

Final Regulations on HITECH Security Breach Notification for HIPAA Protected Health Information

The American Recovery and Reinvestment Act of 2009 (the Act), signed into law on February 17, 2009, contains the most significant revisions to the Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules since their release.¹ One of the most important changes is the new Health Information Technology for Economic and Clinical Health (HITECH) breach notification requirement applicable to HIPAA covered entities and their business associates.² As required by HITECH, the Department of Health and Human Services (HHS) has released interim final regulations implementing this new breach notification requirement.³ The regulations take effect on September 23, 2009, but due to the short compliance timeframe, HHS has decided to delay seeking sanctions for another five months (*i.e.*, not before February 22, 2010).

OVERVIEW

HIPAA covered entities, including group health plans, must now notify individuals when there is a breach of unsecured protected health information (PHI) that affects them. The new rule applies to all types of PHI — electronic PHI (ePHI), PHI on paper and spoken PHI. Group health plans must provide notice to each affected individual, without unreasonable delay and in no case

later than 60 calendar days after the breach is discovered. Notice must also be provided to HHS — concurrently with the individual notice, if the breach involved 500 or more individuals, or annually in all other situations. In some cases, prominent media outlets must also be notified. The Notice must meet the content standards set forth in the rule, including being written in plain language. If a business associate is responsible for the breach, the business associate must notify the covered entity and provide the information necessary to permit the covered entity to provide the required notices.

The HITECH security breach rule only applies to unsecured PHI, which means PHI that has not been secured through the use of a technology or methodology specified by HHS. In April 2009, HHS released a safe harbor rule stating that encryption and destruction are the only two ways to secure PHI and thus avoid breach notification under the Act.⁴ In the regulations just issued, HHS elaborated on that guidance.

IMPLEMENTING HITECH

The regulations clarify a number of key issues:

- **Use or Disclosure Must Violate Privacy Rule** There is no breach unless the unauthorized use or disclosure of PHI violates the HIPAA Privacy Rule. HHS notes that a use or disclosure that impermissibly involves more than the minimum necessary PHI may qualify as a breach requiring notification.
- **Risk of Harm Threshold** Notification is not required unless the unauthorized use or disclosure of PHI poses a *significant risk of financial, reputational, or other harm to the individual*. Covered entities (or their business associates) would, therefore, need to perform and document a fact-specific risk assessment in order to determine whether there is a significant

¹ For an overview of these changes, see The Segal Company's March 2009 *Bulletin*, "Stimulus Law Includes Major Changes to HIPAA Privacy and Security Rules":

<http://www.segalco.com/publications/bulletins/march09HIPAA.pdf>

² The Act also contains a breach notification requirement applicable to vendors of personal health records. The Federal Trade Commission's implementing regulations were published on August 25, 2009:

<http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf>

³ The HHS interim final regulations were published in the August 24, 2009 *Federal Register*:

<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

⁴ For a discussion of the guidance, see Segal's May 22, 2009 *Capital Checkup*, "HHS Guidance on Securing Protected Health Information and Avoiding Breach Notification": <http://www.segalco.com/publications-and-resources/capital-checkup/archives/?id=1273>

risk of harm and, consequently, whether notification is required. Factors to consider include: the type and amount of PHI, the identity of the unauthorized person who impermissibly used the PHI or to whom PHI was disclosed, whether the entity has taken immediate steps to mitigate harm, and whether the PHI is returned prior to being accessed for an improper purpose. As examples, HHS notes that a list of names of people who received services from a general hospital poses less of a risk than a list of people treated at a substance abuse facility. The type of identifiers is also relevant: for example, names alone would not be as sensitive as names plus social security numbers. A disclosure to another covered entity, with its own legal obligation to protect the PHI, would pose less risk than disclosure to someone without such a legal duty.

- **Concrete Examples of Breach Exceptions** HITECH includes exceptions for certain unintentional or inadvertent actions and situations where the unauthorized recipient could not reasonably have been able to retain the PHI. For example, if an employee acting in good faith opens an e-mail that was sent by mistake by another employee, there is no breach if the receiving employee alerts the sender of the misdirected e-mail, deletes the e-mail, and makes no further use of the information. Similarly, if a health plan mails an Explanation of Benefits (EOB) form to the wrong individuals, but it is returned by the post office unopened, this is not treated as a breach. HHS cautions that EOBs that are not returned as undeliverable should be treated as potential breaches if the plan knows they were sent to the wrong people.
- **Flexibility in Dealing with Business Associates** Although both HITECH and the regulations require business associates to notify the covered entity of any breach, covered entities and their business associates may still allot duties in their business associate contract. This could include requiring the business associate to provide notices, and addressing when the business associate must tell the covered entity of the breach.
- **Technology Guidance Does Not Amend Security Rule** Encryption is not required by the Security Rule itself. For purposes of Security Rule compliance, covered entities seeking to protect data at rest (e.g., data stored in a database) may choose to rely on firewalls and other access controls in lieu of encrypting data at rest. However, this would not render ePHI secure for purposes of the breach notification rule.
- **Privacy Rule's Administrative Requirements Apply** The regulations amend the HIPAA Privacy Rule,

confirming that various administrative requirements apply to breach notification. These include the requirements to develop written policies and procedures, to maintain written documentation (to demonstrate that notice was provided or that the use or disclosure did not constitute a breach), to train the workforce, and to sanction workforce members who violate the law or the plan's policies.

IMPLICATIONS FOR PLAN SPONSORS

Even with the five-month delay in sanctions, plan sponsors need to start now to achieve compliance by determining whether new security safeguards will be implemented, developing or enhancing systems to detect breaches, drafting and implementing breach notification policies and procedures, reviewing duties and timelines with business associates, and training affected members of the workforce.



As with all issues involving the interpretation or application of laws and regulations, plan sponsors should rely on their attorneys for authoritative advice on the interpretation and application of the breach notification requirements. The Segal Company can be retained to work with plan sponsors and their attorneys on HIPAA compliance.



ATLANTA	678.306.3100
BOSTON	617.424.7300
CALGARY	403.692.2264
CHICAGO	312.984.8500
CLEVELAND	216.687.4400
DENVER	303.714.9900
HARTFORD	860.678.3000
HOUSTON	713.664.4654
LOS ANGELES	818.956.6700
MINNEAPOLIS	952.857.2480
MONTREAL	514.989.3735
NEW ORLEANS	504.483.0744
NEW YORK	212.251.5000
PHILADELPHIA	215.854.4017
PHOENIX	602.381.4000
PRINCETON	609.520.2700
RALEIGH	919.233.1220
SAN FRANCISCO	415.263.8200
TORONTO	416.969.3960
WASHINGTON	202.833.6400

www.segalco.com