POWERS

POWERS PYLES SUTTER & VERVILLE PC

ATTORNEYS AT LAW

MEMORANDUM

REVISED/UPDATED

To: **Clients and Friends**

From: **Jim Pyles**
Rob Portman
Amita Sanghvi

Date: **January 25, 2013**

Re: **HIPAA Final Omnibus Rule is Here!**

On January 17, 2013, the US Department of Health and Human Services (HHS) unveiled its long awaited final omnibus rule (Omnibus Rule) which implements privacy, security, and enforcement measures under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Genetic Information Nondiscrimination Act (GINA).[1]

Leon Rodriguez, HHS Office for Civil Rights Director, noted in a press release that the Omnibus Rule:

> …marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.

Required Actions

The effective date for the Omnibus Rule is March 26, 2013, and organizations must be in compliance with the Omnibus Rule by September 23, 2013 (with the exception that existing business associate agreements must be revised by September 22, 2014). Between now and September, covered entities and business associates, will need to, among other things:

- *Modify their Notices of Privacy Practices and patient authorization forms;*
- *Update and/or execute new business associate agreements; and*
- *Revise HIPAA policies and procedures, including breach notification procedures.*

[1] A copy of the rule is available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

1501 M STREET, NW ■ SEVENTH FLOOR ■ WASHINGTON, DC 20005 ■ PH 202.466.6550 ■ FX 202.785.1756 ■ WWW.PPSV.COM

Below we have summarized specific changes required by the Omnibus Rule.

Covered Entities

- Individuals have a right to access and to obtain a copy of Protected Health Information (PHI) within 30 days of the request (with a one-time 30-day extension after written notice for the delay and when the records will be provided). If an individual requests a copy of PHI that is maintained electronically, the covered entity must provide the individual with access to the information in electronic form.

- When an individual requests a restriction on disclosure of his or her PHI to a health plan, a health care provider must agree to the requested restriction if disclosure is not required by law, the request relates to payment or health care operations, and the individual has paid for the item or service out of pocket in full. HHS directs covered entities to employ some method to flag medical records with respect to the PHI that has been restricted.

- Covered entities may disclose PHI to family members of a decedent who were involved in the person's care prior to his or her death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. The Omnibus Rule also clarifies that HIPAA does not apply to information 50 or more years after the decedent's death, despite many commentators expressing concern that the protection for sensitive information (*e.g.*, psychotherapy notes, HIV/AIDS information) should not be limited. However, the rule does not prohibit covered entities from affording privacy protections beyond the 50-year period as they may elect or as may be required by state laws or standards of professional responsibility.

- The Omnibus Rule requires covered entities and business associates to obtain an individual authorization for the sale of PHI. However, the sale of PHI excludes numerous transactions such as disclosures for certain research purposes, treatment and payment, and for any other purpose permitted by the Privacy Rule, where the only remuneration received by the seller is "a reasonable cost-based fee" to cover the cost of preparation and transmission of the PHI for such purpose or a fee otherwise expressly permitted by other law.

- In any fundraising materials sent by a covered entity, the entity is required to give individuals the opportunity to opt-out of receiving further fundraising communications.

- A covered entity may combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components, allows the individual the option to *opt in* to the unconditioned research activities, and the research does not involve the use or disclosure of psychotherapy notes. For research that involves the use or

disclosure of psychotherapy notes, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

- While the HIPAA rules have previously required that authorizations for research be study specific, the Omnibus Rule permits an individual to authorize the use or disclosure of PHI for future research, provided that the authorization adequately describes the purpose of the use or disclosure of PHI such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research.

- The definition of "marketing" has been modified to encompass communications by a covered entity (or its business associate) for purposes of treatment and health care operations about health-related products or services if the covered entity receives financial remuneration in exchange for making the communication from or on behalf of the third party whose product or service is being described. A covered entity must obtain an individual's written authorization prior to sending marketing communications to the individual.

- As a result of the above changes, covered entities must revise their notices of privacy practices to advise individuals of the following:

    (1) For health plans that underwrite, the prohibition against health plans using or disclosing PHI that is genetic information about an individual for underwriting purposes;

    (2) The prohibition on the sale of PHI without the express written authorization of the individual;

    (3) A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization, as well as a statement that other uses and disclosures not described in the notice will be made only with authorization from the individual;

    (4) The duty of a covered entity to notify affected individuals of a breach of unsecured PHI;

    (5) For covered entities that have stated their intent to fundraise in their notice of privacy practices, the individual's right to opt out of receiving fundraising communications from the covered entity; and

    (6) 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 in full.

Business Associates

- The Omnibus Rule adds "subcontractors" to the definition of "business associate." As a result, all downstream entities that work at the direction of or on behalf of a business associate and handle PHI will also have direct liability under HIPAA. Other examples of business associates added by the Omnibus rule include: (1) patient safety organizations; (2) health information organizations (including, health information exchanges), e-prescribing gateways, and document storage entities that receive PHI; and (3) entities that offer personal health records to patients on behalf of a covered entity as "business associates."

- Business associates will have direct liability under certain HIPAA Privacy and Security rule provisions.

- The HIPAA Security Rule provisions applicable to business associates include the implementation of administrative, physical, and technical safeguards to protect PHI, the implementation of policies and procedures to comply with HIPAA, and the maintenance of documentation of this compliance.

- Business associates must furnish any information the Secretary of Health and Human Services requires to investigate whether the business associate is in compliance with the regulations.

- HHS has published sample guidance business associate agreement provisions on its website.[2] The sample provisions are merely recommendations, and it will be necessary for organizations to carefully craft these agreements to ensure unnecessary liability is not imposed on the covered entity or business associate. Although new business associate agreements must be updated for compliance with the Omnibus Rule by September 23, 2013, existing business associate agreements do not need to be modified until September 22, 2014 (one year after the date required for compliance with the Omnibus Rule).

[2] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Breach Notification Rule

- The "harm" standard in the interim final rule is eliminated. Any acquisition, access, use, or disclosure of unsecured PHI not permitted under HIPAA is *presumed* to be a breach unless a covered entity or business associate can demonstrate a low probability that the PHI has been *compromised* based on a four-factor risk assessment:

  (1) The nature and extent of PHI involved;

  (2) The unauthorized person who used the PHI or to whom the disclosure was made;

  (3) Whether PHI was actually acquired or viewed; and

  (4) The extent to which the risk to PHI has been mitigated (*e.g.*, assurances from trusted third-parties that the information was destroyed).

- The presumption-of-breach rule differs significantly from the proposed rule, which set several conditions that had to be met before a covered entity had to treat a disclosure as a breach. The rule also provides that covered entities and business associates may dispense with a risk assessment if they provide notice of the breach to individuals. The rule maintains the standard that the disclosure of properly encrypted PHI is not a breach for HIPAA purposes.

Penalties

- The Omnibus Rule incorporates the increased and tiered civil money penalty structure provided by the HITECH Act, with penalties based on the level of negligence and with a maximum penalty of $1.5 million per violation.

- When assessing civil monetary penalties, an organization's history of compliance and non-compliance will be considered.

This summary is for informational purposes only. It does not constitute and should not be treated as legal advice. Please contact Jim Pyles at Jim.Pyles@PPSV.com, Rob Portman at Rob.Portman@PPSV.com, or Amita Sanghvi at Amita.Sanghvi@PPSV.com, if you have any questions about this topic. We will continue to provide updates as this new rule is analyzed.