Bricker & Eckler ATTORNEYS AT LAW

eALERT

INCompliance

January 24, 2013

Once More into the Breach: Major Changes to the HIPAA Breach Notification Requirements

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) issued the final omnibus HIPAA rule. Covered entities and business associates must comply with applicable requirements by September 23, 2013.

While much of the final rule simply adopts the interim final rules, one major exception to this is the breach notification rule. Covered entities have analyzed and reported breaches in accordance with the provisions of the interim final rule for more than three years, and the changes contained in the final rule will have a major impact on covered entities' breach analysis and reporting procedures.

This bulletin analyzes the final rule on breach notification and provides guidance to assist all covered entities in achieving compliance with the rule.

What Constitutes a Reportable Breach

The interim final rule defined "breach" as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the privacy regulations, which compromises the security or privacy of the PHI. Under the interim final rule, the standard for determining whether the use or disclosure compromised the security or privacy of the PHI was whether it posed "a significant risk of financial, reputational, or other harm to the individual" (the "risk of harm standard").

HHS noted that 60 of the 70 comments it received on the risk of harm standard were in favor of retaining the standard. Nevertheless, the final rule *completely removes the risk of harm standard* and replaces it with a statement that an impermissible use or disclosure of PHI is "presumed to be a breach unless the covered entity demonstrates that there is a low probability that the protected health information has been compromised."

Under the final rule, covered entities must determine whether there is a low probability that the PHI was compromised – a far different standard than whether there is a significant risk of harm to the individual. As a result, covered entities will have to significantly modify their current procedures for conducting a risk assessment, and ***it is likely that more impermissible uses and disclosures will be reportable breaches under the final rule than under the interim final rule***.

Objective Risk Assessment Factors

The final rule identifies four "objective factors" that *must* be considered in performing the risk analysis of whether PHI has been compromised. The four factors identified by HHS are:

(1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

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

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

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

HHS expects risk assessments to be "thorough, completed in good faith, and for the conclusions reached to be reasonable," and noted "additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised."

HHS also stated that it will issue additional guidance to aid covered entities in performing risk assessments with respect to frequently occurring scenarios. It should be noted, however, that HHS has been extremely slow to issue additional guidance when similar comments have been included in previous rules.

Exceptions to the Definition of "Breach"

The interim final rule included three exceptions to the definition of "breach." These exceptions were adopted without modification in the final rule. The exceptions are as follows:

(1) unintentional acquisition, access, or use of PHI by an employee or other person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the covered entity or business associate, and such information is not further acquired, accessed, used, or disclosed by any person;

(2) inadvertent disclosure of PHI from one person authorized to access PHI at a facility operated by a covered entity or business associate to another person similarly situated at the same facility, and the information received is not further acquired, accessed, used or disclosed without authorization by any person; and

(3) unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Notifications of Breach

The final rule adopts almost all of the interim final rule's breach notification provisions without modification, including the following:

- Covered entities must notify individuals when a reportable breach is discovered. A breach is treated as "discovered" by the covered entity the first day on which such breach is known or should reasonably have been known to any employee or agent of the covered entity, other than the person who committed the breach.
- Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.

- Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
- First class mail is the default method of notification. A covered entity may use e-mail if requested by the individual, or substitute notice via the covered entity's website or local print or broadcast media if the covered entity does not have current contact information.
- A covered entity must notify major local media outlets of a breach affecting more than 500 individuals.
- Business associates must provide notice of breach to a covered entity without unreasonable delay and in no event later than 60 days from discovery of the breach by the business associate.

The final rule makes one minor modification to the notice provisions of the interim final rule. Covered entities are now required to notify HHS of all breaches affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were "discovered." The interim final rule required reporting 60 days after the end of the calendar year in which the breaches "occurred."

Limited Data Sets

Under the existing HIPAA rules, a limited data set is PHI that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual. Under the interim final rule, the impermissible use or disclosure of PHI in a limited data set would not be considered to compromise the security or privacy of the PHI, and would therefore not be reportable if the limited data set also excluded birth dates and zip codes.

The final rule removes this exception. Under the final rule, a covered entity must perform a risk assessment evaluating the factors above following the impermissible use or disclosure of any limited data set, even if it excludes birth dates and zip codes.

What You Need to Do to Comply

Covered entities must comply with the new breach notification requirements of the final rule by September 23, 2013. Covered entities should do the following:

- Update their policies and procedures for reporting, analyzing, and documenting a possible breach of PHI.
- Train workforce members regarding the revised policies and procedures.
- Modify their notice of privacy practices to include the individual's right to receive the breach notice. (We will release a future bulletin capturing all of the necessary changes to the notices of privacy practices resulting from the final rule.)
- Look for future guidance on this topic from HHS.

This joint e-Alert is the second in a series analyzing the final HIPAA omnibus rule. Please watch for our future alerts on additional topics covered under the final rule, and for an

announcement of our new tool to help you make the changes to your HIPAA compliance program required by the final rule.

This joint e-Alert from Bricker & Eckler LLP and INCompliance was prepared by Chris Bennington (513) 870-6572 or mcbennington@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com or any member of the Bricker & Eckler LLP Health Care Practice Group for more information. This and previous email Alerts may be accessed at our publications page.

.