Bloomberg BNA

# Health IT Law & Industry Report™

VOL. 5, NO. 14 APRIL 8, 2013



## Key Compliance Actions for the New HIPAA Privacy Regulations



BY LEAH ROFFMAN, PAMELA TYNER, PATRICIA WAGNER

The long-awaited final Health Insurance Portability and Accountability Act omnibus rule (''Omnibus Rule'') issued by the Department of Health and Human Services (''HHS'') was published in the *Federal Register*.[1] The Omnibus Rule makes sweeping changes to the privacy and security regulations under the Health Insurance Portability and Accountability Act (''HIPAA'').

Although the Omnibus Rule effect on March 26, 2013, affected parties have until September 23, 2013, to come into compliance with most of its provisions. However, there are several key regulatory changes and suggested action items that entities will want to consider as they develop plans to come into compliance with the new requirements.

*Leah A. Roffman is an associate with Epstein Becker & Green in the New York office. She may be contacted at (212) 351-4618 or lroffman@ebglaw.com. Pamela D. Tyner is a member of the law firm in Houston. She can be reached at (713) 300-3213 or ptyner@ebglaw.com. Patricia M. Wagner is a member of the law firm in Washington. She can be reached at (202) 861-4182 or pwagner@ebglaw.com.*

[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; Department of Health and Human Services, Office of the Secretary (45 C.F.R. Parts 160 and 164), 78 Fed. Reg. 5566 (Jan. 25, 2013).

 ISSN 2151-2876

## 1. Review Business Associate Relationships and Update Business Associate Agreements

The Omnibus Rule makes a number of significant changes to the definition of a ''business associate.''[2] The definition now expressly includes the following types of entities as business associates:

1) Health information organizations, e-prescribing gateways, and entities that provide data transmission services for protected health information (''PHI'') to a covered entity and that require access to PHI on a routine basis;

2) Entities that offer personal health records to individuals on behalf of a covered entity; and

3) Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.

The preamble of the Omnibus Rule (''Preamble'') warns that the terms ''health information organization'' and ''e-prescribing gateway'' are illustrative and not intended to be an all-inclusive list of qualifying entities.[3] On the other hand, the Preamble confirms a prior interpretation that ''mere conduits'' of information are not business associates, provided that they do not access PHI other than on a random or infrequent basis.[4] The Preamble takes the position that entities that ''manage the exchange of PHI through a network, including providing record locator services and performing various oversight and governance functions for an electronic health information exchange, have more than ''random'' access to PHI and, thus, would fall within the definition of a ''business associate.''[5]

As a result, in analyzing relationships with vendors to determine whether business associate covenants must be obtained, covered entities and ''intermediate'' business associates should look beyond mere naming conventions and make determinations regarding whether the data transmission organization has more than ''random or infrequent'' access to PHI.

Conversely, the Omnibus Rule provides clarification on entities that do not qualify as business associates (incorporating prior guidance) and specifically includes in the list:

1) Providers receiving treatment-related PHI from a covered entity;

2) Plan sponsors receiving PHI from group health plans;

3) Government agencies determining eligibility for, or enrollment in, a government health plan providing public benefits that are administered by another government agency or that collect PHI for such purposes; and

4) Covered entities participating in Organized Health Care Arrangements (''OHCA'') that perform certain services for, or on behalf of, an OHCA.

Of course, if a business associate relationship does exist, the business associate and covered entity need to enter into a business associate agreement. The Omnibus Rule imposes new requirements that must be addressed in business associate agreements.

Key required covenants include a covenant to comply with the applicable provisions of the Security Rule; a covenant to report breaches of unsecured PHI to the covered entity; and a covenant to enter into written business associate agreements with any subcontractors. Therefore, entities that already have a business associate agreement in place will need to make sure that the agreement meets the specifications of the Omnibus Rule. HHS has posted a sample business associate agreement on its website.[6]

Business associates are charged with evaluating their relationships with vendors to determine whether a second- (or subsequent- ) tier business associate agreement is required. Of course, any such second-tier business associate agreements must also reflect the requirements of the Omnibus Rule.

## 2. Evaluate Compliance with Heightened Safeguard Requirements

The Omnibus Rule enhances business associates' HIPAA obligations substantially.[7] Business associates are now subject to civil monetary penalties for any violations. Specifically, under the Omnibus Rule, business associates are legally required to implement certain administrative safeguards, physical safeguards, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI that they create, receive, maintain, or transmit (the requirements of the Security Rule).

In order to meet their responsibilities, business associates are now required to perform risk analyses. Such risk analyses must be accurate and thorough assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits. The Security Rule also compels corrective actions to minimize any identified risks and vulnerabilities.

## 3. Update Notices of Privacy Practices[8]

The Omnibus Rule requires covered entities to provide additional information in their Notices of Privacy Practices (''NPP'') as to how PHI will (and will not) be used and disclosed. The NPP must now include:

1) A description of activities, involving uses or disclosures of PHI, that require an individual's authorization, such as activities relating to the use of psychotherapy notes and disclosures of PHI for marketing purposes (in addition to the prior required statement that any uses or disclosures, other than those permitted, would be made only with an authorization); [9]

[2] See 45 C.F.R. § 160.103.
[3] 78 Fed. Reg. 5571.
[4] *Id.*
[5] *Id.*
[6] HHS posted sample business associate agreement provisions at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
[7] See 45 C.F.R. § 160.102.
[8] See 45 C.F.R. § 164.520.
[9] See 45 C.F.R. § 164.520; 78 Fed.Reg. 5622.

  HITR ISSN 2151-2876

2) Notice that individuals have a right to opt out of receiving fundraising communications;[10]

3) A statement explaining that covered entities are required by law to notify affected individuals following a breach of unsecured PHI;[11] and

4) For covered entities that are health plans and intend to use PHI for underwriting purposes, a statement that the plan is prohibited from using or disclosing PHI that is genetic information of an individual for underwriting purposes.[12]

The Omnibus Rule also eliminates certain content requirements. For example, the Omnibus Rule removes the requirement that covered entities' NPPs notify individuals of any plans to contact individuals to provide appointment reminders or information about alternative treatment options.[13]

The Omnibus Rule and Preamble are also instructive to covered entities regarding how such revised NPPs need to be made available to individuals. Specifically:

- For health plans:
- If the health plan posts its NPP on a website, then the plan must prominently post the change or the revised NPP on its website by the effective date of the change. Information on the revision or the revised NPP itself must also be provided to enrollees in its next annual mailing.
- If the health plan does not post its NPP on its website, then the plan must provide either the revised NPP or information about the change and how to obtain the revised NPP to enrollees within 60 days of the material revision.[14]
- For providers:

Providers should post the revised NPP at the site of service and have copies available for individuals to request.

Providers must still provide new patients with a copy of the revised NPP.[15]

## 4. Update Privacy Policies and Procedures

The following are examples of policies and procedures that may need to be updated as a result of new requirements in the Omnibus Rule:

### a. Authorization Forms and Related Policies[16]

In the new HIPAA landscape, covered entities are required to obtain an authorization for any disclosure of PHI that constitutes a sale of PHI. Such authorization must state that the disclosure will result in remuneration to the covered entity.[17]

On the other hand, the Omnibus Rule liberalized aspects of research authorizations. Specifically, an authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Certain restrictions apply when a provider has conditioned the provision of research-related treatment on the provision of an authorization.[18]

Additionally, the Omnibus Rule liberalizes a few types of uses and disclosures that do not require an authorization. Under the Omnibus Rule, covered entities may now disclose PHI about students and prospective students to a school if the PHI is limited to proof of immunization that the school is legally required to have, and the covered entity obtained agreement for the disclosure from the individual or the individual's parent or guardian.

### b. Procedures for Using PHI for Fundraising[19]

Under the Omnibus Rule, covered entities may still use and disclose certain PHI for fundraising purposes. However, such use and disclosure is subject to several new conditions. First, covered entities must state their intention to use certain PHI for fundraising purposes in their NPPs. Second, each fundraising communication must provide the recipient with a clear and conspicuous opportunity to elect not to receive future communications. Third, covered entities may not condition treatment or payment on individuals' decisions to receive fundraising communications.

### c. Marketing Policy

The Omnibus Rule also makes certain changes to the definition of ''marketing.''[20] These changes are important because they inform when authorizations are required.[21] Typically, a covered entity must obtain an authorization for the use or disclosure of PHI for marketing purposes, unless the communication is a face-to-face communication between the covered entity and an individual, or a promotional gift of nominal value provided by the covered entity. As described below, if the marketing involves financial remuneration to the covered entity from a third party, this use or disclosure will require the individual's authorization.

Generally, ''marketing'' means communications about a product or service that encourage recipients of the communication to purchase or use the product or service. However, there are many exceptions.

One new exception is that ''marketing'' does not include a communication made to provide refill reminders or communicate about a drug currently being described to the individual if financial remuneration received by the covered entity is reasonably related to the cost of the communication.

[10] *Id.*
[11] *Id.*
[12] See 45 C.F.R. § 164.520(b)(iii)(C).
[13] See 45 C.F.R. § 164.508(a)(3).
[14] See 45 C.F.R. § 164.520(c)(2)(v).
[15] 78 Fed. Reg. 5625.
[16] See 45 C.F.R. § 164.508.
[17] See 45 C.F.R. § 164.508(a)(4).
[18] See 45 C.F.R. § 164.508(b)(3)(i).
[19] See 45 C.F.R. § 164.514.
[20] See 45 C.F.R. § 164.501.
[21] See 45 C.F.R. § 164.508(a)(3).

Excepted purposes also include case management and care coordination, but the Omnibus Rule now limits them to instances where the covered entity does not receive financial remuneration in exchange for the communication. Likewise, uses or disclosures to describe a health-related product or service **available only to a health plan enrollee that adds value to, but is not part of, a plan of benefits** remain permissible, unless the covered entity receives financial remuneration in exchange for the communication. Note that, as used to define ''marketing,'' the term ''financial remuneration'' means direct or indirect payment from or on behalf of a third party whose product or service is being described, and it does not include payment for treatment.

### d. Access Policy[22]

The Omnibus Rule also expands the rights of individuals to access their own PHI. Pursuant to the Omnibus Rule, if an individual requests an electronic copy of PHI maintained electronically in a designated record set from a covered entity, the covered entity must provide access to the PHI in the electronic form and format requested if readily producible.

If not readily producible in such format, then the covered entity must provide the PHI in a readable electronic form and format that the parties find to be mutually agreeable.

Additionally, the Omnibus Rule permits individuals to instruct covered entities to transmit copies of PHI directly to another designated person, and covered entities must abide by such requests that are in writing and signed and clearly identify the recipient.

## 5. Update Policies Regarding Determination of Breaches of Unsecured PHI[23]

The Omnibus Rule implements a new definition of the term ''breach of unsecured PHI.'' Specifically, there is a new presumption that an unauthorized use or disclosure of unsecured PHI constitutes a breach unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised.

Thus, entities will no longer be able to conduct analyses to determine whether uses or disclosures of PHI pose a significant risk of harm to individuals. Under the Omnibus Rule, organizations must instead analyze the following:

1) The nature and extent of PHI involved in the use or disclosure, including the types of identifiers and the likelihood of re-identification;
2) The unauthorized entity to whom the PHI was disclosed or who used the PHI;
3) Whether the PHI was actually acquired or viewed; and
4) The extent to which the risk to the PHI has been mitigated.

## 6. Update HIPAA Training

In order to implement all the changes discussed above, covered entities and business associates will need to update the HIPAA training of their workforces. Employees, volunteers, and consultants need to understand that there are new rules to be applied when using, disclosing, and protecting PHI.

Training is a vital step to achieving and maintaining compliance, in addition to being an independently required element of the Omnibus Rule.

## Conclusion

Covered entities and business associates must amend policies, procedures, and business associate agreements to account for the changes affected by the Omnibus Rule. In addition, personnel must be trained to understand the revised parameters of the Omnibus Rule and to adopt the new preventative measures dictated by the Omnibus Rule.

Beginning the process prior to the September 2013 deadline will ease the transition into the new HIPAA privacy and security compliance landscape.

---

[22] See 45 C.F.R. § 164.524(c).
[23] See 45 C.F.R. § 164.402.



HITR ISSN 2151-2876