Advisory

JANUARY 2013

If you have any questions about this Advisory, please contact:

MICHELLE WILCOX DEBARGE
860.297.3702
mdebarge@wiggin.com

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

Keeping Up with HIPAA: OCR's New Omnibus Rule

Last week, the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published the long-awaited final HIPAA regulations commonly referred to as the Omnibus Rule. These new regulations (1) implement changes to HIPAA that were mandated by the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH); (2) finalize the 2009 Enforcement and Breach Notification Interim Final Rules; and (3) modify HIPAA's Privacy Rule to strengthen the protections for genetic information required under the Genetic Information Nondiscrimination Act of 2008 (GINA).

While many of the changes to the HIPAA regulations were expected, the Omnibus Rule will nevertheless require covered entities and business associates to modify their HIPAA policies, procedures and forms. The Omnibus Rule also extends HIPAA obligations to certain subcontractors of business associates. The new regulations become effective on March 26, 2013, but entities have an additional 180 days, until September 23, 2013, to become fully compliant. In certain circumstances, an additional year is provided to bring existing business associate agreements into compliance.

Following are some of the Omnibus Rule's most significant provisions:

BUSINESS ASSOCIATES

The Omnibus Rule amended the definition of business associate to explicitly include entities that "maintain" protected health information (PHI), Health Information Organizations, E-prescribing Gateways, and other entities that provide data transmission services with respect to PHI to a covered entity and that require access on a routine basis to such PHI. The preamble to the Omnibus Rule attempts to provide guidance on how to distinguish between business associates that maintain or transmit PHI and mere "conduits" of PHI that are not classified as business associates. OCR explains that the conduit exception is narrowly applicable to entities providing courier services, such as the United Parcel Service and their electronic equivalents, but not to data storage facilities that maintain PHI on a more permanent basis. Although OCR's intent to define business associates broadly is clear, the contours of this classification remain murky and the preamble states that OCR intends to issue further guidance in this area.

As expected, and as required by HITECH, the Omnibus Rule also applies HIPAA's Security Rule and enforcement provisions, as well as certain Privacy Rule provisions, directly to business associates. The Privacy Rule provisions that now apply directly to business associates include, among other things, requirements to: provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee; disclose PHI to the Secretary of HHS for purposes of determining HIPAA compliance; provide an accounting of disclosures; and limit uses and disclosures of PHI to the minimum necessary.

CONTINUED ON NEXT PAGE

Keeping Up with HIPAA: OCR's New Omnibus Rule CONTINUED

Most significantly, the new regulations extend the HIPAA business associate obligations to certain subcontractors of business associates. If a subcontractor of a business associate creates, receives, maintains, or transmits PHI on behalf of the business associate, the subcontractor is itself deemed to be a "business associate." These subcontractors will be directly liable under HIPAA as business associates and will have to comply with the Security Rule, the Breach Notification Rule, and certain Privacy Rule provisions, as summarized above. This expanded definition significantly increases HIPAA's applicability, changing the law from one that applied to a narrow category of covered entities and their business associates to one that potentially now applies across a wide range of different types of corporate entities.

BUSINESS ASSOCIATE AGREEMENTS

Whereas previously business associates were not required to have written agreements with their subcontractors to address the use, disclosure and safeguarding of PHI, the Omnibus Rule now requires a written agreement between a business associate and its subcontractor when the subcontractor creates, receives, maintains, or transmits PHI on behalf of a business associate.

Moreover, the Omnibus Rule requires that covered entities and business associates amend their business associate agreements to include some new provisions. Business associate agreements must now state that the business associate will: comply with the Security Rule; report breaches of unsecured PHI to the covered entity; and ensure that subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree in writing to the same restrictions and conditions that apply to the business associate with respect to such information. Business associate agreements will also be required to state that to the extent the business associate carries out a covered entity's obligation under the Privacy Rule, the business associate is required to comply with the requirements that apply to the covered entity in the performance of such obligation.

NOTICE OF PRIVACY PRACTICES

Covered entities will have to revise their Notice of Privacy Practices under the Omnibus Rule. The Omnibus Rule requires that the Notice include a statement that the individual has the right to opt out of fundraising communications; a description of the types of uses and disclosures that require an authorization; an explanation that the covered entity is required to agree to restrict disclosures of PHI to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual has paid in full; and a provision regarding the covered entity's breach notification obligations. If a health plan intends to use or disclose PHI for underwriting purposes, a statement must also be added regarding the prohibition on the use or disclosure of genetic information for underwriting purposes.

Health plans are no longer required to provide their Notice of Privacy Practices to individuals covered by the plan within 60 days of a material revision, provided that the health plan prominently posts the change or its revised notice on its website by the effective date of the material change and, in its next annual mailing, provides the revised notice or information about the material change and how to obtain the revised notice. A health plan that does not post its revised notice on its website must provide the revised notice 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.

BREACH NOTIFICATION

The Omnibus Rule generally adopted the Breach Notification Interim Final Rule without change, subject to one noteworthy exception. Under the Breach Notification Interim Final Rule, notification was not required unless the breach posed a significant risk of financial, reputational, or other harm to the individual. HHS removed the "significant harm" test, stating that it is "too subjective." Instead, the regulation provides that notification is "presumed" to be required, unless the covered entity or business associate demonstrates that there is a "low probability that the protected health information has been compromised based upon a risk assessment" that considers at least the following four factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

While these factors might overlap with the considerations under the old significant harm test, OCR intends for the new test to focus more on the objective evaluation of whether the information was compromised rather than on the more subjective assessment of harm to the individual.

CONTINUED ON NEXT PAGE

Keeping Up with HIPAA: OCR's New Omnibus Rule CONTINUED

MARKETING, FUNDRAISING, AND THE SALE OF PHI

With regard to marketing, the Omnibus Rule requires authorization before a covered entity can use and disclose an individual's PHI for the purpose of making a marketing communication whenever the covered entity receives financial remuneration for making the communication from a third party whose product or service is being marketed. As under HITECH, the Omnibus Rule includes an exception for refill reminders or other communications about a drug or biologic that is currently being prescribed for the individual if the financial remuneration received by the covered entity in exchange for the communication is reasonably related to the cost of making the communication.

The Omnibus Rule also included the HITECH prohibition against the sale of PHI, defined as the disclosure of PHI by a covered entity or business associate where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. A number of activities are not considered a sale of PHI, including the disclosure of PHI for public health purposes and research purposes where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI.

OCR also loosened HIPAA's fundraising restrictions to allow covered entities to use or disclose additional types of demographic information for fundraising purposes without an authorization. Specifically, covered entities can use the patient's name, address, age, gender, date of birth, treating physician, outcome status, and health insurance status for fundraising purposes without authorization. However, the new regulations also provide that every fundraising communication must provide the individual with a clear and conspicuous opportunity to opt out of further fundraising communications and that the opt out method may not cause the individual to incur an undue burden or more than nominal cost. Moreover, treatment or payment may not be conditioned on the individual's choice regarding receipt of fundraising communications. Finally, the covered entity must abide by any opt-out requests, but may provide an individual who has elected not to receive further fundraising communication with a method to opt back in to receive fundraising communications.

RESEARCH

The Omnibus Rule now allows an authorization for the use or disclosure of PHI for a research study to be combined with any type of written permission for the same study or another study, under certain circumstances.
In addition, in the preamble to the Omnibus Rule, OCR explained that it has changed its previous position concerning authorizations for future, unspecified research. Whereas OCR previously prohibited the practice, after March 26, 2013, the effective date of the Omnibus Rule, "covered entities that wish to obtain individual authorization for the use or disclosure of protected health information for future research may do so."

DECEDENTS

The new regulations amend the definition of PHI to exclude PHI regarding a person who has been deceased for more than 50 years. Also, OCR added a provision allowing a covered entity to disclose PHI about a deceased individual to a family member, other relative, or a close personal friend of the decedent, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the covered entity.

ACTION STEPS

Covered entities, business associates and subcontractors of business associates, as applicable, will need to begin taking steps as soon as possible to comply with the Omnibus Rule's provisions.

- **Revise Your Policies And Procedures and Re-Train.** Many of the changes outlined above will require revisions to written policies and procedures and the implementation of changes to actual practices. The Omnibus Rule made other changes to the HIPAA regulations as well, such as adding greater flexibility regarding disclosure of student immunization information to schools, specific requirements regarding requesting access to electronic PHI, and enhanced protections for genetic information. It is essential to become educated about how the Omnibus Rule will affect your organization so that you can revise policies, procedures, and practices, as necessary. You must also retrain your workforce, as necessary, on your updated policies and procedures.

- **Assess Whether You Are Subject to the Business Associate Requirements.** Business associates' subcontractors must carefully assess whether they are

CONTINUED ON NEXT PAGE

Keeping Up with HIPAA: OCR's New Omnibus Rule CONTINUED

directly liable under HIPAA. If so, the subcontractors will need to conduct a thorough risk assessment of the methods that they use to protect PHI, implement HIPAA-compliant policies and procedures, train their workforce, and enter into business associate agreements with their own subcontractors, if and as applicable. Although these tasks will likely require a significant investment of time, effort, and financial resources, HIPAA compliance is legally required, and these expenditures may be relatively small in comparison to the potential penalties that OCR may impose for noncompliance.

- **Inventory Vendors And Put in Place the Proper Written Agreements.** Since the Omnibus Rule mandates that business associate agreements contain new provisions, existing business associate agreements will need to be revised. This may be a colossal job for some organizations. Even though existing business associate agreements may be grandfathered-in until September 22, 2014 under certain circumstances, covered entities and business associates should start inventorying their arrangements and re-negotiating these business associate agreements now.

- **Audit Your Compliance.** Aside from the new requirements and the concomitant changes to policies, procedures, and arrangements, the release of the Omnibus Rule provides a good opportunity for covered entities and business associates to audit their HIPAA compliance. These new regulations are merely the latest wave in the new era of increased HIPAA enforcement since HITECH's enactment in 2009. Be sure that you are prepared to face an OCR audit or complaint investigation, that you feel confident about your level of compliance, and that you are in a position to defend your policies, procedures, and practices.

UPCOMING OMNIBUS RULE PROGRAMS

Wiggin and Dana will be offering educational presentations on the Omnibus Rule. The presentations will take place from 8:30 - 11:30 a.m. on the following dates:

- Wednesday, February 27 - New Haven office
- Friday, March 1 - Hartford office

Email rsvp@wiggin.com to RSVP. Please indicate which location you would like to attend in the body of the email.