SMITH ANDERSON

Client Alert

April 2013

Newly Effective HIPAA Omnibus Rule Makes Sweeping Changes to HIPAA

The long-awaited final omnibus rule (Omnibus Rule) that modifies the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] took effect last week, on March 26, 2013. Leon Rodriguez, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) calls the changes the "most sweeping" since the HIPAA Privacy and Security Rules were first implemented. Among the changes is an enhanced opportunity for OCR to enforce compliance. **HIPAA covered entities and business associates generally have 6 months – until September 23, 2013 – to become compliant with the Omnibus Rule.**

Who do the Changes Affect?

- HIPAA covered entities, including health care providers, health systems, health plans (including insured and most self-insured employer group health plans) and clearinghouses.
- HIPAA business associates, including a wide range of vendors who contract with covered entities and access protected health information (PHI). Examples include technology vendors, services organizations, accountable care organizations (ACOs), and third party administrators.

What Action is Required?

HIPAA covered entities and business associates should act now to take the following measures:

- Revise Business Associate Agreement template forms;
- Evaluate existing contractor arrangements to determine whether modifications or new agreement provisions are necessary, including to existing Business Associate Agreements;
- Revise HIPAA Policies and Procedures, including modifications to address response to potential breaches involving unsecured PHI;
- Update and redistribute Notices of Privacy Practices;
- Analyze current arrangements for compliance with restrictions on the sale of PHI, and marketing and fundraising restrictions; and
- Train employees on updated obligations.

[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, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. Parts 160 and 164).

Authors

Alicia A. Gilleskie
919.821.6741
agilleskie@smithlaw.com

Mary Pat K. Sullivan
919.821.6692
msullivan@smithlaw.com

Practice Areas

Data Use and Information Privacy

Employee Benefits and Executive Compensation

Health Care

Technology

SMITH ANDERSON
150 Fayetteville Street, Suite 2300
Raleigh, NC 27601
919.821.1220
www.smithlaw.com

Copyright © 2013 by Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. Reproduction in whole or in part is permitted when credit is given to Smith Anderson.

Smith Anderson publishes Alerts periodically as a service to clients and friends. The purpose of this Alert is to provide general information about significant legal developments. Readers should be aware that the facts may vary from one situation to another, so the conclusions stated herein may not be applicable to the reader's particular circumstances.

Some of the Key Changes Under the Omnibus Rule Include:

Definition of Business Associate Expanded. The Omnibus Rule expands the definition of business associate to include:

- Any downstream subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate, even if they have an indirect relationship with a covered entity;
- Health information organizations, e-prescribing gateways, or other persons that provide data transmission services to a covered entity that require routine access to PHI; and
- Any person that offers a personal health record to individuals on behalf of a covered entity.

Covered entities and business associates will want to evaluate existing arrangements to determine whether a Business Associate Agreement is required or modifications to existing agreements are necessary.

Liability and Obligations of Business Associates Expanded. The Omnibus Rule expands the liability and obligations of business associates, such that:

- Business associates and their subcontractors who have access to PHI are directly liable for compliance with the HIPAA Privacy and Security Rules, and thus, may be assessed civil monetary penalties and criminal penalties for violations;
- Business associates and their direct subcontractors that access PHI must enter compliant Business Associate Agreements all the way "down the chain" of the information flow; and
- Business Associate Agreements must be updated to include specific new provisions; however, existing Business Associate Agreements entered before January 25, 2013 that are compliant with the interim rules may operate until the agreement is amended or renewed, or until September 22, 2014, whichever is earlier.

Covered entities and business associates will want to modify their business associate agreement forms not only to include new legal requirements, but also to allocate risk through the use of insurance requirements and indemnity provisions.

Revised Breach Notification Standard. The Omnibus Rule eliminates the "significant risk of harm" standard as the threshold for breach notification.

- Under the previous rule, breaches were not required to be reported unless they posed a "significant risk of reputational, financial or other harm" to individuals. The new standard presumes that a reportable breach has occurred ***unless*** the covered entity or business associate, through the use of a multi-factor risk assessment, determines that there is a ***low probability*** that the PHI has been compromised by the unauthorized use or disclosure.

Copyright © 2013 by Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. Reproduction in whole or in part is permitted when credit is given to Smith Anderson.

Smith Anderson publishes Alerts periodically as a service to clients and friends. The purpose of this Alert is to provide general information about significant legal developments. Readers should be aware that the facts may vary from one situation to another, so the conclusions stated herein may not be applicable to the reader's particular circumstances.

Covered entities and business associates will want to revise their breach notice policies and procedures to reflect this new breach analysis standard.

Marketing, Fundraising, and the Sale of PHI.

- Marketing: The Omnibus Rule imposes stricter limitations on marketing communications made in exchange for financial remuneration. Specifically, written communications promoting purchase or use of a third party's products or services require prior individual authorization if the covered entity receives financial remuneration in exchange for sending the communication. Limited exceptions exist to permit face-to-face marketing communications, certain promotional gifts and refill reminders so long as the remuneration is reasonably related to the cost of the communication.
- Fundraising: The Omnibus Rule provides a limited set of circumstances in which a covered entity can use and disclose certain PHI for fundraising without an authorization. Regardless of whether an authorization for fundraising was required or obtained, covered entities must provide an individual with a clear and conspicuous opportunity to opt-out of receiving future fundraising communications.
- Sale of PHI: The Omnibus Rule prohibits the sale of PHI unless the individual has authorized it. The requisite authorization must acknowledge that the covered entity will receive remuneration in exchange for PHI.

Covered entities and business associates will want to analyze arrangements for compliance with these marketing, fundraising and sale of PHI restrictions.

Changes to Enforcement Rules.

- HHS may impose civil monetary penalties up to $1.5 million for all violations of an identical HIPAA requirement in a calendar year.
- The Omnibus Rule eliminates an exception under the previous rule that shielded covered entities from civil penalties stemming from the conduct of their business associates if certain conditions were met. Under the Omnibus Rule, covered entities and business associates are liable for the acts of their respective business associate agents. Whether a business associate is an agent is based on the Federal common law of agency and depends on the principal's right or authority to control the business associate's conduct in the course of performing services. Covered entities and business associates should consider how best to allocate risk related to any agency relationship through the use of indemnity provisions in the underlying services agreement or their Business Associate Agreement.
- The Omnibus Rule eliminates HHS's discretion in choosing whether to investigate complaints or potential violations in cases where HHS's preliminary review reveals a ***possible*** violation due to willful neglect. HHS is ***required*** to initiate a formal investigation when a party appears to have exhibited willful neglect.

Copyright © 2013 by Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. Reproduction in whole or in part is permitted when credit is given to Smith Anderson.

Smith Anderson publishes Alerts periodically as a service to clients and friends. The purpose of this Alert is to provide general information about significant legal developments. Readers should be aware that the facts may vary from one situation to another, so the conclusions stated herein may not be applicable to the reader's particular circumstances.

Other Notable Changes.

- Covered entities must change their Notices of Privacy Practices to describe certain uses and disclosures of PHI and redistribute such notices to patients.
- The Omnibus Rule gives individuals the right to have their provider restrict certain PHI from disclosure to health plans where the individual pays for the care out-of-pocket in full and requests such a restriction.
- The Omnibus Rule prohibits health plans from using or disclosing genetic information for underwriting purposes, as required by the Genetic Information Nondiscrimination Act.

This Client Alert does not include a full summary of all changes implemented by the Omnibus Rule. For the full rule text, click here. To discuss how these or any other changes provided by the Omnibus Rule may apply to your organization, please contact us.

Copyright © 2013 by Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. Reproduction in whole or in part is permitted when credit is given to Smith Anderson.

Smith Anderson publishes Alerts periodically as a service to clients and friends. The purpose of this Alert is to provide general information about significant legal developments. Readers should be aware that the facts may vary from one situation to another, so the conclusions stated herein may not be applicable to the reader's particular circumstances.