porterwright

Employee Benefits Law Alert

A Corporate Department Publication

October 2009

Breach Notification Under the HITECH Act:
Action Points for Employers Who Sponsor Self-Insured Group Health Plans

The Department of Health and Human Services (HHS) recently issued an interim final rule (Rule) under the HITECH Act requiring notification by HIPAA-covered entities of breaches of unsecured protected health information (PHI). The Rule became effective September 23, 2009, but HHS indicated it will use its enforcement discretion and not impose sanctions for failure to provide required notifications for breaches that are discovered before February 22, 2010. Employers who sponsor self-insured group health plans (one category of HIPAA-covered entity) thus need to take immediate action to ensure compliance with the new Rule.

Background

Passed as part of the American Recovery and Reinvestment Act of 2009, the Health Information Technologies for Economic and Clinical Health Act (HITECH Act) substantially alters federal privacy and security law related to PHI. (See our March 2009 alert *HITECH Act Brings New Vigor to HIPAA's Privacy and Security Rules.*) The HITECH Act expands the definition of "business associate," directly applies certain aspects of the HIPAA Privacy Rule and HIPAA Security Rule to business associates for the first time, and increases penalties for HIPAA violations. One of the most significant aspects of the HITECH Act, however, is its breach notification requirements, which are the subject of the Rule.

The Rule

Definitions

Under the Rule, upon discovering 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, acquired, used, or disclosed as a result of the breach. "Unsecured PHI" is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technologies or methodologies specified by the Secretary of HHS. (The Secretary has specified that encryption and destruction are two technologies and methodologies that will secure PHI.) Subject to certain exceptions, a "breach" is the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of PHI. The security or privacy of PHI is compromised if a significant risk of financial, reputational, or other harm to the individual is posed.

Ann M. Caresani
216-443-2570
acaresani@porterwright.com

Brian D. Hall
614-227-2287
bhall@porterwright.com

Richard J. Helmreich
614-227-2088
rhelmreich@porterwright.com

Susan N. Lubow
614-227-2061
slubow@porterwright.com

James H. Prior
614-227-2008
jprior@porterwright.com

Deborah A. Boiarsky
614-227-2001
dboiarsky@porterwright.com

Kaleb J. Brankamp
614-227-2010
kbrankamp@porterwright.com

Please see our other publications at www.porterwright.com/publications.

porterwright

Discovery of a Breach of Unsecured PHI

A covered entity "discovers" a breach on the date the breach is first known to the covered entity or on the date the breach would have been known by the covered entity had it exercised reasonable diligence. The knowledge of workforce members and agents of a covered entity (as determined in accordance with the federal common law of agency) is imputed to the covered entity. Thus, if a covered entity's business associate is considered to be an agent of the covered entity, then the covered entity is deemed to have discovered a breach of unsecured PHI on the same date its business associate first knows of or, by exercising reasonable diligence, would have known of the breach.

Breach Notification Requirements

A covered entity must provide breach notification to an affected individual "without unreasonable delay and in no case later than 60 calendar days after" the covered entity discovers the breach. If an individual's contact information is insufficient or out-of-date, substitute notice will need to be provided, the form of which will vary according to whether 10 or more individuals are involved. For breaches of unsecured PHI involving more than 500 residents of a state or jurisdiction, a covered entity must notify prominent media outlets serving that state or jurisdiction. Also, for breaches involving 500 or more individuals (regardless of their location), a covered entity must notify the Secretary of HHS in the manner specified on the HHS Web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html). For breaches involving fewer than 500 individuals, a covered entity must maintain a log of such breaches and notify the Secretary of HHS on an annual basis, no later than 60 days after each calendar year, in the manner specified on the HHS Web site. Business associates must notify a covered entity of a breach of unsecured PHI without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

Action Points for Employers Who Sponsor Self-Insured Group Health Plans

Because the Rule is currently effective and because sanctions will be imposed by HHS for failure to provide required notifications for breaches that are discovered on or after February 22, 2010, what should employers who sponsor self-insured group health plans begin doing now to comply?

Modify Written HIPAA Privacy Policies and Procedures

The Rule requires a covered entity to implement written policies and procedures that are designed to comply with the breach notification requirements. In addition to creating processes for notifying affected individuals and the Secretary of HHS of breaches of unsecured PHI once they are discovered, the policies and procedures should address, among other things, the implementation of reasonable systems for detecting breaches. A covered entity should also review (and revise, as appropriate) its training, complaint, and sanctions policies in light of the requirements of the Rule. "Minimum necessary" policies and procedures should also be reviewed and updated, as HHS indicated in the preamble to the Rule that disclosures of PHI involving more than the minimum necessary amount of information may constitute a breach under the Rule. The HITECH Act directs HHS to issue additional guidance by August 11, 2011 on the meaning of the phrase "minimum necessary."

Train Plan Sponsor Workforce Members Authorized to Have Access to PHI

The Rule also requires a covered entity to train all members of its workforce on the policies and procedures with respect to PHI required by the Rule. For employers who sponsor a group health plan, training is generally provided to those members of the plan sponsor's workforce who are involved in plan administration and who are authorized to have access to PHI of the group health plan. It is important that these workforce members clearly understand what constitutes a breach of unsecured PHI under the Rule and what steps must be taken when a breach is detected, including notification and documentation procedures. This also may be a good time to update training on other HIPAA policies and procedures.

Modify Business Associate Agreements

A covered entity should modify its business associate agreements to address the timing of notification by business associates of any discovery of a breach of unsecured PHI. As previously noted, if a covered entity's business associate is considered to be an agent of the covered entity, the covered entity's time period for providing a breach notification to an individual begins running with the business associate's discovery of the breach. The business associate agreement should also address what information the business associate should provide to the covered entity upon discovery of a breach and what responsibilities, if any, the business associate will have in providing the required notifications.