HIPAA and HITECH

What You Need To Know 2014

Brian E. Curtis, Esq.

Counsel, Becker Meisel LLC
Editor, Employment News Alert

Brian E. Curtis, Esq.
Counsel, HR Counsel
BECKER MEISEL LLC

Brian E. Curtis, Esq., is a recognized authority in the areas of employment law and litigation and human resources management, and serves as Counsel to the law firm of Becker Meisel LLC, with office in New York City and in Livingston, Shrewsbury, and Cherry Hill, New Jersey. Mr. Curtis is the founding Editor of the Employment News Alert series of print and e-mail publications, including the 'Year-In-Review' created in 2004, the 'Quarterly Edition' first published in 2006, and the award-winning 'NewsFlash' Special Alert introduced in 2009. He was appointed as his firm's Human Resources Counsel in 2012.

One of the leading experts in New York and New Jersey on the Patient Protection and Affordable Care Act ("ACA"), he regularly speaks about and provides guidance on the legal implications of health care reform to various industry groups and associations, including the health care, staffing, and hospitality industries as well as the accounting, insurance, financial planning, and human resources professions. For the last 3 years, has been leading the NJ State Bar Association's efforts through continuing education to inform the New Jersey legal and business communities of the wide-ranging impact of health care reform. He currently serves as Co-Chair of the ACA Committee for the NJ State Bar Labor & Employment Section.

He is an action-oriented lawyer and business consultant with extensive experience in executive-level and management employment matters, having consulted in multiple senior HR roles, including C-suite recruitment and compensation structuring, business and professional development, talent and performance management, consultancy agreements, cross-functional team leadership, and internal conflict management.

His comprehensive HR knowledge and skill helps clients to successfully navigate through the myriad legal and regulatory landscape that is today's business environment, including assistance with EEOC, HIPAA, ADA, FMLA, as well as state and federal wage/hour laws, and defense of discrimination, harassment, and retaliation claims.

Mr. Curtis has been licensed to practice law since 1992, and has been admitted to practice before the federal U.S. Court of Appeals since 2001. He has been previously appointed as an Attorney-Trustee for the Supreme Court of New Jersey and has been a contributor and guest commentator on CNN, ABC News, and News 12 NJ.

Brian E. Curtis, Esq.
Becker Meisel LLC
Office (732) 576-8700
Fax (732) 576-8740
Direct (973) 251-8946
becurtis@beckermeisel.com

HIPAA Background

Title II of the 1996 Health Insurance Portability and Accountability Act (HIPAA) required the creation and enforcement of multiple regulations, the best known of which is the ***HIPAA Privacy Rule***.

In addition to the Privacy Rule, there is
the ***HIPAA Security Rule*** (initial compliance date April 20, 2005)
and
the ***HITECH Breach Notification Rule*** (initial compliance date February 22, 2010)
(HITECH is the acronym for the Health Information Technology for Economic and Clinical Health Act)

HIPAA rules for Privacy, Security, and Breach Notification would apply to your organization if it meets the definition of a "Covered Entity."

You become a covered entity by transmitting an electronic "covered transaction," such as submitting an electronic claim to an insurance plan. Your organization would also be considered a covered entity if someone else (like a clearinghouse) sends an electronic "covered transaction" on your behalf. If you are a covered entity, you will have already taken certain steps for compliance, such as appointing a HIPAA Privacy Official and a HIPAA Security Official.

If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules. See definitions of "business associate" and "covered entity" at 45 CFR 160.103.

A Covered Entity is one of the following:
A Health Care Provider. This includes providers such as:
•Doctors
•Clinics
•Psychologists
•Dentists
•Chiropractors
•Nursing Homes
•Pharmacies
...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

A Health Plan. This includes:
•Health insurance companies
•HMOs
•Company health plans
•Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

A Health Care Clearinghouse
This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Breach Notification

The Health Information Technology for Economic and Clinical Health (HITECH) Act authorized the creation and enforcement of a Breach Notification Rule that amended parts of the HIPAA Privacy and Security Rules.

The Breach Notification Rule requires covered entities to provide notification of breaches of unsecured patient information to affected individuals, the federal government, and in some cases, the media.

A number of states, including New York, require that notice may be necessary even if there has been no actual breach.

New York State
A 4254; A 3492

N.Y. St. Tech. Law sec. 208 (applies to state agencies)
N.Y. St. Gen. Bus. Law sec. 899-aa (applies to private businesses)

- Specific notice content is required
- An encryption 'safe harbor' exists in the statute (unless the encryption key has also been "acquired")
- Electronic notice of breach may only be made if consent to such notification has been obtained in advance
- Breach notice is also required to be tendered to the NY State AG and the NY State Consumer Protection Board
- Penalties range from $5,000 to $10,000 per violation up to $150,000 in a calendar year
- No private cause of action – can only be brought by State AG within a 2-year statute of limitations period

Business Associates

HIPAA defines a "business associate" to generally mean an outside person or entity that does a service for a covered entity that involves patient information. Examples include a billing service, practice management or EHR system vendor, document storage company, collection agent, or shredding firm.

HIPAA does not permit a covered entity to let a business associate access patient information until such entity and the business associate have signed a written agreement containing certain required provisions. This agreement is called a "business associate agreement" or "business associate contract." A covered entity must identify each of its business associates and have a compliant agreement in place with each of them.

Deadlines

September 22, 2014 - covered entities must update all of their business associate agreements that were entered into on or before January 24, 2013 ***which had not been modified or renewed after that date***

Automatic renewal agreements: if a business associate agreement was entered into on or before January 24, 2013, and has not been modified after that date, but renews automatically without any change in terms, your compliance deadline date within which to update by September 22, 2014.

Oral agreements: if your organization does not have a written business associate agreement in place, you must do so immediately.

The Omnibus Rule

On January 17, 2013, the US Department of Health and Human Services Office for Civil Rights announced the publication of the HIPAA Privacy and Security Omnibus Final Rule. The Omnibus Final Rule strengthens and re-affirms HIPAA Privacy, HIPAA Security, and HITECH Breach Notification requirements. The Omnibus Final rule also strengthens and finalizes HIPAA provisions that translate into a much more active and tougher enforcement position by HHS and its OCR division regarding HIPAA Privacy and Security.

What does the Omnibus Rule actually include?

In broad terms, the Rule addresses three specific areas that have a bearing on medical and dental professionals as either covered entities or as business associates:

1. Modifies the HIPAA Privacy, Security, and Enforcement regulations in the following ways:

    - Makes business associates and subcontractors of business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rule requirements
    - Strengthens the limitations on the use and disclosure of protected health information (PHI) for marketing and fundraising purposes, and prohibits the sale of PHI without individual authorization
    - Expands an individual's rights to receive electronic copies of his or her health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full
    - Requires modifications to a covered entity's Notice of Privacy Practices
    - Adopts the additional HITECH Act enhancements to the Enforcement Rule, particularly regarding privacy breaches and penalties

2. Creates an increased and tiered civil money penalty structure for security breaches under the HITECH Act.
3. Modifies and clarifies the definition of what constitutes a reportable privacy breach and the factors covered entities and business associates must consider when determining whether a reportable breach has occurred.

What are the penalties for security breaches?

The Omnibus Rule formally adopts the following penalty scheme for violations of the HITECH Act occurring on or after Feb. 18, 2009:

- For violations where a covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, a penalty of not less than $100 or more than $50,000 for each violation
- For a violation due to reasonable cause and not to willful neglect, a penalty of not less than $1,000 or more than $50,000 for each violation
- For a violation due to willful neglect that was timely corrected, a penalty of not less than $10,000 or more than $50,000 for each violation
- For a violation due to willful neglect that was not timely corrected, a penalty of not less than $50,000 for each violation; the penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1.5 million in a calendar year

What constitutes a reportable breach?

Any impermissible use or disclosure of PHI is presumed to be a breach, with a subsequent requirement to provide a breach notification, unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Importantly, the covered entity or business associate, as applicable, has the burden of demonstrating that all notifications were provided or that an impermissible use or disclosure did not constitute a breach, and they must maintain documentation sufficient to meet that burden of proof.

What determines whether PHI has been compromised?

In determining whether notice of a breach is required, a covered entity or business associate must consider at least the following 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
- The extent to which the risk to the PHI has been mitigated

TO DO LIST:

Consult with your counsel

The below items do NOT constitute a complete or exhaustive list of all the steps you must now take to be compliant. We have included only a partial list of your compliance obligations so as to ensure your understanding of the risk exposure for failing to abide by these new requirements under the law. For additional information and assistance, you may contact Mr. Curtis.

What do you have to do to remain HIPAA-compliant under the new rules?

Most of your practices are "Covered Entities" under HIPAA and may also be "Business Associates" to other providers. Generally, a covered entity is a healthcare provider who transmits any health information in electronic form, and a business associate is a person who creates, receives, maintains, or transmits PHI on behalf of a covered entity; business associates may also include subcontractors of an entity. Whether a covered entity or a business associate, you must update your BAAs and your NPPs. You must also consistently monitor, and update as needed, your HIPAA policies and procedures, particularly those regarding privacy breaches and reporting.

Are there additional changes to the definition of business associates?

Yes—business associates now also include:

- ***An individual who creates, receives, maintains, or transmits PHI on behalf of a covered entity.***

Do you need to update your BAAs?

- Business associates must comply, where applicable, with the Security Rule with regard to electronic PHI.
- Business associates must report breaches of unsecured PHI to covered entities.

What changes do you have to make to your Notice of Privacy Practices (NPP)?

- A statement indicating that authorization is required for uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI. If the Covered Entity records or maintains psychotherapy notes, it must also include a statement indicating that authorization is required for most uses and disclosures of those notes.
- A statement that other uses and disclosures not described in the NPP will be made only with authorization from the individual to whom the PHI relates.

Because these changes constitute "material changes" under HIPAA, the revised NPP must be provided to all new patients and made available to existing patients upon request, posted to the office website, and prominently posted in the offices.

Criminal Penalties

The U.S. Department of Justice (DOJ) has already clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable PHI in violation of HIPAA or HITECH face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Covered Entity and Specified Individuals

The DOJ has concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

Knowingly

The DOJ interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of HIPAA is not required.

Resolution Agreements

Resolution Agreements and Civil Money Penalties

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 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 19 resolution agreements and issued CMPs to one covered entity.