SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW
DECEMBER 2009

Health Law Alert

Recent Modifications to HIPAA's Breach Notification and Enforcement Rules

The Health Information Technology for Economic and Clinical Health Act ("HITECH") , enacted as part of the American Recovery and Reinvestment Act of 2009, requires HIPAA covered entities and business associates to provide certain notifications in the event of a breach of protected health information ("PHI") and increases the civil monetary penalties for HIPAA violations.[1]

I. Determining if Notification of a Breach is Required

Notifications discussed below are required if there is a "breach" of PHI by a covered entity or business associate. A breach is the acquisition, access, use, or disclosure of PHI, other than as permitted by HIPAA, which compromises the security or privacy of the PHI. Covered entities and business associates can use the following questions to determine if a breach occurred and notification is required.

Question 1: Did the incident involve PHI?

A breach must involve PHI. PHI is individually identifiable health information that is transmitted or maintained in any form or medium, including electronic media. PHI does not include certain educational records, limited data sets with birth date and ZIP code removed, employment records, or de-identified information.

Question 2: Was there an acquisition, access, use, or disclosure of PHI not permissible under the HIPAA Privacy Rule? A breach must involve the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, such as the disclosure of PHI to an unauthorized person. The following are typically not considered breaches:

- An incident occurring in connection with a permissible disclosure despite the use of reasonable safeguards and proper minimum necessary procedures;
- An incident involving a third party to whom the covered entity or business associate permissibly disclosed PHI; or
- A violation of an administrative requirement, such as a lack of reasonable safeguards or training.

Question 3: Does a safe harbor or exception apply?

1. Secured PHI Safe Harbor.

A breach must involve unsecured PHI. Unsecured PHI is PHI that has not been rendered unreadable, unusable, or indecipherable to unauthorized individuals in accordance with HHS guidance. HHS has approved encryption and destruction consistent

[1] The Department of Health and Human Services ("HHS") issued interim final rules for breach notification on August 24, 2009 and for increased penalties on October 30, 2009.

Questions or Assistance?

If you have further questions about HIPAA breach notification and enforcement, please feel free to contact one of the following members of our Health Law Practice Group.

Joan Feldman
jfeldman@goodwin.com
(860) 251-5104

David Mack
dmack@goodwin.com
(860) 251-5058

Vincenzo Carannante
vcarannante@goodwin.com
(860) 251-5096

William Roberts
wroberts@goodwin.com
(860) 251-5051

www.shipmangoodwin.com

with the National Institute of Standards and Technology or the Federal Information Processing Standards as the only methods to secure PHI.

2. Exceptions.
Notification is not required if the incident satisfies one of the following three exceptions:

- **Unintentional Acts by Workforce Member**. The unintentional acts of a workforce member (e.g. employee, volunteer, trainee, or other person under direct control of the covered entity or business associate) in good faith and acting within the scope of employment or engagement is not a breach, provided that there is no further unauthorized acquisition, access, use, or disclosure. For example, a receptionist opens a file containing PHI and immediately notices that he is looking at the wrong file and closes it. No breach occurred because the receptionist acted in good faith and within the scope of his employment, provided that the receptionist did not further use or disclose the PHI.

- **Inadvertent Disclosures by Authorized Individual**. The inadvertent disclosure of PHI from one authorized individual at a covered entity or business associate to another authorized individual at the covered entity or business associate is not a breach provided that there is no further unauthorized acquisition, access, use, or disclosure. For example, a physician mistakenly sends an email containing patient PHI to a nurse at the same covered entity. No breach occurs because both the disclosing and receiving party are authorized to access PHI, provided that the nurse did not further use or disclose the PHI.

- **PHI Not Retained**. A breach does not occur when PHI is disclosed to an unauthorized person, and the covered entity or business associate has a good faith belief that the PHI was not able to be retained by the unauthorized person. For example, a nurse mistakenly hands a patient the discharge papers of another patient, but quickly realizes the mistake and recovers the discharge papers. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then there is no breach.

Question 4: Did the impermissible acquisition, access, use, or disclosure compromise the security or privacy of the PHI?

A breach must "pose a significant risk of financial, reputational, or other harm to the individual." Therefore a risk assessment must occur to determine the risk that the individual whose PHI was acquired, accessed, used, or disclosed could be identified and, if identified, the risk of harm to the individual. The covered entity or business associate must document its risk assessment to demonstrate why breach notification was or was not provided. The entity must maintain the documentation and make it available to HHS upon request.

II. Notification of Breach

In the event a covered entity or business associate determines that notification of a breach is required, the entity must provide one or more of the following notices as required by HIPAA.

A. Notice to the Patient.
Notice of a breach must be written in plain language and include:

- A brief description of what happened, including the date of breach and discovery;

- A description of the type(s) of unsecured PHI involved;

- Steps the patient should take to protect himself or herself from potential harm;

- A brief description of steps being taken by the covered entity and/or business associate in response to the breach; and

- The covered entity's contact information.

Notice to the patient is to be made by first-class mail or email, if specified as a preference by the individual. In the event more urgent notice is deemed necessary by the covered entity, telephone or other contact may be appropriate, in addition to the written or email notice.

In the event a covered entity lacks sufficient contact information or a notice is returned as undeliverable, substitute notice is required. Where the breach involves fewer than 10 individuals, the covered entity can provide notice by telephone or other means reasonably calculated to reach the individuals. Where the breach involves 10 or more individuals, a covered entity must place a conspicuous posting on its website for 90 days or in major print and broadcast media in areas where the individuals affected by the breach likely reside.

B. Notice by the Business Associate to the Covered Entity.

In the event a business associate discovers a breach of PHI, it must report such breach to the covered entity. Notification to the covered entity must be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. Notice to the covered entity must include the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. After the initial notice, the business associate has a continuing obligation to inform the covered entity of any newly available facts.

C. Notice to the Media.

For breaches involving the PHI of more than 500 individuals of any one state or jurisdiction, the covered entity must notify "prominent media outlets" (e.g. in a press release) in that state or jurisdiction.

D. Notice to HHS.

For breaches involving the PHI of more than 500 individuals, regardless of state or jurisdiction, the covered entity must notify HHS. If necessary, the notice can be sent concurrently with the notice to patients.

For breaches involving the PHI of less than 500 individuals, the covered entity must maintain a log or other documentation of such breaches and submit such log or documentation annually to HHS. Annual submission must be made no later than 60 days after the end of the calendar year, in a manner specified on the HHS website.[2]

E. Application of State Law.

Covered entities and business associates must be aware that state law may require notification of a breach of PHI as well, even in cases where no notification is required under HIPAA.

III. Civil Penalties for HIPAA Violations

HITECH establishes four categories of penalties applicable to HIPAA violations by covered entities or business associates occurring on or after February 18, 2009. Each category has a range or minimum for each violation. The maximum aggregate penalty for multiple violations of the same HIPAA provision in a calendar year is $1,500,000. The four categories are as follows:

- Tier 1: If the covered entity or business associate is not aware of the violation (and would not have known with reasonable diligence), the penalty is at least $100/violation, not to exceed $50,000/violation.

- Tier 2: If the violation is due to "reasonable cause," the penalty is at least $1,000/violation, not to exceed

[2] For calendar year 2009, the covered entity is only required to submit information to HHS for breaches occurring on or after September 23, 2009.

$50,000/violation. Reasonable cause is defined as circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the provision violated.

- Tier 3: If the violation is due to willful neglect and is corrected within 30 days, the penalty is at least $10,000/violation, not to exceed $50,000/violation. Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated.

- Tier 4: If the violation is due to willful neglect and is not corrected within 30 days, the penalty is at least $50,000/violation.

HHS has indicated that it will not impose sanctions for failure to provide notification for a breach discovered before February 22, 2010. Until this time, HHS expects covered entities and business associates to comply with the breach notification rules, but has indicated that it will use technical assistance and voluntary corrective action to achieve compliance.

IV. Action Items

In light of HIPAA's new breach notification requirements and substantially increased penalties for noncompliance, covered entities and business associates should consider taking measures such as the following:

- Develop policies and procedures to determine whether a breach has occurred and for breach notification and response;

- Provide additional HIPAA training regarding identifying and reporting breaches for employees or agents handling PHI;

- Work with business associates to determine breach notification obligations; and

- Revise business associate agreements, as necessary.

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW