HIPAA – THE NEW RULES

Highlights of the major changes under the “Omnibus” Rule

AUTHOR
Gamelah Palagonia, Founder
CIPM, CIPP/IT, CIPP/US, CIPP/G, ARM, RPLU+

PRIVACY PROFESSIONALS LLC
gpalagonia@privacyprofessionals.com
www.privacyprofessionals.com

5 Hanover Square, 22nd Floor
New York, NY 10004
646.354.7065

PrivacyProfessionals.com

PRIVACY PROFESSIONALS LLC

HIPAA – THE NEW RULES

Highlights of the major changes under “The Omnibus Rule”

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Omnibus Rule

On January 17, 2013, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") released its long awaited new expanded rule, the "Omnibus Rule"[1]. The Omnibus Rule amends 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 Act ("HITECH") and the Genetic Information Nondiscrimination Act ("GINA") of 2008. The Omnibus Rule is effective March 26, 2013, and compliance is required no later than September 23, 2013.

One of the biggest changes under the Omnibus Rule affects Business Associates (BA's). Under the Omnibus rule, a business associate is defined as anyone who receives, creates, maintains or transmits protected health information on behalf of a covered entity. The scope of this expanded definition means that subcontractors of BA's are now HIPAA business associates if they handle or process Personal Health Information (PHI). Previously, BA's were only required to ensure that subcontractors agree to the same restrictions in the use of PHI. Beginning September 23, 2013, the Omnibus Rule applies the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule directly to business associates including penalties for data breaches.

Whether systems upgrades are conducted by covered entities or their BA's, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

HIPAA enforcement penalties can range up to $1.5 million per violation. Corrective Actions, Resolutions Agreements and Civil Actions brought State Attorneys General (SAG) may also apply.

This report provides the expanded definitions of Covered Entity and Business Associate and highlights some of the major changes under the Omnibus Rule.

The PDF copy of the Omnibus Rule is available for download at Department of Health and Human Services, Office for Civil Rights website. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.[1]

Gamelah Palagonia, Founder

HHS/OCR DEFINITION

Covered Entity

(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Business Associate

(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

CHANGES TO THE BREACH NOTIFICATION FRAMEWORK

HITECH ACT

In 2009, the HITECH Act established a statutory requirement for breach notification that obligated covered entities, which include healthcare providers, group health plans and healthcare clearinghouses, to notify affected individuals and HHS when more than 500 individuals are affected. 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 that compromises the security or privacy of the protected health information. The term "compromises the security or privacy of the protected health information" was further defined to mean "poses a significant risk of financial, reputational, or other harm to the individual", which is called the harm threshold. This harm threshold will only remain in effect until September 23, 2013.

Under the Omnibus Rule the harm threshold is replaced by the 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.

Protected Health Information (PHI)

Protected health information (PHI) means information that identifies an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual that is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. The HIPAA Privacy Rule covers PHI in any medium while the HIPAA Security Rule covers electronic protected health information (ePHI).

MARKETING

Communications

The Omnibus Rule makes significant changes to marketing communications. The basic definition remains the same but the exceptions have been re-written. Refill reminders or other communications about a drug being prescribed for an individual are not considered marketing only if any financial consideration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's costs of making the communication. Permissible costs for which financial consideration may be received are limited to the costs of labor, supplies and postage. If a financial incentive beyond the costs of making the communication is provided, the exception no longer applies and the communications constitutes marketing.

Covered entities are required to obtain a valid authorization for any use or disclosure of PHI for marketing purposes, subject to two exceptions: (1) the communication is made in a face-to-face encounter between the covered entity and the individual and (2) in the case of a promotional gift of nominal value provided by the covered entity. If the marketing activity involves financial consideration to the covered entity from a third party, the authorization must state that financial consideration is involved.

FUNDRAISING

Opt-Out

The Omnibus Rule makes important changes regarding the use or disclosure of PHI for fundraising purposes. In addition to the limited use of PHI permitted under the existing HIPAA Privacy Rule, the Omnibus Rule adds information about the clinical department that provided services, the treating physician, outcome information and health insurance status.

Each fundraising communication to an individual must now include a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. Covered entities are prohibited from sending fundraising solicitations to individuals that elected to opt-out as such communication would be a violation of the HIPAA Privacy Rule and subject to possible criminal penalties, civil penalties or other corrective action.

SALE OF PHI

Disclosure

The Omnibus Rule makes important changes regarding the use or disclosure of PHI for fundraising purposes. In addition to the limited use of PHI permitted under the existing HIPAA Privacy Rule, the Omnibus Rule adds information about the clinical department that provided services, the treating physician, outcome information and health insurance status.

Each fundraising communication to an individual must now include a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. Covered entities are prohibited from sending fundraising solicitations to individuals that elected to opt-out as such communication would be a violation of the HIPAA Privacy Rule and subject to possible criminal penalties, civil penalties or other corrective action.

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. 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 compensation from or on behalf of the recipient of the PHI in exchange for the PHI, subject to the following exceptions:

- ✓ Disclosure for public health purposes
- ✓ Certain disclosures for research purposes
- ✓ Disclosures for treatment or payment purposes
- ✓ Disclosures for the sale, transfer, merger or consolidation of all or part of the covered entity and for due diligence activities
- ✓ Disclosures to or by a business associate for activities that the business associate undertakes on behalf of a covered entity if the only compensation is for the performance of such activities
- ✓ Disclosures to an individual who is the subject of the PHI pursuant to an individual request for access to the PHI or for an accounting of disclosures
- ✓ Disclosures required by law
- ✓ Any other disclosure permitted by an in accordance with the HIPAA Privacy Rule

EXPANDED INDIVIDUAL RIGHTS

Expanded Access

The Omnibus Rule 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 to address the enhanced individual rights.

NOTICE OF PRIVACY PRACTICES (NPP)

Types of Uses.Providing Notice

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 including 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.
- ✓ For health insurance plans that 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 tied to genetic information for such purposes must be added to the NPP.
- ✓ 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.
- ✓ A covered entity must make its NPP available to any person who asks for it.
- ✓ A covered entity must prominently post and make its NPP available on any web site it maintains that provides information about its customer services or benefits.

HIPAA ENFORCEMENT ACTIONS

Fines.Penalties.Corrective Actions.Resolution Areements

1. **Adult & Pediatric Dermatology P.C. – December 26, 2013**
   Adult & Pediatric Dermatology, P.C., of Concord, Mass., ("AP Derm") has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services, agreeing to a $150,000 payment involving a breach of just 2,200 health records. In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring AP Derm to develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.
   http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-agreement.html

2. **WellPoint Inc. – July 11, 2013**
   WellPoint Inc. has agreed to pay the U.S. Department of Health and Human Services **$1.7 million** to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule. The investigation indicated WellPoint did not: adequately implement policies and procedures for authorizing access to the on-line application database; perform an appropriate technical evaluation in response to a software upgrade to its information systems; or have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.
   http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf

3. **Prime Healthcare Services/Shasta Regional Medical Center – June 13, 2013**
   Shasta Regional Medical Center (SRMC) has agreed to settle an investigation by the U.S. Department of Health and Human Services (HHS) about potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and will pay a **$275,000** monetary settlement. SRMC has also agreed to a comprehensive corrective action plan to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members.
   http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/shasta-agreement.pdf

4. **Massachusetts Eye & Ear Infirmary – September 13, 2012**
   Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services (HHS) **$1.5 million** to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule stemming from the theft of an unencrypted laptop. MEEI also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information.
   http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf

5. **Alaska Department of Health & Social Service – June 26, 2012**
   The Alaska Department of Health and Social Services (DHSS) has agreed to pay the U.S. Department of Health and Human Services' (HHS) **$1.7 million** to settle possible violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. Alaska DHSS has also agreed to take corrective action to properly safeguard the electronic protected health information (ePHI) of their Medicaid beneficiaries.
   http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf

RESOLUTION AGREEMENTS

Civil Monetary Penalties (CMP)

A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make periodic reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement likely would include the payment of a resolution amount. These agreements are reserved to settle investigations with more serious outcomes. When HHS has not been able to reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity. To date, HHS has entered into ten resolution agreements and issued CMPs to one covered entity.

STATE ATTORNEYS GENERALS (SAG)

Civil Actions

The HITECH Act gave State Attorneys General (SAG) the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. The HITECH Act permits SAG to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.

This new enforcement authority granted to SAG by section 13410(e) of the HITECH Act will require significant coordination between OCR and SAG. OCR welcomes collaboration with SAG seeking to bring civil actions to enforce the HIPAA Privacy and Security Rules, and OCR will assist SAG in the exercise of this new enforcement authority. OCR will provide information upon request about pending or concluded OCR actions against covered entities or business associates related to SAG investigations. OCR will also provide guidance regarding the HIPAA statute, the HITECH Act, and the HIPAA Privacy, Security, and Enforcement Rules as well as the Breach Notification Rule.

ABOUT US

Privacy Professionals LLC (PRIPRO™) is a risk advisory firm specializing in Cyber & Privacy Risk CPR™ insurance and risk management services. Services include Risk Assessments, Employee Training Programs, Incident Response Planning and Customized Insurance Solutions. PRIPRO™ services enable businesses to build an information privacy awareness risk culture, reduce the cost of cyber and privacy risk, secure the appropriate insurance solution, and meet regulatory compliance and legal requirements.

CONTACT US

Privacy Professionals LLC
5 Hanover Square, 22nd Floor
New York, NY 10004
Phone: 646.354.7065 or 646.354.7066
Email: contact@privacyprofessionals.com
Website: www.privacyprofessionals.com