January 2013

New HIPAA Omnibus Rule: A Compliance Guide

Introduction

The wait is over. On January 17, 2013, the Department of Health and Human Services' ("HHS'") Office for Civil Rights ("OCR") released its long-anticipated megarule ("Omnibus Rule") amending the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. These amendments implement and expand on the requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the Genetic Information Nondiscrimination Act of 2008. The Omnibus Rule is effective March 26, 2013, and compliance is required with respect to most provisions no later than September 23, 2013. Coming into compliance will require significant effort and attention by covered entities and business associates alike. This alert highlights some of the more significant aspects of the Omnibus Rule and provides critical compliance tips.

Expanded Pool of Business Associates and Enhanced Requirements

One of the biggest changes in the Omnibus Rule affects business associates that provide services (such as billing, administrative support or data analysis) to covered entities. Notably, the Omnibus Rule adds "subcontractors" to the definition of "business associate" to provide that subcontractors that perform functions for or provide services to a business associate are also deemed business associates when they create, receive, maintain or transmit protected health information ("PHI") on behalf of the business associate. The broad scope of the new definition of "business associate" means that any subcontractor, no matter how far removed from the original contractor, is considered a HIPAA "business associate" if it handles PHI. Because the Omnibus Rule applies the HIPAA Security Rule standards and implementation specifications and certain HIPAA Privacy Rule provisions directly to business associates, both business associates *and* their subcontractors must now develop comprehensive, written HIPAA security policies and procedures. They also must implement the highly prescriptive and onerous safeguards mandated by the HIPAA Security Rule. Business associates also must now enter into written contracts with subcontractors that contain specific provisions required by the HIPAA Privacy and Security Rules. Previously, business associates were only required to "ensure" that subcontractors agree to the same restrictions on the use and disclosure of PHI.

Additionally, the Omnibus Rule applies the "minimum necessary" standard directly to business associates and their subcontractors. When using, disclosing or requesting PHI, these entities must "make reasonable efforts to limit [the PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Because business associates and subcontractors now must comply with the minimum necessary standard, this change has the potential to significantly alter the flow of PHI from business associates and subcontractors. These organizations will need to focus more closely on what specific PHI they need to use, disclose or request to perform the relevant services.

Changes to the Breach Notification Framework

Another sweeping change produced by the Omnibus Rule affects the breach notification framework. In 2009, the HITECH Act established a statutory requirement for breach notification that obligated covered entities, which include health care providers, group health plans and health care clearinghouses, to notify

affected individuals, HHS and, in certain cases, the media of jurisdictions where more than 500 individuals are affected. The Interim Breach Notification Rule issued in August 2009 that implemented the HITECH Act's requirements defined a breach as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information." The phrase "compromises the security or privacy of the protected health information" was defined to mean "poses a significant risk of financial, reputational, or other harm to the individual." This harm threshold, which will remain effective until September 23, 2013, was significantly altered in the Omnibus Rule.

The harm threshold that had imposed a notification requirement only where there was a "significant risk" of harm to an individual was replaced by a presumption that any acquisition, access, use or disclosure of PHI not permitted under the HIPAA Privacy Rule is a breach unless a covered entity or business associate can demonstrate that "there is a low probability that the [PHI] has been compromised based on a risk assessment." The risk assessment must include consideration of the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.

For the first factor, organizations should focus on whether sensitive data, such as Social Security numbers and detailed clinical information, are involved in an incident. HHS has indicated that such sensitive data "could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests." With respect to the second factor, disclosures to another HIPAA-regulated entity or to a federal agency, for example, may result in a "lower probability that the [PHI] has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity." The third factor typically would involve a forensic analysis or investigation that could determine whether PHI contained on a lost or stolen laptop or other portable electronic device actually was viewed or accessed. Finally, the fourth factor might involve reaching out to an unauthorized recipient of the PHI to obtain "satisfactory assurances" that any PHI sent to a recipient was not further used or disclosed but instead destroyed.

HHS noted in the Omnibus Rule that it will issue future guidance on risk assessments associated with breaches, hopefully before September 23, 2013, when the new risk assessment requirement for breaches becomes effective. Until that occurs, however, it is critical that organizations focus on identifying any gaps in compliance that led to an incident and closing those gaps to ensure that another similar incident will not occur.

Marketing

The Omnibus Rule makes significant changes with respect to marketing communications. The basic definition of "marketing" remains the same — a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. The exceptions, however, have been rewritten. Under the Omnibus Rule, refill reminders or other communications about a drug or biologic currently being prescribed for the individual are generally not considered marketing, *but*

only if any financial remuneration[1] received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

- Permissible costs for which remuneration may be received are limited to the costs of labor, supplies and postage. If a financial incentive beyond the cost of making the communication is provided, the exception no longer applies and the communication constitutes marketing.

Additionally, the following treatment and health care operations communications are not considered marketing *so long as* the covered entity does not receive any financial remuneration (of any type) in exchange for making the communication:

- Communications for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual;

- communications to describe a health-related product or service (or payment therefor) that is provided by or included in a plan of benefits of the covered entity making the communication; or

- communications for case management or care coordination, contacting individuals with information about treatment alternatives and related functions to the extent these activities do not fall within the definition of "treatment."

Covered entities are required to obtain a valid authorization for any use or disclosure of PHI for marketing purposes, subject to two exceptions: (1) no authorization is required if the communication is made in a face-to-face encounter between the covered entity and the individual and (2) no authorization is required in the case of a promotional gift of nominal value provided by the covered entity. If the marketing activity involves financial remuneration to the covered entity from a third party, the authorization must state that remuneration is involved.

Accordingly, if a covered entity receives financial remuneration in excess of its costs to provide refill reminders, the communication will constitute marketing but no authorization will be required if the communication is accomplished in a face-to-face encounter between the covered entity and the individual. Similarly, if a covered entity receives financial remuneration of any type in return for care coordination communications, no authorization will be required if the communication is accomplished in a face-to-face encounter.

Sale of PHI

Under the Omnibus Rule, a covered entity or business associate must obtain an authorization for any disclosure of PHI that constitutes a sale of PHI. For purposes of this requirement, the "sale" of PHI means a 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, subject to the following exceptions:

- Disclosures for public health purposes;

- certain disclosures for research purposes (if the remuneration is limited to a reasonable, cost-based fee to prepare and transmit the PHI);

[1] Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or services are being described (but not including any payment for treatment of an individual). Nonfinancial benefits, such as in-kind benefits, are not financial remuneration.

- disclosures for treatment or payment purposes;
- disclosures for the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence activities;
- disclosures to or by a business associate for activities that the business associate undertakes on behalf of a covered entity (or activities that a subcontractor undertakes on behalf of a business associate), if the only remuneration provided from the covered entity to the business associate (or from the business associate to a subcontractor) is for the performance of such activities;
- disclosures to an individual who is the subject of the PHI pursuant to an individual's request for access to the PHI or for an accounting of disclosures;
- disclosures required by law; and
- any other disclosure permitted by and in accordance with the HIPAA Privacy Rule if the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.

An authorization permitting the sale of PHI must state that the disclosure will result in remuneration to the covered entity.

Fundraising

The Omnibus Rule makes several important changes regarding the use or disclosure of PHI for fundraising purposes, expanding the types of PHI that may be used or disclosed for such purposes, strengthening the opt-out rights of individuals and imposing other requirements.

In addition to the limited range of PHI permitted to be used or disclosed under the existing HIPAA Privacy Rule (largely demographic information), the Omnibus Rule adds information about the clinical department that provided services, the treating physician, outcome information and health insurance status. Department of service information includes information about the general department of treatment, such as cardiology, oncology or pediatrics, but does not include diagnosis information. The Omnibus Rule also clarifies that demographic information permitted to be used or disclosed includes name, address, other contact information, age, gender and date of birth. This expansion of the range of information that may be used or disclosed for fundraising purposes should help covered entities better target their solicitations, particularly with respect to service-line-specific campaigns.

Additionally, each fundraising communication to an individual must now include a clear and conspicuous opportunity to elect not to receive any further fundraising communications. Such opportunity may not impose an undue burden or more than a nominal cost on the individual. Pre-solicitation opt-outs are *not* required prior to the first fundraising solicitation.

Covered entities are prohibited from making fundraising communications to an individual who has elected not to receive them; such a communication would be in violation of the HIPAA Privacy Rule and subject to possible criminal penalties, civil money penalties or other corrective action.

New and Expanded Individual Rights

The Omnibus Rule also enhances the rights of individuals to restrict disclosures of their PHI and provides them with expanded access to their electronic health records. These changes could require covered entities to modify their privacy policies and procedures that address these enhanced individual rights, which are described below.

- ***Right of Individuals to Restrict Certain Health Plan Disclosures.*** Currently, the HIPAA Privacy Rule permits an individual to request a covered entity to restrict uses or disclosures of PHI about the individual for treatment, payment or health care operations purposes, but the covered entity is not required to agree to a restriction. The Omnibus Rule now *requires* covered health care providers[2] to agree to such requests, if the request is to restrict disclosures to a health plan for payment or health care operations purposes; if the request is not otherwise required by law; and if the PHI at issue pertains solely to a health care item or service for which payment has been made in full by the individual or a third party other than the health plan. Such restrictions do not override disclosures that are otherwise required by law. This means covered entities will "need to employ some method to flag or make a notation in the [patient's] record with respect to the PHI that has been restricted to ensure that such information is not inadvertently sent to or made accessible to the health plan for payment or health care operations purposes, such as audits by the health plan." A disclosure of restricted PHI is a disclosure in violation of the HIPAA Privacy Rule and is subject to possible criminal penalties, civil money penalties or other corrective action.

- ***Enhanced Rights to Access PHI.*** The Omnibus Rule enhances the existing right of individuals to request access to their own PHI. Under the HITECH Act, if a covered entity uses or maintains an electronic health record with respect to the PHI of an individual, the individual has the right to obtain from the covered entity a copy of such information in electronic format. The Omnibus Rule expands this requirement so that it applies to PHI maintained electronically in one or more designated record sets. Access to such PHI must be provided by the covered entity in the electronic form and format requested by the individual (if readily producible) or (if not readily producible) in a readable electronic form and format as agreed to by the covered entity and the individual. If no agreement can be reached as to electronic format, the covered entity must provide a hard copy of the information. If a covered entity utilizes older technology that is not capable of providing any form of electronic copy, some investment may be required to upgrade the technology to meet the basic requirement to provide some form of electronic copy. Unencrypted email may be used to deliver the information to the individual if the covered entity advises the individual of the risk and the individual still prefers that delivery method. The Omnibus Rule also requires that, if requested by the individual to do so in a writing that meets certain requirements, the covered entity must transmit the copy of the PHI directly to a third party specified by the individual.

    - *Timing.* Generally, requests for access to PHI must be acted on within 30 days, though under certain circumstances an additional one-time 30-day extension is available. The Omnibus Rule eliminates the 60-day period that applies when PHI is not maintained or accessible to the covered entity on-site. The response period for the covered entity to provide access to the individual's PHI begins on the date of the request, and any time spent reaching agreement with an individual about the electronic form and format counts against the required response time.

    - *Fees.* The rules continue to permit the covered entity to charge a reasonable cost-based fee for the copies, but clarifies that labor costs for copying the PHI (paper or electronic) and the cost of supplies for creating a paper copy or electronic media (if the copy is requested on portable media) may be charged. Fees associated with maintaining systems and recouping capital for data access, storage and infrastructure are not considered reasonable, cost-based fees.

[2] The regulatory language uses the term "covered entity," but the preamble to the Omnibus Rule clarifies that as a practical matter the Rule applies only to covered health care providers.

Updates to Notices of Privacy Practices

The Omnibus Rule requires a number of changes to the Notice of Privacy Practices ("NPPs") published by covered entities:

- NPPs must now include a description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4). These include most uses or disclosures of psychotherapy notes, marketing communications and sales of PHI. The NPP also must state that other uses and disclosures *not described in the notice* will be made only with the individual's written authorization.

- The previously required statement regarding fundraising communications must now include a statement that the individual has a right to opt out of receiving such communications (but the specific opt-out method is not required to be included in the NPP).

- For health plans that intend to use or disclose PHI for underwriting purposes as permitted by the HIPAA Privacy Rule, a statement that the covered entity is prohibited from using or disclosing PHI that is genetic information for such purposes must be added to the NPP.

- The previously required statement regarding an individual's right to request restrictions on the uses and disclosures of the individual's PHI must now reflect that covered entities must now agree to certain restrictions (as described above).

- The NPP must now include a statement that the covered entity is required by law to notify affected individuals following a breach of unsecured PHI. This statement may be general in nature and is not required to provide detailed information about what constitutes a breach or what notices are required.

How We Can Help

Hunton & Williams has extensive experience developing and advising on comprehensive privacy and information security programs, including those required by HIPAA. We have assisted our clients with more than 900 data breaches worldwide (including numerous large HITECH breaches), handling every aspect of the breach event. We also have significant experience advising clients about the requirements of HIPAA and the Privacy and Security Rules, the relationships between covered entities and their business associates, electronic health records, health information exchanges and the HITECH Act breach requirements. If you need assistance in developing, revising or implementing your organization's privacy or data security practices, or have questions regarding any facet of HIPAA as it applies to covered entities or business associates, please contact us.

Our Privacy, Data Security and Health Care Practices

Hunton & Williams' global Privacy and Data Security practice has been ranked as the top law firm globally for privacy and data security by *Computerworld* magazine in each of its four surveys of more than 4,000 corporate privacy leaders (2006, 2007, 2008, 2010), and is rated by Chambers and Partners as the top privacy and data security practice in its *Chambers UK*, *Chambers Global* and *Chambers USA* guides in 2012. The *Legal 500* also recognizes Hunton & Williams as a top-rated firm for data protection and privacy in 2012. For additional information visit the Privacy and Information Security Law Blog at http://www.huntonprivacyblog.com.

The lawyers composing Hunton & Williams' Health Care practice bring the experience, knowledge and creativity required to help clients bridge the gap between the delivery models of yesterday and tomorrow.

For decades, we have successfully guided organizations through the twists and turns of federal and state health care policy shifts, as well as the ups and downs of economic cycles. Just as our clients are held to high standards of patient outcomes and business performance, we hold ourselves to equally high standards. The quality of our counsel can be measured by our focused consideration of client needs and our ability to sort through the details of a complex problem or project to provide comprehensive, efficient and effective solutions. We advise large health systems, hospitals, academic medical centers, large multispecialty group practices, pharmaceutical companies, medical-device manufacturers and other providers on matters involving virtually every aspect of doing business in this complex and competitive arena, including health information privacy and security and the requirements of HIPAA, the HITECH Act and their implementing regulations.

Contacts

Lisa J. Sotto
lsotto@hunton.com

Aaron P. Simpson
asimpson@hunton.com

Mark S. Hedberg
mhedberg@hunton.com

Ryan P. Logan
rlogan@hunton.com