PUBLICATION

HITECH Breach Notification Rules Are a Reality

August 31, 2009

The much anticipated “breach notification” rule was recently published by the Department of Health and Human Services (HHS), Office of Civil Rights (OCR). As required by the provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the rule adds new specifications for covered entities and business associates, outlining how they must provide notification when "unsecured" protected health information (PHI) has been breached. The HHS rule, combined with the new FTC final rule regarding the breach of unsecured, identifiable personal health records (PHR) from non-covered entities such as vendors and their third-party service providers, ushers in the new era of the privacy and security protections for individuals. Most entities will be subject to only one rule. There are a finite number of entities required to comply with both the HHS and FTC rule, and companies must quickly make sure they are clear on which rules apply to their businesses. HHS worked with the FTC to ensure both sets of regulations were "harmonized."

The HHS interim final rule provides covered entities and business associates with a short window in which they can impact the breach notice policy process. Comments on the interim final rules are due on or before October 23, 2009, while comments regarding the information collections requirements are due on or before September 8, 2009. Baker Donelson is currently assisting clients in drafting and submitting comments and can assist you in having your voice heard on these key issues.

Click **here** for key terms and highlights of the Interim Final Rule.

Click **here** to review our prior Alert on the HITECH Act.

Key Terms and Highlights of the Interim Final Rule

Under HITECH and the HHS Rule, notice to an individual of a “breach” is required if the PHI is “unsecured”. The definitions of “breach” and “unsecured” are key in understanding the law. Simply put, a breach is the “unauthorized acquisition, use or disclosure” of PHI.

Breach

In the HHS rule, HHS provided an algorithm by which an entity can assess whether a breach actually occurred that requires notice. Specifically, HHS provides that the covered entity should ask the following questions:

1. Was there an impermissible use or disclosure of unsecured PHI?
2. Was the use or disclosure a violation of the HIPAA Privacy or Security Rules?
3. Was there significant risk of financial, reputational or other harm to the individual? (Perform a risk of harm analysis/assessment).
4. Does an exception to the breach rules apply?

If the answer to any of the first three questions is "yes" and no exception exists, then notice likely will be required under the HITECH provisions.

Risk of Harm Assessment

HHS paid heed to some comments to the Guidance advocating that the definition of “breach” include a risk assessment component to determine if there was an actual risk of harm to the individual(s) whose information was potentially exposed. HHS chose to include this assessment, but noted that the risk assessment must be documented so that it can be demonstrated that no breach notification was required following an impermissible use or disclosure of PHI. HHS provided several examples of what may or may not qualify as an “actual risk of harm” to an individual and further pointed to a memorandum used by the government in determining whether it believes it has breached the privacy of individuals and whether a notice is required. HHS was addressing several concerns when developing this aspect of the definition of breach, most notably the fear that, without this risk of harm analysis, individuals could receive notices when there was no real need for concern. HHS provided as one example a stolen laptop that is later recovered and found by forensic analysis not to have been “opened, altered transferred or otherwise compromised.” In this case, HHS deemed it would be unreasonable to panic individuals unnecessarily when their information had not been compromised.

Notably, the “risk of harm” analysis is not present in the FTC rule, and therefore, those vendors and their third-party service providers of personal health records who are covered by both the HHS rule and the FTC rule must pay close attention to the nuances. The FTC final rule provides several examples to illustrate the interaction between these two rules.

Breaches Treated as Discovered

HHS also took the opportunity to specify with greater precision the nexus between the breach notification regulations and the HIPAA enforcement rule. A breach is considered “discovered” as of the first day the breach is known or should have been known if reasonable diligence was exercised. The enforcement rule had previously introduced this concept as an acknowledgement that companies cannot just bury their heads in the sand. They must implement reasonable systems to discover if a breach has occurred.

Exceptions

Further, the HHS rule sets forth three regulatory exceptions to the definition of "breach" rules, including certain good faith misuses or disclosures among a company's workforce members.

Further, HHS noted that de-identified health information and certain employment records of employers are not PHI, and therefore, could not be “breached.” If identifiable health information that is not PHI is used or disclosed in an unauthorized manner, such use or disclosure would not qualify as a breach. On the other hand, uses or disclosures that impermissibly involve more than the minimum necessary information may qualify as a breach. Also, the breach provisions apply to the impermissible uses or disclosures of PHI that constitute a limited data set unless no significant risk of harm resulted. The rule sets forth other examples that may qualify as an exception under the "breach" rules.

Notice Requirements Under HHS Rule

Covered entities must provide written notice directly to the individual in the manner and with the content prescribed in HITECH and the HHS rule. If the covered entity has insufficient or out of date information for less than ten individuals, then the covered entity should provide an alternative form of notice (such as notice via telephone). If more than ten individuals require alternative/substitute notice, then notice of the breach must be posted prominently on the home page of the covered entity's web site or notice must be made via the media as described in the rule. The ten-person threshold is a fairly low threshold, as most individuals do not notify their providers or health plans when their address changes. There are also special requirements if there is an imminent risk of harm to individuals. Covered entities must also notify the Secretary of HHS of breaches. The

Secretary is required to post on the HHS website a list of covered entities that experience breaches of unsecured PHI involving more than 500 individuals.

Further, business associates are required to report breaches of PHI to the covered entity. The rule also sets forth the type of information a business associate must provide to a covered entity following a breach of unsecured PHI.

"Unsecured"

Section 13402 of the HITECH Act defined "unsecured" PHI as information that was not secured through the use of technology rendering the information "unusable, unreadable or indecipherable." Congress then directed HHS to offer specific guidance on what technology would qualify as "unusable, unreadable or indecipherable." Predating the HHS interim final rule, this Guidance was provided in April, 2009. The Guidance specified two methods for rendering PHI "unusable, unreadable or indecipherable" – (1) encryption and (2) destruction. HHS uses certain National Institute for Standards and Technologies (NIST) standards in determining both acceptable methods of encryption and destruction. HHS received many comments and suggestions for additions to the approved methodologies. The HHS interim final rule and Guidance references the NIST standards several times. For those who have worked closely with the Security Rule, the standards outlined by NIST are not new. HHS frequently looks to NIST to ensure that the technologies are within certain established security standards.

HHS provided some clarifications on encryption specifications that will meet the safe harbor provided for PHI that was breached but can be considered "secured." However, HHS has made clear that encryption remains an addressable standard that is not required by the Security Rule. That said, covered entities and business associates who do not give strong consideration to ensuring the PHI they access or control is considered "secure" by the Guidance are exposing themselves to some potentially significant adverse consequences if a breach were to occur.

Effective Dates

The HHS rule is effective on September 23, 2009 and comments are due October 23, 2009. The FTC rule, which has been released to the public, is effective 30 days from its publication in the *Federal Register* with enforcement delayed until February, 2010 to allow for entities falling within the requirements to come into compliance.

Action Items:

5. Conduct an audit to determine whether the technologies utilized by the organization falls within the acceptable technologies specified by the Guidance, HHS rule and the FTC rule.
6. Amend business associate (BA) agreements and third-party vendors servicing PHI/PHR vendor's agreements. As HITECH requires more than one amendment to BA agreements, coordinating and planning the timing of the changes merits significant thought.
7. Update policies and procedures to reflect the changes, including the addition of a (1) breach detection policy and procedure, (2) breach response timetable and policy and procedure, (3) risk of harm analysis algorithm and policy and procedure, and (4) breach notification policy and procedures.
8. Retrain workforce to enable covered entities, business associates and PHR vendors to identify breaches, timely report privacy and security incidents and to comply with the rule.
9. Ensure internal auditing systems are able to detect breaches.
10. Attempt to verify the current addresses of individuals whenever possible.