The Law Offices of
Jason M. Healy PLLC

Health Care Plans and Providers
Legal Alert

June 2013 Vol. 3, No. 3

Complying With The HIPAA/HITECH Act Omnibus Rule: Next Steps for Group Health Plans and Providers

In This Issue:

www.HealyLawDC.com

A health law firm in the nation's capital

Contact Us:

Amy D. Healy
ahealy@healylawdc.com
(703) 712-4743
(703) 967-4829 cell

1701 Pennsylvania Ave., NW
Suite 300
Washington, DC 20006

1750 Tysons Boulevard
Suite 1500
McLean, VA 22102

The omnibus final rule (the "Omnibus Rule") issued by the U.S. Department of Health and Human Services ("HHS") makes significant changes to the area of health care privacy. 78 Fed. Reg. 5566 (Jan. 25, 2013). The Omnibus Rule includes a wide variety of modifications and clarifications to the privacy and security rules established by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). These changes will impact the operations and compliance responsibilities of covered entities, including group health plans and health care providers, and their business associates. In anticipation of the September 23, 2013 deadline for compliance with these new requirements, this article outlines the necessary steps group health plans and health care providers must take to ensure their HIPAA policies and procedures comply with these changes.

Please feel free to reach us at the phone number or email address to the left if you have questions about these HIPAA privacy and security issues or for assistance in complying with the new requirements for covered entities and business associates.

Background and Effective Dates. Enacted in 1996, HIPAA established national standards to protect the privacy and security of an individual's health information maintained in electronic health records and other formats. The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), enacted as part of the American Recovery and Reinvestment Act of 2009, significantly increased privacy protections and implemented additional security and enforcement rules. In particular, the HITECH Act addressed the privacy and security concerns associated with the electronic transmission of health information and strengthened the civil and criminal enforcement provisions of HIPAA. The Omnibus Rule modifies these privacy, security and enforcement rules enacted by the HITECH Act.

The Omnibus Rule is effective as of March 26, 2013, and compliance is generally required by September 23, 2013. Transitional relief provides that business associate agreements that were in effect on January 25, 2013, have until September 23, 2014 to comply with the Omnibus Rule.

Expanded Definition of Business Associates. HIPAA permits a covered entity to disclose protected health information ("PHI") to a business associate, provided that the covered entity obtains assurances (in the form of a business associate agreement) that the business associate will safeguard

the PHI. The Omnibus Rule expands the definition of business associate and extends direct liability for compliance with the security rule to business associates. In general, a "business associate" means a person or entity that performs functions or activities that involve the use or disclosure of PHI on behalf of a covered entity. The Omnibus Rule defines business associate as a person who "creates, receives, maintains or transmits" PHI. 45 C.F.R. § 160.103. This definition includes, for example, any person or entity who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services (other than mere payment processing activities) to or for a covered entity.

The Omnibus Rule expands the definition of business associate to include: (1) subcontractors; (2) health information organizations or other entities that provide data transmission services of PHI and require routine access to PHI; (3) any entity that maintains PHI even if the entity does not access or view PHI, such as a data storage facility (whether digital or hard copy); and (4) certain personal health record vendors that provide services to covered entities.

Under the Omnibus Rule, subcontractors will be subject to the same compliance obligations and direct liability as a business associate. HHS rejected the argument that applying the business associate provisions of the HIPAA rules to subcontractors exceeded its statutory authority and concluded that the HITECH Act expressly contemplated that modifying the definition of terms such as business associate may be necessary to carry out the provisions of the Act. HHS reasoned that the privacy and security protections for an individual's PHI should not lapse when a business associate engages a subcontractor to perform functions or services that require access to PHI. Covered entities must enter into agreements with their business associates, and business associates must enter into agreements with their subcontractors, "and so on, no matter how far 'down the chain' the information flows." 78 Fed. Reg. at 5574.

Revised Breach Notification and Reporting Requirements. The Omnibus Rule modifies the breach notification provisions and replaces the "significant risk of harm" standard established by an interim final rule. *See* 74 Fed. Reg. 42740 (Aug. 24, 2009). The "significant risk of harm" threshold is replaced by a presumption that an impermissible use or disclosure of PHI is a breach, unless the covered entity or business associate demonstrates a "low probability" that the PHI was compromised. 45 C.F.R. § 164.402. The risk assessment for assessing the probability that PHI has been compromised must include at least the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and 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. 45 C.F.R. § 164.402(2).

The content and timing requirements for a breach notification are largely unchanged, with one noteworthy exception. For a breach affecting less than 500 individuals, the covered entity must maintain documentation and notify HHS no later than 60 days after the end of the calendar year in which the breach is *discovered*, not the year in which the breach occurred (as under the current rules).

Business associate agreements between business associates and subcontractors must require subcontractors to report a breach to the business associate. Reporting of the breach will then move up the chain until it reaches the covered entity. For example, if a breach occurs at a second-tier subcontractor, that subcontractor must notify the first-tier subcontractor, which then must notify the business associate, which then must notify the covered entity. The covered entity then must notify affected individuals in accordance with the breach reporting requirements.

New Content for Notice of Privacy Practices. The Omnibus Rule also impacts the required content of the notice of privacy practices ("NPP"). In general, NPPs must include a description of the uses and disclosures of PHI that require an authorization, and a statement that other uses and disclosures not included in the notice will be made only with an individual's authorization. NPPs also must include the following separate statements:

- A statement that the covered entity may contact the individual for fundraising purposes (if applicable), and that the individual has the right to opt-out of receiving such communications;
- For group health plans or health insurance issuers, a statement that PHI may be disclosed to the plan sponsor;
- For health plans that perform underwriting, a statement that genetic information may not be used for underwriting purposes (in compliance with the Genetic Information Nondiscrimination Act of 2008);
- A statement that most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require the individual's authorization;
- For health care providers, a statement that individuals may restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service (note that this requirement no longer applies to health plans and should be removed from a plan's NPP); and
- A statement of the individual's right to be notified following a breach of unsecured PHI.

A health plan that posts its NPP on its website must "prominently post" the updated NPP by September 23, 2013, and provide the revised NPP (or information about the changes and how to obtain a copy of the revised NPP) in the next annual mailing to individuals covered by the plan. A health plan that does not post its NPP on a website must provide the revised NPP (or information about the changes and how to obtain a copy of the revised NPP) to individuals covered by the plan within 60 days of the changes (*i.e.*, by November 22, 2013).

Individuals' Access to PHI Expanded. The Omnibus Rule expands an individual's right of access to PHI maintained electronically and shortens the timeframe for covered entities to provide PHI. If an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible. If it is not readily producible, the covered entity must provide the information in a readable electronic form and format as agreed to by the covered entity and the individual. HHS clarified that this electronic right of access requirement preempts contrary state law unless the state law permits greater rights of access to the individual. *See* 78 Fed. Reg. at 5632.

If an individual requests access to PHI, covered entities must provide access within 30 days of the request when possible, with a 30-day extension available (for a total of 60 days, as opposed to the 90 days permitted currently). This timeframe applies regardless of whether the PHI to be accessed is maintained in paper or electronic form. The Omnibus Rule provides additional guidance regarding what reasonable, cost-based fees may be charged to individuals who request access to PHI.

Penalties for Noncompliance. The Omnibus Rule adopts the tiered civil money penalty structure provided by the HITECH Act and implemented in an interim final rule. *See* 74 Fed. Reg. 56123 (Oct. 30, 2009). There are four tiers of increasing penalty amounts to correspond with levels of culpability, and the penalty for all violations of an identical provision is capped at $1.5 million annually. HHS has discretion to determine the amount of a penalty on a case-by-case basis, and may settle any issue or waive a penalty in whole or in part for certain violations.

Next Steps. The changes and clarifications in the Omnibus Rule have a broad ranging impact and touch on virtually all of a covered entity's or business associate's existing HIPAA policies and procedures. Covered entities must review and update existing privacy policies and procedures, breach notification policies and procedures, business associate agreements, and notices of privacy practices. Business associates will need to review and revise existing business associate agreements and enter into compliant business associate agreements with subcontractors who will be subject to the same compliance obligations as a first-tier business associate when the Omnibus Rule takes effect.

About Us

The Law Offices of Jason M. Healy PLLC is a Washington, D.C. based law firm serving national and local clients. We focus primarily on legal issues affecting health care providers and welfare benefit plans. We help health care providers and their trade associations understand Medicare and Medicaid laws and regulations, and address compliance matters. We also represent health care providers in reimbursement audits, appeals, litigation, and transactions. We help sponsors of welfare benefit plans understand and comply with federal and state laws and prepare plan documents. Located in Washington, DC, just minutes from the Department of Health and Human Services, Congressional offices, and the White House, we are well positioned to provide legal support for advocacy efforts. Our Principal, Jason M. Healy, is a health care lawyer with over 14 years of experience with the array of legal issues facing health care providers. Amy D. Healy is an employee benefits lawyer with over 10 years of experience with the regulatory and compliance issues related to welfare benefit plans.