HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

June 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

High-level stress:
Remembering the first OIG Medicare Compliance Review

an interview with Tessa Lucey

Corporate Compliance Officer/Chief Privacy Officer

See page 16

by Adam H. Greene, JD, MPH and Rebecca L. Williams, JD, RN

Complying with the new HIPAA Omnibus Rule: Part 2

» The definition of business associate has been broadened.
» Business associate agreements are required for all qualifying, downstream subcontractors.
» Direct and vicarious liability for non-compliance has been increased in scope.
» Patient rights to access and restrict PHI disclosures are expanded.
» Enhanced enforcement of noncompliance due to willful neglect is likely.

Adam H. Greene *(adamgreene@dwt.com) is a Partner in the Washington DC offices of Davis Wright Tremaine LLP and Co-Chair of its Health Information Practice Group.* ***Rebecca L. Williams*** *(beckywilliams@dwt.com) is a Partner in the Seattle office of Davis Wright Tremaine LLP and Co-Chair of its Health Information Practice Group.*

This is the second part in a two-part series designed to assist you in understanding the new rule. Part 1 (in our May 2013 issue) focused on changes to the breach notification standard and new limits and flexibility on uses and disclosures of PHI. Part 2 explains new requirements for business associates and subcontractors, enhancements for patient rights, and enforcement clarifications.

On January 17, 2013, the Department of Health and Human Services (HHS) released the long-awaited "Omnibus Rule,"[1] which amends a wide range of privacy, security, and breach notification requirements under the Health Insurance Portability and Accountability Act (HIPAA)[2] and the Health Information Technology for Economic and Clinical Health (HITECH) Act.[3] The Omnibus Rule represents the most comprehensive set of changes to the HIPAA regulations since their inception, and it is important to understand how the changes apply to your organization.

Expansion of the definition of "business associate"

Greene

Williams

Covered entities, business associates, and subcontractors are facing a new world. The Omnibus Rule modifies the definition of a "business associate" to include an entity that "creates, receives, maintains, or transmits" protected health information (PHI) on behalf of a covered entity. This expanded definition seems likely to bring certain organizations into the business associate fold that previously may not have been affected, such as certain document storage organizations.

The Omnibus Rule also adds certain entities to the list of entities defined as business associates, including:

- Subcontractors
- Patient safety organizations
- Health information organizations (and similar organizations)
- E-prescribing gateways
- Vendors of personal health records that provide services on behalf of a covered entity

Business associate contracts

HHS emphasizes the continued need for business associate contracts, even though business associates now are held directly accountable for many provisions of HIPAA. HHS notes that business associate contracts are necessary to clarify and limit permissible uses and disclosures of PHI, ensure business associates are contractually responsible for activities for which they are not directly liable under HIPAA, and clarify respective responsibilities related to patient rights, such as access to PHI. Of note, each agreement in the business associate contract chain must be as-or-more stringent than the one above it regarding the uses and disclosures of PHI.

Covered entities likely will need to revise their business associate contracts to address some or all of the following:

- Require compliance with all applicable provisions of the Security Rule (not just the provisions set forth in the HITECH Act or the administrative, physical, and technical safeguards);
- Require reporting of breaches of unsecured PHI in accordance with the Breach Notification Rule (which encompasses both the timing and content of a business associate's breach notification to the covered entity);
- Revise provisions related to subcontractors (e.g., ensuring that the business associate passes on the same or more stringent restrictions to any subcontractor that creates, receives, maintains, or transmits PHI on the business associate's behalf); and
- Ensure that, if the covered entity delegates to the business associate any compliance obligations under the Privacy Rule (e.g., distributing the covered entity's Notice of Privacy Practices), the business associate will perform such obligations in

compliance with the Privacy Rule as if the business associate were the covered entity.

Subcontractors

As noted above, subcontractors are among the entities the Omnibus Rule pulls into the definition of business associate. The Omnibus Rule defines a subcontractor as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." This means that a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate is now itself a business associate and subject to the same HIPAA provisions applicable to business associates. This does not mean, however, that a covered entity is required to enter into a contract or other arrangement with business associate subcontractors. Rather, a covered entity only needs to contract directly with the business associate with which it has a direct relationship.

Direct liability

The Omnibus Rule makes business associates (and business associate subcontractors) directly liable for non-compliance with the Security Rule and with some of the Privacy Rule requirements of the business associate contract. HHS explains that directly liability will flow from the following violations:

- Impermissible uses and disclosures;
- Failure to provide breach notification to the covered entity;
- Failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate contract);
- Failure to disclose PHI where required by HHS to investigate or determine the business associate's compliance with HIPAA;
- Failure to provide an accounting of disclosures; and
- Failure to comply with the applicable requirements of the Security Rule.

Business associates also remain contractually liable for other requirements of the business associate contract.

Agency liability

Prior to the Omnibus Rule, covered entities generally could not be held liable for the actions of agents who were business associates if a valid business associate agreement was in place (there was an exception if the covered entity learned the business associate was violating its business associate contract and the covered entity failed to take appropriate action). The Omnibus Rule, however, eliminated the covered entity exception for business associate agents. As a result, HHS will be able to hold a covered entity liable for the actions of a business associate that qualifies as an agent.

In the Preamble to the Omnibus Rule, HHS clarifies that the essential factor in determining the existence of an agency relationship is whether the principal has the authority to control the questioned conduct of the agent in the performance of the agent's duties. If the principal lacks that authority (e.g., the principal's only recourse would be to modify the underlying agreement or sue for its breach), then the business associate will not be considered an agent and the covered entity cannot be held directly liable for the business associate's conduct. HHS further noted that the existence of federal agency will depend on the facts and circumstances of each relationship. Federal common law has identified several analytical factors that must be considered:

- When, where, and why the agent acted the way it did;
- Whether an agent's conduct was subject to the principal's control;

- Whether the agent was doing something that typically is done by such agents; and
- Whether the principal reasonably expected the agent to engage in the questioned conduct.

A covered entity will need to be sensitive to whether a business associate may qualify as an agent. In particular, a covered entity should be cognizant of contractual provisions that authorize the covered entity to provide interim instructions that control how the business associate performs the service (e.g., the business associate will perform certain services "in the time and manner" as instructed by the covered entity). When a business associate is an agent, the covered entity should consider whether it is reasonably monitoring the business associate's compliance obligations and whether any indemnification provision adequately protects the covered entity from potential liability based on the business associate's conduct.

A covered entity will need to be sensitive to whether a business associate may qualify as an agent.

Implementation deadline

Business associates, like covered entities, must comply with the Omnibus Rule's provisions by no later than September 23, 2013. The Omnibus Rule provides up to a one-year extension (until September 22, 2014) for updating business associate contracts that are not otherwise modified after March 26, 2013. Accordingly, for all business associate contracts that are modified after March 26, 2013, covered entities should ensure that such contracts reflect the Omnibus Rule (otherwise the parties will need to amend the contract by September 23, 2013). For contracts that are not modified after March 26, 2013 (e.g., evergreen contracts that are automatically renewed each year), covered entities have until September 22, 2014 to update the contracts.

Expanded individual rights under the Omnibus Rule

Finalizing provisions of the HITECH Act, the Omnibus Rule provides individuals with greater rights to access electronic copies of their PHI and greater ability to restrict when their information is shared with health plans. Additionally, covered entities will need to revise their Notices of Privacy Practices to reflect the Omnibus Rule's new rights and restrictions with respect to PHI.

Expanded rights to access PHI

The Omnibus Rule has expanded an individual's right to obtain an electronic copy of PHI stored electronically in a designated record set (e.g., medical records, billing records, and other records relied upon to make decisions about the individual). This is a relatively minor change. HIPAA already provided that an individual has the right to receive access in the form and format requested by the individual, if readily producible. If not readily producible, HIPAA previously required the covered entity to provide a hard copy. Under the Omnibus Rule, if an individual requests an electronic copy and the covered entity maintains the designated record set electronically, then the covered entity must continue to provide a copy in the form and format requested by the individual, if readily producible, but now must provide an electronic copy as a default if it cannot readily produce the requested form and format. For example, if a covered entity maintains an electronic medical record and the patient requests to receive

a copy of the medical record through a secure patient portal, but the covered entity does not offer such a patient portal, then the covered entity must provide the patient an electronic copy as a default (e.g., an electronic copy in PDF format provided on a CD or USB drive) rather than a hard copy.

The individual also has the right to direct that the copy of the PHI be transmitted directly to another person designated by the individual. A covered entity must comply with such a directive, as long as it is in writing, signed by the individual, and clearly identifies both the designated person and where to send the PHI. An authorization would not be required in such a situation.

As clarified in the Preamble to the Omnibus Rule, if an individual requests that a copy of his/her PHI be sent via unencrypted email, then a covered entity is permitted to do so, as long as the covered entity has advised the individual of the risks and the individual still prefers the unencrypted email. Covered entities may wish to document the individual's request and that the covered entity warned the individual of the risk in such circumstances.

Also, covered entities will have 30 days fewer to respond to requests for access when the information is maintained offsite. Previously, a covered entity had 60 days to respond to a request for access when the information was not accessible onsite. Under the Omnibus Rule, electronic and hard copy PHI, no matter where located, will need to be provided within 30 days (with a single 30-day extension permitted if the covered entity provides notice of the delay to the requesting individual within the initial 30 days).

The Omnibus Rule also clarifies the fees that may be charged (e.g., the covered entity may only charge its costs for copies to individuals, even if state law permits a greater charge).

Right of individuals to request restrictions on PHI

The Omnibus Rule incorporates the HITECH Act requirement that a covered entity comply with an individual's request to restrict uses and/or disclosures of PHI, such as disclosure to a health plan (or the plan's business associate) of his/her PHI that pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket and in full. There is an exception to this right for disclosures required by law, such as mandatory claim submission provisions under Medicare and similar requirements under Medicaid or state law.

This right extends to situations where a family member or other person, including another health plan, pays for the service on behalf of the individual.

> …the Omnibus Rule provides individuals with greater rights to access electronic copies of their PHI and greater ability to restrict when their information is shared with health plans.

It may be advisable for providers to collect payment up front in connection with these requests, to the extent permitted by law. According to the Preamble, if payment by an individual making a restriction request is dishonored, HHS expects providers to make a reasonable effort to contact the individual and obtain payment prior to billing the health plan. What efforts a health care provider must make is left to the

provider's policies and individual circumstances, consistent with its usual payment and collections processes.

With regard to referrals to and treatment by other providers in the future, it is the responsibility of the individual—not the provider—to notify subsequent providers of a restriction request. HHS, however, encourages providers to engage in dialogue with patients so that patients understand they may need to make the restriction request with a subsequent health care provider (e.g., a pharmacy) if they wish to avoid the information being disclosed to the health plan.

Updates to Notices of Privacy Practices

Providers and health plans likely will need to update their Notices of Privacy Practices (NPPs). These revisions include:

- The duty of a covered entity to notify affected individuals of a breach of unsecured PHI;
- The individual's right to opt out of receiving fundraising communications from the covered entity (only applicable if the covered entity uses PHI for fundraising and wishes to do so without authorization);
- The right of the individual to restrict disclosures of PHI to a health plan with respect to health care for which the individual has paid out-of-pocket and in full;
- The requirement for an authorization for uses and disclosures for marketing, sale of PHI; and for most uses and disclosures of psychotherapy notes; and
- In addition, most health plans will need to inform individuals of the prohibition against using or disclosing genetic information for underwriting purposes.

Covered entities also will want to review their NPPs to ensure that they accurately describe their privacy practices, especially in light of the Omnibus Rule's new requirements.

The requirements for distributing updated NPPs have been modified for health plans but not health care providers. Health plans may include their revised NPP in their next annual mailing (rather than within 60 days of the change) as long as they prominently post the revised NPP on their websites by the effective date of the material change to the NPP. Health plans that do not have customer service websites are required to provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the NPP.

Enforcement efforts continue to increase

HHS's HIPAA enforcement powers were significantly strengthened by the HITECH Act and the interim final enforcement rule. The Omnibus Rule left intact much of the HIPAA enforcement approach with some additional expansion and clarification.

The Omnibus Rule left intact much of the HIPAA enforcement approach with some additional expansion and clarification.

For instance, business associates (including their subcontractors) are now subject to civil money penalties and other enforcement actions for non-compliance with applicable provisions of HIPAA.

Another change under the Omnibus Rule provides HHS with discretion to resolve violations of HIPAA by informal means. Previously, HHS was required to seek informal resolution prior to imposing a civil money penalty. Under the Omnibus Rule, HHS may move directly to a civil money penalty, which may be especially likely when HHS determines that non-compliance is due to willful neglect.

The Omnibus Rule retains the definition of willful neglect as "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA. The HITECH Act requires HHS to formally investigate a complaint, which anybody can file, if a preliminary investigation indicates a possible (as opposed to probable) violation due to willful neglect. To implement that change, HHS amended the enforcement rule to eliminate its investigatory discretion in such cases, require a compliance review of the offending party, and mandate civil money penalties if willful neglect is found. HHS retains the discretion to investigate and to resolve complaints by informal means when there are not indications of willful neglect.

The Omnibus Rule also modifies the definition of reasonable cause, which relates to violations due to reasonable cause and not to willful neglect. Essentially, "reasonable cause" becomes anything where the entity knew of a violation (or through reasonable diligence would have known of the violation) but that does not arise to the level of "willful neglect." HHS revised the definition of reasonable cause to ensure that conduct always fits under one of the categories upon which the level of civil money penalty is based.

Finally, HHS revised the factors that may be considered in determining civil money penalty amounts. The factors are:

- The nature and extent of any violation, including the number of individuals affected and the duration of the violation;
- The nature and extent of any individual's resulting physical, financial, or reputational harm, including any hindrance to the individual's ability to obtain health care;
- The history of prior non-compliance, including similar prior indications of non-compliance and the offending party's responses to them;
- The financial condition of the offending party, including difficulties that could have

affected compliance or that could cause a money penalty to jeopardize the future provision of health care; and
- Such other matters as justice may require.

Steps for responding to Omnibus Rule changes

Given the Omnibus Rule's expansion of HIPAA obligations to business associates and subcontractors, organizations subject to HIPAA should consider taking the following steps:

- Revising business associate contract templates;
- Revisiting which third parties are and are not business associates, based on the revised template (i.e., covered entities may have more business associates);
- Beginning the painful process of examining, amending, and re-negotiating business associate agreements, including considering what due diligence and monitoring may be warranted in light of potential liability for business associates that are agents; and
- Evaluating existing liability coverage in light of these changes.

To address changes to enhanced patient rights, organizations should consider taking the following steps:

- Updating NPPs to ensure that they accurately describe the organization's privacy practices, and advising individuals of their rights to request and to restrict disclosures of PHI under certain circumstances;
- Targeting relevant training (e.g., training persons involved in processing patient requests for disclosures of PHI about patients' expended rights); and
- Implement systems to ensure that restricted PHI does not inappropriately go to health plans.

With respect to increased enforcement, covered entities may wish to:

- Perform a gap review of privacy, security, and breach notification policies, procedures, and training to comply with HIPAA (both new requirements of the Omnibus Rule and remaining requirements of prior HIPAA provisions) in order to avoid potential findings of "willful neglect";
- Review whether PHI is created, received, maintained, and transmitted throughout your organization and ensure that safeguards are working; and
- Focus on areas such as your Security Rule risk analysis, the protection of PHI on mobile devices, and the use of social media as areas that have been the subject of recent HHS guidance or areas that have become particularly high risk.

Organizations should remain mindful that they generally have until September 23, 2013 to comply with these new requirements.

1. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566-5,702 (Jan. 25, 2013) (to be codified at 45 C.F.R Parts 160 and 164).
2. Health Insurance Portability and Accountability Act of 1996, as amended, 42 U.S.C. §§ 1320d to 1320d-9.
3. Health Information Technology for Economic and Clinical Health, 42 U.S.C. §§ 17901 to 17954.