BREACH NOTIFICATION FINAL RULE

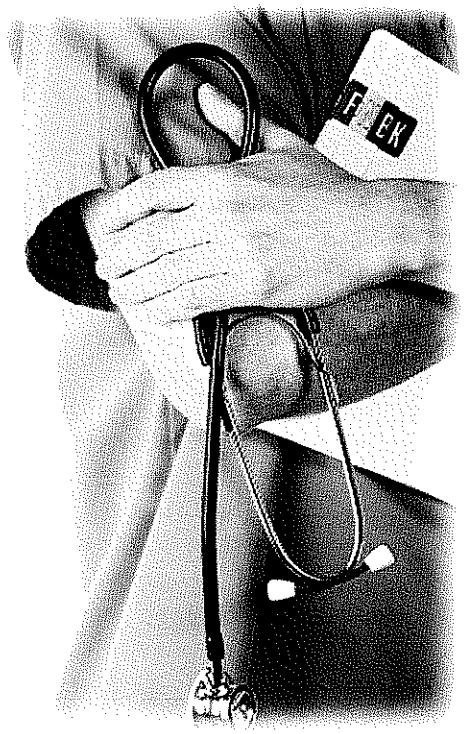
Abby Pendleton, Esq.
Jessica L. Gustafson, Esq.
The Health Law Partners, P.C., Southfield, MI

In compliance with Section 13402 of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, on August 24, 2009, the Department of Health and Human Services ("HHS") issued an interim final rule with comment period ("Final Rule"), which requires covered entities and their business associates to provide notification of breaches of unsecured protected health information ("PHI"). The provisions of this Final Rule were effective September 23, 2009. There are several main components of the Final Rule, which must be considered individually. These considerations, which will be addressed each in turn by this article, include the following:

- Which entities are governed by the Final Rule?
- Has a "breach" occurred?
- If yes, did the breach involve "unsecured protected health information"?
- If yes, to whom must notification be provided, and what information must be provided?

WHICH ENTITIES ARE GOVERNED BY THE FINAL RULE?

The breach notification provisions of the HITECH Act and the Final Rule are applicable to "covered entities" and their "business associates," as these terms are defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Administrative Simplification regulations, codified at 45 C.F.R. § 160.103. Pursuant to these regulations, a covered entity includes a



health plan, health care clearinghouse or health care provider that transmits health information in electronic form (an anesthesia practice that submits a health care claim electronically is an example of a covered entity). A business associate is a person or entity that performs functions on behalf of a covered entity that involve the use or disclosure of protected health information. Examples of business associates include billing companies, transcription companies, legal counsel and entities performing management or administrative services for covered entities who require access to protected health information. "Protected health information" ("PHI") is defined to include, with certain exceptions, individually identifiable health information held or transmitted in any form or medium by HIPAA covered entities and business associates. Anesthesia and pain management practitioners are "covered entities" with access to "protected health information" as defined by the regulations and thus are subject to the HITECH Act and the corresponding provisions of the Final Rule.

HAS A "BREACH" OCCURRED?

In cases where a covered entity discovers a disclosure of PHI, the first consideration is to determine whether such a disclosure constitutes a "breach" as defined by the HITECH Act. Section 13400 (1) of the HITECH Act defines "breach" to mean, generally, "the unauthorized acquisition, access, use, or disclosure" of [PHI], which compromises the security or privacy of such information. The Final Rule clarifies that "unauthorized" means "impermissible use." The Final Rule clarifies that a use or disclosure impermissibly involving more than the minimum necessary PHI may constitute a breach; on the other hand, a use or disclosure resulting from an otherwise permissible use or disclosure involving only the minimum necessary PHI and occurring despite reasonable safeguards would not qualify as a breach.

The Final Rule specifies certain exclusions to the term "breach," including the following: disclosures made to an unauthorized person, where such person would not be reasonably able to retain such information, and further excludes certain unintentional acquisitions, access or uses of information made by employees of a covered entity or business associate,

Continued on page 20

BREACH NOTIFICATION FINAL RULE

Continued from page 19

persons acting under the authority of a covered entity or business associate, or individuals otherwise authorized by the covered entity or business associate to access the PHI

In summary, when determining whether a "breach" has occurred, covered entities and business associates must consider the following three matters: (1) whether there has been an impermissible use or disclosure of PHI under the HIPAA Privacy Rule; (2) whether the impermissible use or disclosure compromises the security or privacy of PHI (*i.e.*, is there a risk of financial, reputational or other harm to the individual as a result of the use or disclosure); and (3) whether the incident falls into one of the exclusions of the term "breach" as defined by the Final Rule.

DID THE BREACH INVOLVE "UNSECURED PROTECTED HEALTH INFORMATION"?

Section 13402(h) of the HITECH Act contains the general requirements regarding breach notification, and specifies that such requirements relate only to breaches of "unsecured protected health information." If PHI is not "unsecured," breaches are not subject to Section 13402(h) of the HITECH Act and the corresponding provisions of the Final Rule. The law defines "unsecured protected health information" as PHI "that is not secured through the use of a technology or methodology specified by the Secretary in guidance." The law further requires that such guidance describe those technologies and methodologies rendering PHI "unusable, unreadable, or indecipherable to unauthorized individuals." Such guidance originally was published April 27, 2009 at 74 Fed. Reg. 19006, and listed encryption and destruction as the two technologies and methodologies used to render PHI unusable, unreadable or indecipherable to unauthorized individuals. This guidance was clarified with respect to specific encryption processes to employ by way of the Final Rule, beginning at 74 Fed. Reg. 42742.

Significantly, the Final Rule does not modify any existing requirements of the HIPAA Security Rule (which is technology neutral), and does not require that covered entities and their business associates encrypt all PHI. The requirements of the HITECH Act and Final Rule relate only to a covered entity's and/or business associate's responsibilities in the event of a breach of unsecured PHI.

- By way of clarification, under the HIPAA Security Rule, encryption is an "addressable," not a "required," implementation specification. This means that a covered entity must assess whether encryption would be a reasonable and appropriate safeguard in the entity's environment; however, the covered entity may choose not to implement the specification based upon its internal assessment, if it documents the reason and implements an equivalent alternative measure, if such alternative would be reasonable and appropriate. Thus, a covered entity may be in compliance with the HIPAA Security Rule even if it reasonably decides not to encrypt electronic PHI and instead uses an alternative method to safeguard information. In this scenario, in the event that a breach of PHI occurs, even though the covered entity or business associate is in compliance with the HIPAA Security Rule, the covered entity or business associate nonetheless will be required to provide the requisite notification pursuant to the HITECH Act and corresponding provisions of the Final Rule, as the PHI is "unsecured."

- On the other hand, if the covered entity or business associate chooses to encrypt PHI as part of its safeguarding of electronic PHI under the HIPAA Security Rule, and provided that such encryption is in compliance with published guidance in the Final Rule, in the event of a breach, the covered entity or business associate will not be required to provide notification under the HITECH Act and corresponding provisions of the Final Rule, as such information was not "unsecured."

A BREACH OF UNSECURED PHI HAS OCCURRED. TO WHOM MUST BREACH NOTIFICATION BE PROVIDED, AND WHAT INFORMATION MUST BE PROVIDED?

Notice to Each Individual

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured

PHI has been (or is reasonably believed by the covered entity to have been) accessed, used or disclosed. Under the Final Rule, a breach is deemed to be discovered either (1) on the first day the entity obtains actual knowledge of the breach; or (2) the day on which the breach would have been known had the covered entity exercised reasonable diligence. Per the Final Rule, the notification to each individual must be made "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."

Such notice must be written in plain language, and must be made either (1) via first class mail to the individual (or to his or her next of kin or personal representative, if such individual is deceased) at the individual's last known address, or (2) via email, if the individual agreed to receive such communications via email. The written notice must include the following elements:

- A description of what happened with respect to the breach, including the date the entity discovered the occurrence of the breach;
- A description of the types of unsecured PHI that were involved in the breach;
- A description of those steps individuals should take to protect themselves from any potential harm resulting from the breach;
- A description of the covered entity's actions to investigate the breach, to lessen the harm to the individuals affected by the breach, and to protect against further breaches; and
- The contact information for individuals to obtain additional information, which should include a toll-free telephone number, an email address, a website or a postal address.

In the alternative, codified at 45 C.F.R. § 164.404 (d) (2), the Final Rule also sets forth requirements for substitute notice, permissible in cases where a covered entity has insufficient or out-of-date contact information for individuals that are the subject of a breach of unsecured PHI.

Notification to the Media

In the event a breach of unsecured PHI involves more than 500 individuals, the covered entity also must notify prominent media outlets of the breach. Such media notification must include all elements included in the individual notification, and must be made without unreasonable delay, but in no case later than 60 calendar days after the discovery of the breach.

Notification to HHS

In all cases in which a covered entity discovers a breach of unsecured PHI, the covered entity must notify HHS. If the breach involves 500 or more individuals, the notification to HHS must be made at the same time notification to each individual is made. If the breach involves fewer than 500 individuals, the covered entity will maintain documentation of the breach and provide notification to HHS no later than 60 days following the end of the calendar year.

Business Associates

The Final Rule also requires that business associates notify the covered entity of any breach of unsecured PHI that occurs. Such notification must be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

CONCLUSION

The Final Rule requires that anesthesia and pain practices adopt and implement policies and procedures related to the breach notification provisions of the HITECH Act and Final Rule. The Final Rule also requires that these entities train their workforce members regarding these breach notification requirements. As a practical matter, because the provisions of the HITECH Act and Final Rule are rather detailed, covered entities and business associates should train their employees to inform the HIPAA Privacy or Security Officer of any potential breach, so that the entity's management can render a decision as to what notification, if any, must be made. This is not an easy task and will likely require investigation and coordination with legal advisors. ▲

Abby Pendleton

Jessica L. Gustafson

Abby Pendleton and **Jessica L. Gustafson** are partners with the health care law firm of The Health Law Partners, P.C. in Southfield, Michigan. The firm represents hospitals, physicians, and other health care providers and suppliers with respect to their health care legal needs. Pendleton and Gustafson specialize in a number of areas, including but not limited to: Recovery Audit Contractor (RAC), Medicare, Medicaid and other payor audit appeals, healthcare regulatory matters, compliance matters, reimbursement and contracting matters, transactional and corporate matters, and licensing, staff privilege and payor de-participation matters. They can be reached at apendleton@thehlp.com and jgustafson@thehlp.com.