

Highlights of the Omnibus HIPAA/HITECH Final Rule

Health Law Whitepaper

Katherine M. Layman

215.665.2746
klayman@cozen.com

Gregory M. Fliszar

215.665.7276
gfliszar@cozen.com

Judy Wang Mayer

215.665.4737
jmayer@cozen.com

Robert A. Chu

215.665.2101
rchu@cozen.com

William P. Conaboy

215.665.5580
wconaboy@cozen.com

On January 25, 2013, the Office of Civil Rights (OCR) of the Department of Health & Human Services (HHS) published the long-awaited omnibus final regulation governing health data privacy, security and enforcement (Omnibus Rule).¹ The Omnibus Rule is a group of regulations that finalizes four sets of proposed or interim final rules, including changes to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act² and proposed in 2010;³ changes to the interim final breach notification rule;⁴ modifications to the interim final enforcement rule; and implementation of changes to the Genetic Information Nondiscrimination Act of 2008 (GINA). The Omnibus Rule goes into effect on March 26, 2013, and compliance is required by September 23, 2013. As expected, the Omnibus Rule did not finalize the May 31, 2011 proposed regulation regarding accounting for disclosures.

As was made clear by the statutory mandate of HITECH, the most significant changes involve business associates who are now directly subject to the mandates of the HIPAA Privacy and Security Rules and HIPAA enforcement. In addition, covered entities will need to carefully evaluate changes to the breach notification rule, individual rights, additional requirements for Notices of Privacy Practices (NPPs) and the parameters around the use of protected health information (PHI) for marketing and fundraising.

Business Associates

The Omnibus Rule expands HIPAA's coverage to directly regulate business associates and other "downstream" entities. Compliance with the new regulations is required by September 23, 2013. For business associate agreements (BA agreements) that were in effect prior to January 25, 2013, covered entities have until September 23, 2014 to amend those BA agreements to comply with the new rules.

1. The Omnibus Rule Expands the Definition of Business Associate

The Omnibus Rule expands the definition of "business associate" to include subcontractors who create, receive, maintain, or transmit PHI on behalf of a business associate. A "subcontractor" is any downstream entity that has no direct contractual relationship with a covered entity, but to whom a business associate delegates a function, activity or service performed on behalf of the covered entity or business associate.⁵ The preamble to the Omnibus Rule explains that the expansion of the definition of business associate to include subcontractors was necessary to ensure privacy and security protections for PHI do not lapse when a business associate delegates authority to and shares PHI with a subcontractor. The definition of business associate was also broadened to include entities such as health information organizations that provide data transmission services to a covered entity that require access to PHI on a routine basis. The definition of business associate excludes "conduits," or entities that merely transfer PHI on behalf of a covered entity or business associate, such as the U.S. Postal Service or Internet service providers. However, the preamble to the Omnibus Rule stresses that the conduit exception is "a narrow one" and that an entity that "maintains" PHI on behalf of a covered entity is a business associate, not a conduit, even if the entity does not view the PHI.⁶ Thus, a data or document storage company that stores and has access to PHI would be considered a business associate, even if it never views the information.

2. The Omnibus Rule Directly Regulates Business Associates and Their Subcontractors

Prior to the Omnibus Rule, a violation of a BA agreement merely exposed a business associate or its subcontractor to contractual damages enforceable only by the covered entity or business associate that was a party to the BA agreement. Under the Omnibus Rule, however, business associates and their subcontractors are now directly governed by HIPAA, subjecting them to potential criminal and civil sanctions

for violations of HIPAA's Privacy and Security Rules to the same extent as covered entities. As referenced in the enforcement section below, these penalties can be substantial.

3. Portions of the Privacy and Security Rules Now Apply Directly to Business Associates

The Omnibus Rule sets forth specific violations of the Privacy Rule for which a business associate will be held liable. Under the Omnibus Rule, a business associate may be directly liable for violations of the Privacy Rule for:

- uses and disclosures of PHI in violation of its BA agreement and/or the Privacy Rule;
- failing to disclose PHI to the Secretary of HHS when investigating the business associate's compliance with the Privacy Rule;
- failing to provide breach notification to the covered entity;
- failing to disclose PHI to comply with an individual's request for PHI;
- failing to provide an accounting of disclosures; and
- failing to make reasonable efforts to limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose.⁷

In addition, the Security Rule now applies equally to all covered entities, business associates and subcontractors. Specifically, the Omnibus Rule now explicitly requires business associates and their subcontractors to comply with the Security Rule's administrative, technical and physical safeguard requirements.⁸ This will include, among other obligations, conducting a risk analysis, developing and implementing HIPAA security policies and procedures, and training staff on those policies. It is important that business associates and subcontractors who have not done the hard work to come into compliance with HIPAA's Security Rule requirements develop and implement HIPAA compliance programs and put into place appropriate safeguards as soon as possible.

4. Requirement That Business Associates Enter into Agreements with Their Subcontractors

Prior to the Omnibus Rule, business associates were merely required to "ensure" a subcontractor agreed to follow the same Privacy and Security Rules that the business associate had agreed to comply within its BA agreement with a covered entity. The Omnibus Rule now requires business associates to enter into formal BA agreements with their subcontractors. The Omnibus Rule further clarifies that agreements between a business associate and a subcontractor must contain the same requirements as the BA agreement between the covered entity and the business associate.⁹ In other words, each BA agreement in a chain of BA agreements must be equally comprehensive in setting forth the particular party's HIPAA obligations. For example, the preamble notes that if the initial BA agreement between a covered entity and its business associate does not permit de-identification of PHI, then each subsequent BA agreement between business associates and their subcontractors must also prohibit de-identification. The Omnibus Rule also states that a covered entity is not required to enter into a BA agreement with a subcontractor of its business associate as that requirement belongs exclusively to the business associate.¹⁰

5. Compliance

Certainly, covered entities and business associates will need to address the significant changes to the regulation of business associates in the Omnibus Rule. In regard to revising BA agreements, covered

entities that had BA agreements in place prior to January 25, 2013 will have until September 23, 2014 to amend those agreements to comply with the new rules. To assist with this undertaking, HHS recently published sample business associate provisions, which can be found [here](#).

Aside from reviewing BA agreements, it is imperative business associates and subcontractors begin to immediately review their privacy and security policies and develop rigorous programs to comply with the Omnibus Rule as enforcement against business associates will begin in September 2013.

Breach Notification

The Omnibus Rule made significant changes to the interim final breach notification rule by: (1) adding a presumption that any unauthorized use or disclosure of unsecured PHI is a breach; (2) removing the prior risk of harm standard; and (3) adding parameters for the risk assessment that should be conducted to determine if PHI has been compromised following an unauthorized use or disclosure.

1. Omnibus Rule Revises Definition of Breach by Adding Presumption of Breach

The Omnibus Rule revised the interim final rule's definition of breach to include a presumption of a breach. Under the interim final rule, a "breach" was generally defined to be "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information."¹¹ The Omnibus Rule revised the definition of breach by adding an express presumption that an impermissible use or disclosure of protected health information is a breach "unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised"¹² The agency explained that it added this express presumption to ensure uniform application of the breach notification rule. The express presumption is also meant to promote consistency with 45 C.F.R. § 164.414's burden of proof, which places the burden on covered entities and business associates to either prove that breach notifications were provided or that the impermissible use or disclosure did not constitute a breach.¹³

2. Omnibus Rule Removes "Harm Standard" and Modifies Risk Assessment

The Omnibus Rule also revised the interim final rule by removing the "harm standard," i.e., whether there was a significant risk of harm to the individual whose personal health information was impermissibly used or disclosed. As above, an impermissible use or disclosure of PHI is, under the Omnibus Rule, presumed to be a breach unless it can be demonstrated that there is a "low probability that the protected health information has been compromised." Accordingly, the Omnibus Rule replaced the risk of harm analysis with a four-part risk assessment that is to be conducted following an unauthorized use or disclosure of PHI that focuses on whether there exists a low probability that the PHI has been compromised.¹⁴ The four factors of the modified risk assessment are as follows:

- (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
- (iii) Whether the protected health information was actually acquired or viewed; and
- (iv) The extent to which the risk to the protected health information has been mitigated.¹⁵

HHS explains that all of the above factors must be evaluated in combination, and that, unless the evaluation

concludes there is a low probability the PHI has been compromised, the covered entity or business associate must make a breach notification.¹⁶

The preamble provides some guidance and examples regarding how to apply the factors.¹⁷ For example, with respect to the first factor, the agency explains how an entity might evaluate whether an individual can be re-identified from an improperly disclosed list of patient discharge dates and diagnoses. For the second factor, the agency explains that if the protected health information is impermissibly disclosed to an entity that must comply with the HIPAA rules or to a federal agency, there may be a lower probability that the health information is compromised because the recipient is required to protect the privacy and security of that information. For the third factor, the agency explains that a forensic analysis of the electronic protected health information might show that the protected health information was never actually viewed. For the fourth factor, the agency explains that entities could potentially mitigate the risks to the protected health information through agreements to destroy or maintain the confidentiality of the protected information. The agency recognizes the difficulty in evaluating the risks through these assessments and stated it will issue additional guidance with respect to frequently occurring improper use or disclosure scenarios.¹⁸ It is clear, though, that the burden is definitely on the covered entity and/or business associate to demonstrate that there is a low probability the PHI has been compromised.

Marketing and Fundraising

1. Marketing

The HIPAA Privacy Rule generally requires a covered entity to obtain authorization from an individual before using that individual's PHI for marketing purposes. Prior to HITECH, certain communications, including health-related communications, were excluded from the definition of marketing. The Omnibus Rule dramatically changes the definition of marketing by requiring authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being promoted. The term "financial remuneration" includes payments made in exchange for making communications about a product or service and does not include nonfinancial benefits.¹⁹ Accordingly, in order to make a marketing communication to an individual, the individual must provide a valid authorization, which, in addition to containing the elements and statements of a valid HIPAA authorization, must disclose the fact that remuneration is being received from a third party for making the communication.²⁰

A narrow exception still exists for prescription refill reminders as such communications are excluded from the definition of "marketing" so long as any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.²¹ Under this limited exception, a third party may cover the Covered Entity's cost of labor, supplies and postage to make the communication. Amounts in excess will constitute financial remuneration in violation of the exception and will require the covered entity to obtain a valid authorization.

Notably, the Omnibus Rule does not change the existing exceptions to the authorization requirement for face-to-face communications and promotional gifts of nominal value by a covered entity to an individual.²² In addition, communications promoting health in general and communications about government and government-sponsored programs are exempt from the marketing requirements.²³

2. Fundraising

Previously, the HIPAA Privacy Rule required that a covered entity make reasonable efforts to ensure individuals who opt-out do not receive further communications. The Omnibus Rule toughens that standard by making any further fundraising communications with a person who has opted out a violation of the HIPAA Privacy Rule.²⁴ Although the Omnibus Rule permits a covered entity to use or disclose certain limited PHI without an authorization for purposes of raising funds for its own benefit, a covered entity is now required to include in each fundraising communication a clear and conspicuous opportunity for the individual to whom the PHI relates to opt out of receiving further fundraising communications. The opt-out method used cannot cause the individual to incur an undue burden or more than a nominal cost, and a covered entity may not condition treatment or payment on the individual's choice. Once an individual opts out, the covered entity may not send fundraising communications to that individual.

3. New Requirements for Notices of Privacy Practices

The HIPAA Privacy Rule required covered entities to have and to distribute to individuals a Notice of Privacy Practices (NPP), which describes the uses and disclosures of PHI that the covered entity is permitted to make, information about privacy practices, the covered entity's legal duties and the individual's rights with respect to PHI.

The Omnibus Rule modifies and expands the statements that covered entities must include in their NPPs to ensure individuals are aware of the additional privacy protections and individual rights that were included in the HITECH Act.²⁵ Specifically, the Omnibus Rule amends the content requirements of the NPP to require the following:

- A statement that an individual's authorization is required for most uses and disclosures of psychotherapy notes (if the covered entity records or maintains psychotherapy notes), uses and disclosures of PHI for marketing purposes, disclosures that constitute a sale of PHI, and uses and disclosures other than those described in the NPP.
- If a covered entity intends to contact an individual for fundraising purposes, a statement of such intent and the individual's right to opt out of receiving fundraising communications.
- For health care provider covered entities, a statement informing individuals of the right to request the restriction of the disclosure of PHI to a health plan or other party when the PHI relates solely to a health care item or service for which the individual, or another person on behalf of such individual (other than a health plan), has paid the covered entity, and that the health care provider covered entity is required to agree to such request.
- For health plan covered entities (other than certain issuers of long-term care policies) that intend to use or disclose PHI for underwriting purposes, a statement that the health plan covered entity is prohibited from using or disclosing PHI that is genetic information about an individual for such purposes.
- A statement describing an individual's right to be notified following a breach of unsecured PHI.

The Omnibus Rule does not modify the current requirement that covered entities must redistribute its NPP when there has been a material change to it.

Individual Rights

1. Restrictions on Uses and Disclosures of PHI

Under the HIPAA Privacy Rule, an individual is permitted to request that the covered entity restrict both the use and disclosure of PHI for treatment, payment or health care operations and disclosures to others who are involved in the individual's care or payment for that care. However, a covered entity has not been required to agree to a requested restriction. The Omnibus Rule adds a provision that requires certain covered entities to agree to requests to restrict disclosure if the disclosure would be for the purpose of payment or health care operations, the disclosure is not otherwise required by law, and the PHI pertains only to a health care item or service for which the individual or another person (other than a health plan) has paid in full.²⁶ HHS commented that while covered entities are not required to create separate medical records or otherwise segregate PHI subject to this restriction, covered entities will need to somehow flag in the record PHI that has been restricted.

2. Request for Access to PHI

The HIPAA Privacy Rule currently provides that an individual is permitted to review or obtain copies of his or her PHI that is maintained in a designated record set and, subject to limited exceptions, a covered entity must grant that access (or provide a written explanation of why access is being denied) within 30 days after receipt of the request.

The Omnibus Rule amends the Privacy Rule to require that if the requested PHI is maintained electronically, and the individual requests an electronic copy, the covered entity must provide the PHI in the electronic form and format requested by the individual if the PHI is readily producible in that form and format.²⁷ If not, the covered entity must provide the PHI in a readable electronic form and format that is acceptable to the individual. In addition, if an individual requests his or her PHI be provided directly to another person, the covered entity must comply with the request if the request is in writing, signed by the individual, and identifies the designated person and where to send the PHI.

The Enforcement Rule

1. Investigations and Compliance Reviews

The Omnibus Rule clarifies the parameters in which HHS will investigate a potential violation or initiate a compliance review. Under the Omnibus Rule, HHS is required to investigate a complaint if a preliminary review of the facts indicates a possible HIPAA violation due to willful neglect.²⁸ Similarly, HHS must conduct a compliance review to determine whether a covered entity or business associate is complying with HIPAA when a preliminary review of the facts indicates a possible violation due to willful neglect.²⁹ The preamble explains that compliance reviews may be used by HHS to investigate allegations of HIPAA violations brought to its attention through a media report or from a state or another federal agency. In cases where the initial review does not indicate a possible violation due to willful neglect, HHS retains the discretion to either investigate the matter further or conduct a compliance review.³⁰

The Omnibus Rule also contains a subtle change in language that will likely have a profound impact on enforcement. Previously 45 C.F.R. § 160.312(a)(1) provided that if an investigation of a complaint or compliance review indicates noncompliance with HIPAA, HHS will attempt to reach a resolution of the matter through informal means. The Omnibus Rule changes "will" to "may," which means HHS may now move directly to a civil monetary penalty without having to exhaust informal resolution efforts.

2. Business Associates

The Omnibus Rule also clarifies that business associates (which, as above, are now defined to include subcontractors) are directly subject to HIPAA's enforcement provisions.³¹ In addition, the Omnibus Rule also provides that a covered entity is liable for a civil monetary penalty based on the act or omission of business associates or other agents acting within the scope of agency.³² The preamble explains that the analysis of whether a business associate is an agent will be done in accordance with the federal common law of agency and will be fact specific, taking into account the terms of the BA agreement as well as the totality of the circumstances between the parties. Further, the essential factor in determining if such a relationship exists is the right or authority of a covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity.³³

3. Civil Monetary Penalties

Prior to HITECH, HHS was only authorized to impose civil monetary penalties of no more than \$100 per violation, with the annual amount of penalties for all violations of one provider capped at \$25,000. Under HITECH and the Omnibus Rule, the penalties are as follows:³⁴

- If the covered entity or business associate did not know of the violation and would not have known of the violation by exercising reasonable diligence, the penalties are no less than \$100 and no more than \$50,000 per violation, with an annual cap of \$1,500,000 for identical violations.
- If the HIPAA violation is due to reasonable cause and not to willful neglect, the penalties are no less than \$1,000 and no more than \$50,000 per violation, with an annual cap of \$1,500,000 for identical violations.
- If the HIPAA violation is due to willful neglect, but was corrected within 30 days of the covered entity or business associate discovering the violation, the penalties are no less than \$10,000 and no more than \$50,000 per violation, with an annual cap of \$1,500,000 for identical violations.
- If the HIPAA violation was due to willful neglect and was not corrected within 30 days, the penalties are no less than \$50,000 per violation, with an annual cap of \$1,500,000 for identical violations.

4. Factors Considered in Determining the Amount of a Civil Monetary Penalty

Once HHS has determined that a violation of HIPAA has been committed, it will consider a number of factors when determining the penalty to be imposed. The first factor considered is the nature of the violation, which includes a review of the number of individuals affected and the time period during which the violation occurred. The second factor is the nature and extent of the harm resulting from the violation, which includes physical harm, financial harm, reputational harm and whether the violation hindered an individual's ability to obtain health care. The third factor is the entity's history of compliance/noncompliance with HIPAA. The fourth factor relates to the financial condition of the covered entity or business associate and the entity's ability to comply with HIPAA as well as whether the penalty would jeopardize the covered entity or business associate's ability to provide or to pay for health care.³⁵

5. Affirmative Defenses

The Omnibus Rule modifies the affirmative defenses available to covered entities and business associates. The Omnibus Rule provides that a civil monetary penalty may not be imposed on a covered entity or

business associate if a criminal penalty has already been imposed for the same violation. In addition, the Omnibus Rule also limits the affirmative defenses available to an entity that violates HIPAA. If the violation occurred prior to February 18, 2009, the Secretary of HHS is not allowed to impose a civil monetary penalty if the entity did not have knowledge of the violation, nor would have known of the violation through reasonable diligence. For violations occurring on or after February 18, 2009, an affirmative defense is available only if the violation was not due to willful neglect and was corrected within 30 days of when the entity knew, or by exercising “reasonable diligence” would have known, of the violation.³⁶

6. Impact

The Omnibus Rule significantly strengthens HIPAA enforcement, which should be of concern to all covered entities and particularly to business associates. Over the last two years OCR has become much more aggressive in enforcing HIPAA and now has a more robust enforcement rule at its disposal. Thus, it is more important than ever for covered entities and business associates to understand their obligations under HIPAA and have compliance programs in place to help make sure those obligations are met.

(Endnotes)

- 1 78 Fed. Reg. 5,566 (Jan. 25, 2013) (the complete Omnibus Rule can be [found here](#)).
- 2 Title XII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb. 17, 2009).
- 3 75 Fed. Reg. 40,868 (July 14, 2010).
- 4 74 Fed. Reg. 42,740 (Aug. 24, 2009).
- 5 45 C.F.R. § 160.103, 78 Fed. Reg. at 5573.
- 6 78 Fed. Reg. at 5571-72.
- 7 45 C.F.R. § 164.502 (a)(3)-(4); 78 Fed. Reg. at 5598-99.
- 8 45 C.F.R. § 164.104(b).
- 9 45 C.F.R. § 164.504(e)(5).
- 10 78 Fed. Reg. at 5573.
- 11 45 C.F.R. § 164.402.
- 12 78 Fed. Reg. at 5695 (to be codified at 45 C.F.R. § 164.402).
- 13 78 Fed. Reg. at 5641.
- 14 *Id.*
- 15 78 Fed. Reg. at 5695 (to be codified at § 164.402).
- 16 78 Fed. Reg. at 5643.
- 17 See 78 Fed. Reg. at 5642-43.
- 18 78 Fed. Reg. at 5643.
- 19 78 Fed. Reg. at 5593, 5595 (to be codified at 45 C.F.R. § 164.501).
- 20 42 C.F.R. § 164.508.
- 21 78 Fed. Reg. at 5596-97.
- 22 78 Fed. Reg. at 5596.
- 23 78 Fed. Reg. at 5597.
- 24 78 Fed. Reg. at 5680.
- 25 78 Fed. Reg. at 5624-26.
- 26 78 Fed. Reg. at 5626, 5628.
- 27 78 Fed. Reg. at 5631.
- 28 45 C.F.R. § 160.306(c)(1).
- 29 45 C.F.R. § 160.308(a).
- 30 78 Fed. Reg. at 5579.
- 31 45 C.F.R. § 160.402(a).
- 32 45 C.F.R. § 160.402(c).
- 33 78 Fed. Reg. at 5581.
- 34 45 C.F.R. § 160.404(b)(2).
- 35 45 C.F.R. § 160.408.
- 36 45 C.F.R. § 160.410.