, a point made repeated by the OCR in the Interim Rule.

Comment

While the provisions of the Act are relatively straight-forward – if a business associate discovers a breach related to the protected health information of a covered entity, the business associate must notify the covered entity and the covered entity must provide the notification to individuals required by the Act – the mechanics of implementation are likely to be more complicated, as reflected in the OCR's discussion of the issue.

The OCR indicates, and common sense supports, negotiation of specific allocations of breach notification responsibility between the parties to a business associate agreement, within the parameters of the Act. The OCR indicates a significant degree of flexibility; while the Act contemplates notice to individuals by the covered entity, the OCR, in language quoted above, appears to authorize that burden to be shifted to the business associate in appropriate circumstances.

The status of a business associate as an agent or as an independent contractor has significant consequences in terms of the deemed date of discovery of a breach by a covered entity. The OCR's test for agency status is the federal common law, which, while not always as well fleshed out as state law, is typically used in federal regulations to ensure national uniformity. The Restatements of Law have been referred as a source of federal common law, in the absence of any more specific authority. This business associate's status as an agent may be influenced by language in the business associate agreement or in the underlying service arrangement, depending on the circumstances. This and other provisions of the Act mean that covered entities and business associates should be alert to situations in which a "standard" business associate agreement may not be in the best interests of the parties and negotiate accordingly.

For more information, contact James B. Wieland, a principal in the Health Law Group at Ober|Kaler, at jbwieland@ober.com or 410-347-7397. Jim heads Ober|Kaler's Health Care Information Privacy, Security and Technology practice. Watch for a new Ober|Kaler blog, authored by Jim and covering health information technology issues, coming later this year.