January 28, 2012

HHS Releases Final Rule Expanding HIPAA

On January 17, 2012, the U.S. Department of Health and Human Services (HHS), in conjunction with the Office of Civil Rights (OCR), released for preview their long-anticipated omnibus regulation to implement the statutory expansion of the scope of the Health Insurance Portability and Accountability Act (HIPAA) by the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), and the Genetic Information Nondiscrimination Act (GINA). The rule was published in the Federal Register on January 25, 2013, with an effective date of March 26. Covered entities and business associates have 180 days – until September 23, 2013 – to comply with the new rule.

In announcing the Final Rule, HHS Office for Civil Rights Director Leon Rodriguez stated that the rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented" and will assist OCR "to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates." This client Alert highlights several key takeaways from the expansive 563-page rule. Should you require further analysis or explanation of the new HIPAA regulations, please contact the authors of this Client Alert or the Brownstein Hyatt Farber Schreck attorney with whom you normally consult.

Business Associate Liability

The Final Rule's most notable change is the expansion of direct liability for HIPAA violations to business associates, and the modification of the "business associate" definition.

What is a "Business Associate"

HIPAA traditionally applied to "covered entities" such as health care providers, health plans, and clearinghouses processing insurance claims. Under the new rule, however, a business associate of a covered entity who "creates, receives, maintains, or transmits protected health information [PHI] on behalf of a covered entity" will be held directly liable for compliance with HIPAA privacy and security rules. The rule also expands the definition of "business associate" to specifically include:

1. Patient Safety Organizations (PSOs) in conformity with the Patient Safety and Quality Improvement Act of 2005
2. Health Information Organizations, E-prescribing Gateways, or other persons that provide data transmission services on behalf of a covered entity and require routine access to PHI
3. Organizations that offer a personal health record to one or more individuals on behalf of a covered entity

One East Washington Street
Suite 2400
Phoenix, AZ 85004

4. Subcontractors of business associates who receive, create, maintain, or transmit PHI on behalf of a business associate

These entities are now required to enter into a written business associate agreement with the covered entity in accordance with HIPAA rules. The rule imposes direct civil penalty liability on business associates for any privacy and security violations.

Who is a "Business Associate"

The omnibus rule recognizes that the definition of “Health Information Organizations” is ever-evolving, and for this reason, refused to include a specific definition of the term. The rule clarifies, however, that entities that maintain or store PHI on behalf of a covered entity are business associates, even if they do not actually view it.

The rule outlines the conduit exception to the business associate definition, and recognizes the subtle nuances of the exception. Determining whether an organization is a business associate or a conduit depends on the access the entity has to PHI. According to the Final Rule, “such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity.” Thus, the conduit exception excludes only those entities providing mere courier services, such as a postal service or its electronic equivalent (i.e. an internet service provider's mere data transmission services).

These fact specific determinations- of when a personal health record vendor is considered to be providing or maintaining PHI on behalf of a covered entity and what it means to have “access on a routine basis” to PHI – will foreseeably cause disagreement about who is and isn't a business associate or subcontractor. HHS and OCR acknowledge this reality, promising further guidance to be published on their website. HHS, however, does not give a time line for issuing this guidance.

The new rule removes the exception for covered entity liability for acts of its agent and makes covered entities and business associates liable for the acts of their business associate agents. Whether a business associate or subcontractor is an agent is based on the Federal common law rule of agency and depends on the principal’s right or authority to control the business associate’s conduct in the course of performing a service on behalf of the covered entity. Covered entities will need to obtain satisfactory assurances from their business associates, and business associates must do the same with regard to their subcontractors, to protect from such liability.

One East Washington Street
Suite 2400
Phoenix, AZ 85004

Overall, the expansion of the business associate definition alleviates concerns that PHI is not adequately protected when provided to associates and their subcontractors. Further, the shared liability under the HIPAA rules are positive incentive for all parties to fully comply with the law's requirements.

Changes to the Enforcement Rules

The Rule revises the HIPAA Enforcement Rules to incorporate provisions from HITECH that apply to privacy and security violations and were not effective immediately upon passage of the Act. One such provision addresses enforcement of noncompliance with the HIPAA Rules due to willful neglect.

The rule requires HHS to investigate all possible, rather than probable, violations of HIPAA due to willful neglect. In addition, HHS may now move directly to a civil money penalty without exhausting information resolution efforts, particularly in cases involving willful neglect violations.

Enforcement of the HIPAA rules is further strengthened by allowing HHS to coordinate with and disclose PHI as necessary to other law enforcement agencies, such as with the State Attorneys General pursuing civil actions to enforce the HIPAA rules on behalf of state residents or the FTC pursuing remedies under other consumer protection authorities.

The rule also incorporates the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim Final Rule on October 30, 2009. Prior to this change, the total amount imposed on a covered entity for all violations of an identical requirement during a calendar year could not exceed $25,000. The change now allows HHS to impose a civil monetary penalty with a maximum of $1.5 million for all violations of an identical requirement in a calendar year . The new rule also removes affirmative defenses against the imposition of such penalties, so that business associates and covered entities can no longer plead ignorance of the violation. Lack of knowledge of the violation is now punishable under the lowest tier of penalties – at least $100 per violation. .

New Breach Notification Standard

The Breach Notification Rule implements section 13402 of HITECH by requiring covered entities and their business associates to provide notification following a breach of unsecured PHI.

The rule changes the standard for when a covered entity or its business associate must provide notification of a breach of the security rules from the subjective "harm" standard to an objective standard.

Before the change, covered entities were only required to report a breach if the unauthorized disclosure of information presented a significant risk of financial, reputational, or other harm to the patient. The new rule, however, presumes a breach unless a covered entity or business associate can demonstrate a low

One East Washington Street
Suite 2400
Phoenix, AZ 85004

probability that the PHI has been compromised. A covered entity or business associate should consider the following four factors in determining whether PHI has been compromised:

1. the nature and extent of the PHI involved, including the type of identifiers;
2. the unauthorized person who impermissibly accessed the PHI or to whom the impermissible disclosure was made;
3. investigation of the disclosure to determine if the PHI was actually accessed or viewed, or if the opportunity merely existed but was not taken advantage of; and
4. the extent to which the risk to the PHI has been mitigated

Unless a covered entity or its business associate is able to make a showing under these four factors of a low probability that the PHI has been compromised, the new rule requires the entity to notify the patients and the Secretary regardless of the risk of harm where there is an unauthorized disclosure.

Other Notable Changes

The Final Rule is expansive and contains additional important changes that will affect covered entities and their business associates alike. The following changes are worth noting:

1. Updates the definition of "electronic media" to comport with modern and evolving technology.
2. Requires covered entities to obtain authorization from an individual for any disclosure of the individual's PHI in exchange for direct or indirect remuneration.
3. Grants individuals enhanced rights to receive electronic copies of their PHI and restricts disclosure to a health plan concerning treatment for which the individual pays out of pocket in full.
4. Requires covered entities to change their privacy notices to describe certain uses and disclosures of PHI and to redistribute to patients.
5. Modifies the definition of PHI to not include individually identifiable health information of persons who have been deceased for over 50 years and modifies individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools.
6. Prohibits health plans from using or disclosing genetic information for underwriting purposes, as required by the Genetic Information Nondiscrimination Act.

One East Washington Street
Suite 2400
Phoenix, AZ 85004

Conclusion

The Final Omnibus HIPAA Rule makes sweeping changes that covered entities and business associates alike should pay attention. The biggest change is the expansion of liability for HIPAA violations to business associates, which now includes subcontractors and any entity which transmits, stores, or maintains PHI on behalf of a covered entity. Any entity dealing with protected health information should be sure to take note of these HIPAA change and ensure compliance within the next 180 days.

Ishra M. Solieman
Phoenix
isolieman@bhfs.com
602.382.4058

Darryl T. Landahl
Phoenix
dlandahl@bhfs.com
602.382.4071