ROBINSON & COLE LLP
ATTORNEYS AT LAW

Attorney Advertising

UPDATE
Health Law Pulse

FEBRUARY 2013

U.S. Department of Health and Human Services Releases HIPAA Omnibus Rule

On January 25, 2013, the Department of Health and Human Services (HHS) published a final rule modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules (referred to as the Omnibus Rule or the Rule). The Omnibus Rule (1) strengthens the privacy and security protection for individuals' health information, (2) modifies the breach notification rule consistent with the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), and (3) bolsters privacy protections for genetic information. The Final Rule becomes effective on March 26, 2013, and covered entities and business associates must comply by September 23, 2013.

Highlights about the following provisions of the Omnibus Rule are summarized below:

GENERAL CHANGES TO DEFINITIONS

Definition of Business Associate

The Omnibus Rule expands the definition of "business associate" in several important ways:

- **First**, the definition now includes "patient safety activities" in the list of functions that qualify a person as a business associate. Accordingly, Patient Safety Organizations (PSOs) that review and provide analysis of patient safety events or provider concerns are now required to be treated as business associates.

- **Second**, business associates are expanded to include any person or organization that provides data transmission services regarding protected health information (PHI) to a covered entity and that requires routine access to such PHI. Two examples that fall under this definition are health information organizations and e-prescribing gateways. However, HHS has specifically declined to define what type of entity qualifies as a health information organization. Also, HHS does not quantify how much access constitutes "routine access," as used in the definition. HHS stated that additional guidance on this subject will be provided through the HHS website.
- **Third**, the definition of business associate has also expanded to include any person who offers a personal health record to one or more individuals on behalf of a covered entity in compliance with the express requirements of the HITECH Act. An example of someone who "offers" a personal health record is a personal health record vendor who establishes electronic means with a covered entity to deliver PHI to individuals. Further, HHS does not specify what types of activity are considered to be "on behalf of," stating that such determinations are fact specific based on the nature of services provided and the extent to which the entity needs access to the PHI to perform the service for the covered entity.
- **Fourth**, subcontractors that create, receive, maintain, or transmit PHI on behalf of business associates are now considered to be business associates themselves. Accordingly, HHS has clarified that a subcontractor is a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for the covered entity; it is not a person who provides a service for the business associate for its own management or who does not have access to PHI.

Covered entities may want to consider reviewing their existing vendor relationships to ensure that business associate agreements have been entered into with the entities that meet the expanded definition of business associates.

Definition of Electronic Media

Electronic Media is broadly defined as something having the ability to store PHI. Covered entities and business associates must safeguard any Electronic Media that has such storage capability. The Omnibus Rule has expanded the definition to include any electronic storage media on any device on which data is or can be recorded electronically. Additionally, the intranet is now included as a means by which the transmission of Electronic Media can occur. In response to commenters' concerns regarding the storage capabilities of photocopiers, facsimile machines, and other office machines, HHS has emphasized that whenever PHI is stored on such machines, even inadvertently, it is subject to the Privacy and Security Rules.

Other Definitions

- The definition of PHI has been revised to clarify that individually identifiable health information of individuals deceased for more than 50 years is no longer considered to be PHI.
- The definition of "health care operations" has been expanded to include "patient safety activities," such as efforts to improve patient safety and the quality of health care delivery as well as the collection and analysis of patient safety work product.
- The definition of "marketing" has been revised to require authorization for all communications for which the covered entity or business associate receives financial

remuneration unless an exception applies.

THE PRIVACY RULE

The Omnibus Rule implements certain provisions of the HITECH Act, improves the flexibility and effectiveness of the Rule, and conforms the Privacy Rule to the Patient Safety and Quality Improvement Act of 2005.

Applicability

The Omnibus Rule ensures that the Privacy Rule is applicable to business associates as well as to covered entities. It also expands the applicability of the Privacy Rule to a business associate's subcontractor(s) who are now directly liable for noncompliance under the HIPAA rules. The business associate also has the obligation to ensure the subcontractor's compliance with the Privacy Rule.

Business Associate Permitted Uses and Disclosures

A business associate is liable for any impermissible use or disclosure of PHI. Accordingly, a business associate can only disclose PHI as permitted by its business associate agreement unless otherwise required by law. A business associate is allowed to disclose PHI to a subcontractor of such business associate provided that the business associate receives notice such that the subcontractor will treat the PHI in an appropriate manner.

The Omnibus Rule also makes covered entities and business associates liable for the acts of their business agents, regardless of whether the covered entity has a business associate agreement in place. Previously, a covered entity would not have been liable for the acts of its agent provided (1) the agent was a business associate, (2) there was a compliant business associate agreement in place, (3) the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and (4) the covered entity did not violate the Privacy or Security Rule. This change was made to ensure that the covered entity or business associate would remain liable for its obligations even if they had been delegated to another party. To determine if an agency relationship exists, HHS will assess the totality of the circumstances.

Sale of Protected Health Information

The HITECH Act introduced a prohibition on the sale of PHI without authorization. The Omnibus Rule defines "sale of protected health information" as "a disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of PHI in exchange for PHI" unless otherwise excepted. Two such exceptions noted by HHS are (1) payment by a research sponsor to a covered entity conducting a research study, as the PHI is merely a byproduct of the research service being provided and (2) the receipt of a grant or funding from a governmental agency to conduct a program. Additionally, HHS has clarified that the exchange of PHI through a health information exchange is exempt from the definition of sale because the fees assessed are for services provided.

Moreover, HHS has clarified that disclosures of PHI for the sale, transfer, merger, or consolidation of all or part of a covered entity to another covered entity and the due diligence

related to such transfer are exempt from the definition of sale of PHI.

Other Uses and Disclosures of PHI: Decedents and Proof of Immunization

Under the Omnibus Rule, a covered entity may disclose PHI of a decedent to family members and others involved in the care or payment of the decedent prior to the decedent's death unless the covered entity has prior knowledge that disclosing PHI would be contrary to a decedent's wishes. Additionally, a covered entity may disclose proof of immunization where state law requires such proof before admission of a student. Although written authorization to disclose immunization information is no longer required, a covered entity must still obtain verbal authorization from a parent or guardian, or the individual in the case of an emancipated minor.

Notice of Privacy Practices for Protected Health Information

Prior to the Omnibus Rule, the notice of privacy practices (NPP) was required to contain (1) a general description of the types of uses and disclosures the covered entity may make for treatment, payment, and health care operations, including one example of a use or disclosure for each of treatment, payment, and health care operations and (2) a description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without written authorization. Under the Omnibus Rule, the NPP must also now include (1) a separate description of the types of uses and disclosures that require authorization, including psychotherapy notes (when appropriate), marketing purposes, and the sale of PHI and (2) a statement regarding fundraising communications and the individual's right to opt out of receiving such communications. The notices in the NPP must also reflect any more stringent law that may be applicable and must include descriptions that are sufficient in detail to place the individual on notice of the uses and disclosures that are permitted or required.

Health care providers must include a statement that individuals may restrict certain disclosures of PHI when they pay for a health care item or service out of pocket. Finally, the NPP must include a statement regarding the individual's right to be notified of a breach of unsecured PHI. Health providers are required to post the revised NPP in a clear and prominent location and have copies of the NPP available for individuals upon request. Health plans are required to inform members of the change to the NPP within 60 days of the revision.

Right to Request a Restriction of Uses and Disclosures

The Omnibus Rule requires covered entities to comply with an individual's request to restrict the disclosure of PHI in certain circumstances. Two requirements must be met. First, the disclosure must not otherwise be required by law, and second, if the request for restriction is on disclosures of PHI that solely pertain to a health care item or service, the health care provider must be paid in full by the individual before the provider is required to observe the restriction.

The right to request a restriction on the disclosure of PHI raises important issues in a variety of circumstances. HHS has clarified certain components of this right, and some highlights from the clarification follow below:

- **Medical Records**: Health care providers are not required to create separate medical files for the PHI subject to a restricted health care item or service but will have to implement safeguards to ensure that such information is not inadvertently sent or made accessible.

- **Bundled Services**: In the event that an individual requests a restriction of PHI to only some of the services rendered in a single encounter, HHS advises that the provider make the client aware of the difficulties of unbundling services and that, even in the event the provider is able to unbundle the services, there is still the potential for a health plan to deduce what services were performed. In the event that a provider is unable to unbundle the services, the provider should give the option to the individual to pay for the bundled services out of pocket.
- **Invalid Payment**: If payment by an individual is rejected, a provider is no longer required to abide by the individual's request to restrict PHI. That said, HHS expects a provider to make efforts to try to obtain proper payment before dishonoring such a request. To potentially avoid such conflict, HHS suggests that a provider can require payment to be made in full at the time by which individuals request the disclosure of their PHI to be restricted.
- **Downstream Services**: HHS has clarified that it is the responsibility of the individual, not the provider, to advise downstream providers (i.e., pharmacies, specialists, etc.) of a restriction on the disclosure of PHI although HHS encourages providers to counsel individuals of such responsibility if they choose to continue the restriction.
- **Follow-Up Care**: When a provider renders follow-up care to an individual, and the individual does not request a continuance on their restriction of PHI or pay out of pocket for the services, the provider can submit previously restricted PHI to a health plan, if it is necessary to classify the medical necessity of the service, without authorization from the individual.
- **Mandatory Billing**: If federal law mandates a covered entity or provider to submit PHI to a government health plan, for example, mandatory claim submission provisions of the Social Security Act, a provider must do so; however, if an individual does not authorize a submission to Medicare and pays out of pocket, the provider must comply with the request for a restriction on the submission of the PHI.

It is important for covered entities to review policies and procedures to ensure compliance with the situations described above, and to examine whether mechanisms need to be built into any existing electronic systems to abide by the restrictions on disclosure of PHI.

Access of Individuals to Protected Health Information

The Omnibus Rule strengthens individuals' right to access their own PHI. Covered entities and business associates are now required to provide electronically stored PHI within 30 days of an individual's request. Covered entities and business associates may charge the individual for the actual cost of providing the PHI.

Modifications to the HIPAA Privacy Rule under GINA

The Genetic Information Nondiscrimination Act of 2008 (GINA) is a federal law prohibiting discrimination of health coverage and employment based on an individual's genetic information. The aim of GINA is to prohibit a health plan from using or disclosing genetic information for underwriting purposes. The Omnibus Rule extends the scope of GINA to all health plans subject to the Privacy Rule. The Omnibus Rule adds numerous definitions to conform with GINA, explains how to comply with the new regulations, and describes how to incorporate the regulation into the notice of privacy practices (NPP). Some of the modifications to GINA are described in further detail below.

Definitions

- The term "health information" now includes genetic information.
- The definitions for "genetic information," "genetic test," and "family member," as defined in GINA, have been adopted to align GINA and HIPAA.
- The Omnibus Rule adopts the proposed definition for "manifestation" or "manifested." GINA uses these terms in a variety of contexts, including for when genetic information can be included in family medical history. The Rule's definition provides that a disease, disorder, or pathological condition has "manifested" when such condition could have been reasonably diagnosed by a health professional.

Uses and Disclosures of PHI

The Omnibus Rule has adopted the proposed prohibition on health plans and business associates from using or disclosing genetic information for underwriting purposes, except for long-term care policies. Health care providers can still disclose genetic information as necessary for treatment purposes.

Notice of Privacy Practices for PHI

The Omnibus Rule requires health plans that use or disclose PHI for underwriting purposes to include such a statement in their NPP. The Omnibus Rule also prohibits health plans from using or disclosing any PHI that contains genetic information about an individual.

THE SECURITY RULE

The Omnibus Rule revised the Security Rule to apply directly to business associates and to the health care components of hybrid entities. Hybrid entities are now also required to include all business associate functions within its health care component. Not doing so allows the health care component of a hybrid entity to avoid direct liability and compliance obligations for its business associate components.

THE ENFORCEMENT RULE

The HITECH Act requires the Secretary of the HHS (Secretary) to investigate complaints and to impose a civil money penalty for violations of the Act (referred to as the "Enforcement Rule"). The Omnibus Rule provides HHS with greater flexibility to carry out the Enforcement Rule by allowing more cooperation between HHS and other law enforcement agencies. The Omnibus Rule also creates a harm-based structure for determining civil money penalty amounts.

Compliance and Investigations

The Omnibus Rule makes it mandatory that the Secretary investigate any complaint against a covered entity or a business associate of a possible HIPAA violation due to willful neglect. The Omnibus Rule also requires the Secretary to review covered entity and business associate

compliance with the applicable administration simplification provisions when a preliminary review suggests there is a willful neglect violation. The Secretary retains the discretion to investigate other complaints and to initiate other compliance reviews. In addition, the Omnibus Rule permits the Secretary to disclose PHI to other law enforcement agencies if permitted under the Privacy Rule.

Civil Money Penalty (CMPs) Tiers

The HITECH Act established four tiers of CMPs corresponding to the levels of culpability associated with the violation:

1. the violation was caused without the knowledge of the covered entity or business associate, and the covered entity or business associate would not have known of the violation even by exercising reasonable diligence;
2. the violation was due to reasonable cause and not to willful neglect;
3. the violation was caused by willful neglect and was corrected within a certain time period; and
4. the violation was caused by willful neglect and was not corrected.

The Omnibus Rule revises the definition of "reasonable cause" as used in the second tier to include violations "due both to the 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 administrative simplification provision, as well as to other circumstances in which a covered entity or business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations."

CMPs Amounts

The Omnibus Rule imposes a new method to calculate CMPs that is tied to the four tiered levels of culpability.

Violation Category	Each Violation	Maximum Penalty for All Such Violations of an Identical Provision in a Calendar Year
1. Did Not Know	$100 - $50,000	$1,500,000
2. Reasonable Cause	$1,000 - $50,000	$1,500,000
3. Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
4. Willful Neglect - Not Corrected	$50,000	$1,500,000

Factors Considered in Determining Amount of CMPs

The Secretary considers the following factors when assessing the amount of a CMP: the

nature and extent of the violation; the nature and extent of resulting harm; the history of the covered entity or business associate's prior compliance; the financial condition and size of the covered business entity or business associate; and other matters as justice may require. The Secretary has the discretion whether to treat any one of the factors as aggravating or mitigating.

HHS clarified that each individual affected by a breach impacting multiple individuals, such as a breach of unsecured PHI, constitutes a separate violation. In addition, HHS has noted that with respect to a continuing violation, each day of noncompliance constitutes a separate violation. Furthermore, HHS has clarified that the maximum penalty imposed could be greater than $1.5 million if there are multiple violations across different violation categories.

THE BREACH NOTIFICATION RULE

The Omnibus Rule makes certain changes to the Breach Notification Rule in accordance with the HITECH Act. The HITECH Act enhances the responsibilities that covered entities and business associates have under HIPAA. A key requirement of the HITECH Act is that covered entities and business associates must provide notification when a breach of PHI to unauthorized individuals has occurred unless such PHI had been rendered unusable, unreadable, or indecipherable through encryption or destruction.

Definition of Breach

The Omnibus Rule presupposes that any unauthorized use or disclosure of unsecured PHI is a "breach." In order to not be classified as a breach and thereby not be required to send a breach notification, the Omnibus Rule requires an objective risk assessment to determine whether an impermissible use or disclosure of unsecured PHI has occurred. A breach has occurred unless the analysis of the risk assessment exhibits a low probability that the PHI has been compromised.

While the Omnibus Rule does not establish a bright-line standard of when a breach has occurred, the new definition of breach requires the covered entity to consider the following four factors as part of the risk assessment to determine whether a breach has occurred:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
2. the identity of the unauthorized person that used the PHI or to whom the disclosure of PHI was made;
3. whether or not the PHI was actually acquired or viewed; and
4. the extent to which the risk of PHI has been mitigated.

Covered entities and business associates may want to examine and revise their policies regarding investigation of a potential breach to ensure that such policies reflect at least the required factors mentioned above, and apply the four factors mentioned above to determine the likelihood of whether any PHI has been compromised. Under this new definition, covered entities and business associates must demonstrate that either all notifications were provided or show proper documentation, via a risk assessment analysis, that there was a low probability that PHI was compromised.

EFFECTIVE DATES

The Omnibus Rule increases the burden on covered entities, business associates, and their subcontractors by effectively requiring all business associates and subcontractors to comply fully with the HIPAA privacy rules. Such a change requires most covered entities to modify their current business associate agreements to address these new requirements by the compliance date of September 23, 2013. However, HHS has included in the Omnibus Rule a grandfathering provision providing that if a covered entity had a business associate agreement in place prior to January 25, 2013, and that business associate agreement is not renewed or modified between March 26, 2013, and September 23, 2013, then such agreements will not need to be modified to comply with the new standards until the earlier of September 22, 2014, or the date on which the agreement otherwise renews or is modified.

If you have any questions regarding any portion of the Final Rule regarding modifications to the HIPAA rules please contact a member of Robinson & Cole's Health Law Group.

Lisa M. Boyle	Theodore J. Tucci	Stephen W. Aronson
Michael J. Kolosky	Charles W. Normand	Pamela H. Del Negro
Teri E. Robins	Brian D. Nichols	Susan E. Roberts
Meaghan Mary Cooper	Eric R. Greenberg