Employee Benefits and Executive Compensation | Health Law Advisory: Complying with the HIPAA Privacy and Security Mandates under the HITECH Act: A Field Guide for Benefits Brokers and Consultants and other Business Associates

1/20/2010

Better known colloquially as the "stimulus" bill, the American Reinvestment and Recovery Act of 2009 (the Act) contained a hodgepodge of additional provisions with little apparent connection to the U.S. economy. Title XIII of the Act, entitled the Health Information Technology for Economic and Clinical Health (HITECH) Act, is such a provision. Among other things, HITECH makes "business associates" directly responsible for complying with certain provisions of the HIPAA privacy rule and all of the HIPAA security rules. But as a consequence of an important disconnect between the Act's legislative history relating to the scope of the expansion of the privacy rule, it is not entirely clear what is required. Moreover, while the statutory effective date is fast approaching, the Department of Health and Human Services (HHS) has yet to issue guidance in the matter. For a full discussion of the requirements imposed by the HITECH Act, please click here to read our HITECH Summary.

While all HIPAA business associates are affected, the problem is particularly acute for benefits brokers and consultants who advise group health plans and on whom employers and plan sponsors rely to assist with their HIPAA compliance. The purpose of this advisory is to explain the status of the HITECH privacy and security mandates as they apply to business associates and to offer three possible approaches to compliance—low, medium, and high—that business associates might pursue pending the issuance of formal guidance.

Background/Prior Law

The administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a comprehensive set of rules regulating, among other things, the privacy and security of medical information.

The Privacy Rule

The HIPAA privacy rule established a set of patient rights, including the right of access to one's medical information, and placed certain limitations on when and how health plans and health care providers may use and disclose protected health information (PHI). Interpretive regulations prescribe detailed rules governing the conduct of "covered entities." Covered entities include health care providers, health care clearinghouses and health plans—including employer-sponsored group health plans. Generally, plans and providers may use and disclose health

information for the purpose of treatment, payment, and other health care operations without the individual's authorization and with few restrictions. In certain other circumstances (*e.g.*, disclosures to family members and friends), the rule requires plans and providers to give the individual the opportunity to object to the disclosure. The rule also permits the use and disclosure of health information without the individual's permission for various specified activities (*e.g.*, public health oversight, law enforcement) that are not directly connected to the treatment of the individual. For all uses and disclosures of PHI that are not otherwise required or permitted by the rule, plans and providers must obtain a patient's written authorization.

The Privacy Rule imposes on covered entities a series of requirements designed to safeguard PHI. These include the following:

- **Privacy Policies and Procedures.** A covered entity must adopt written privacy policies and procedures that are consistent with the Privacy Rule.
- **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.
- **Workforce Training and Management.** Workforce members include employees, volunteers, and trainees, and may also include other persons whose conduct is under the direct control of the covered entity (whether or not they are paid by the entity). A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must also have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.
- **Mitigation**. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
- **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule, and to limit its incidental use and disclosure pursuant to otherwise permitted or required uses or disclosures.
- **Complaints**. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice. Among other things, the covered entity must identify to whom individuals may submit complaints and advise that complaints also may be submitted to the Secretary of HHS.
- **Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.
- **Documentation and Record Retention.** A covered entity must maintain documentation, until six years after the later of the date of their creation or last effective date, of its privacy policies and procedures, privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

The Security Rule

HIPAA dictates a suite of security-related rules under which covered entities must:

- ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the rule
- ensure compliance with the rule by its workforce.

Covered entities must implement reasonable and appropriate written polices and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule. They must also maintain documentation for six years from the later of the date of creation or last use, make the documentation available to those persons responsible for implementing the procedures to which the documentation relates, and review documentation periodically, and update as needed, to reflect environmental or operational changes that affect the security of ePHI.

Business Associates

Both the HIPAA privacy and security rules permit covered entities to share health information with "business associates" who provide a wide variety of functions for them, including legal, actuarial, accounting, data aggregation, management, administrative, accreditation, and financial services. A covered entity is permitted to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided certain requirements are satisfied, including a requirement that the covered entity enter into a written agreement with the business associate containing business associate covenants. Importantly, however, because the privacy and security rules govern covered entities, neither rule imposed any substantive requirements directly on business associates. Therefore, prior to HITECH, violations of the HIPAA privacy and security rules could not be enforced directly against business associates.

Summary of the HITECH Changes

HITECH generally expands the reach of the HIPAA privacy and security provisions, and their accompanying penalties, to business associates. With respect to the security requirements, Act § 13401(a) is clear:

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business

associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 establish rules requiring the adoption of administrative, physical, and technical safeguards, and implementation of reasonable and appropriate policies and procedures. (Administrative safeguards are intended to address the organization of the internal security infrastructure of a covered entity or business associate; physical safeguards are intended to protect electronic systems and data from threats, environmental hazards, and unauthorized access; and technical safeguards are primarily IT functions used to protect and control access to data.) As a result, a business associate is now obligated to comply with the requirements of the HIPAA security rule in the same way and to the same extent as a covered entity. This will require business associates to, among other things, conduct a formal risk assessment, appoint a security officer, adopt written security policies and procedures, and train their employees. They will also need to implement safeguards to protect ePHI, such as encrypting e-mails and computer files and limiting access to records.

Separately, business associates will need to consider the adoption of encryption standards that are at least consistent with HHS standards for rendering PHI unusable, unreadable or indecipherable, so that it is no longer "unsecured" and subject to onerous notification requirements in the event of breach. (See our HITECH Summary for an explanation of the rules governing the breaches involving unsecured PHI.) These obligations will also be required to be included in business associate agreements.

The extent to which business associates must comply with the requirements of the HIPAA privacy rule also seems clear if one looks only to the statute. Act § 13404(a) reads:

In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance *with each applicable requirement of section 164.504(e) of such title*. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity. (Emphasis added.)

45 C.F.R. § 164.504(e) governs business associate agreements. The substantive requirements of the HIPAA privacy rule (which are described above) are set out in 45 C.F.R. § 164.512, to which HITECH makes no reference. Thus, while business associates are now bound by the requirement to enter into a business associate agreement, they are not, at least according to the express provisions of the statute, required to comply with the substance of each particular privacy requirement. But this is not the view expressed by the Conference Committee report accompanying the Act, which includes the following statement as to the legislators' intent:

The House bill would apply the HIPAA Privacy Rule, the additional privacy requirements, and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to the providers and health plans for whom they are working.

Given the clear statutory language, it is unlikely that that HHS would attempt to impose substantive privacy requirements on business associates. It is nevertheless possible that the regulators might seek to add some substantive privacy requirements to ensure that business associates are taking affirmative steps to comply, beyond merely signing a business associate agreement.

Compliance Steps

HITECH's business associate provisions take effect February 17, 2010. Absent guidance, what is a business associate to do? We offer three possible approaches below.

1. *The "low" option: do nothing; wait for guidance*

We do not endorse this approach; rather, we include it for the sake of completeness and also recognizing that some business associates may adopt this approach simply by virtue of being unaware of the rules. The statute is clear enough on its face: certain action is required by a particular date. Failure to comply exposes the business associate to penalties under HIPAA, which penalties have been expanded upon under the Act. Moreover, there would also be a ripple effect in the event of a breach of the Act's new breach notice rules.

NOTE: In informal discussions with representatives of the HHS Office for Civil Rights, we understand that the department is contemplating a delayed regulatory effective date. But if it does so, it would be purely a matter of discretion, which should not be counted on and cannot be prudently anticipated.

2. *The "medium" option: bare-bones compliance*

At a minimum, covered entities and business associates should enter into updated business associate agreements that comply with HITECH. The possibility that HHS might subsequently provide us with model language is no reason to delay. Because the additional, substantive HITECH privacy requirements apply to covered entities *and* business associates, business associates should also adopt policies and procedures for these items, the most significant of which is the "breach-notice" rule.

Compliance with the security rule is trickier. While the preamble to the final security rule claims that these rules are "scaleable," in practice this characterization provides little in the way of comfort or relief. There are over two dozen mandatory and optional standards and sub-standards that must be addressed in written policies and procedures. "Policies and procedures" documents tend to be lengthy and complex as a result. Also, their nature is such that they require a good deal

of customization. Thus, any "model" document will likely require extensive modification. Nevertheless, business associates should, at a minimum, do the following:

- Undertake and complete a security risk assessment
- Prepare and adopt written security policies and procedures
- Conduct workforce training in the policies and procedures.

3. *The "high" option: full-blown compliance*

A business associate could choose to comply with the full panoply of HIPAA privacy and security requirements in the same manner as they apply to covered entities. While this might seem like overkill, it ensures compliance. In addition, some covered entities require more than bare-bones compliance of their business associates as a matter of contract. Conversely, some business associates choose to "over-comply" in order to gain a competitive advantage in the marketplace.

Conclusion

The Act has both raised and broadened the HIPAA compliance bar for business associates. Prior law gave business associates something of a free pass. That was—as they say—then. Among other things, business associate agreements will need to be reviewed and updated to comply with HITECH's new rules, and employees with access to PHI will need to be trained. Covered entities and business associates should be aggressively moving to anticipate these rules and to comply with them even in the absence of guidance.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Employee Benefits and Executive Compensation

Alden Bianchi
Practice Group Leader, Employee Benefits and Executive Compensation
(617) 348-3057
AJBianchi@mintz.com

BOSTON

Tom Greene
(617) 348-1886
TMGreene@mintz.com

Addy Press
(617) 348-1659
ACPress@mintz.com

Patricia Moran
(617) 348-3085
PAMoran@mintz.com

NEW YORK

David R. Lagasse
(212) 692-6743
DRLagasse@mintz.com

Gregory R. Bennett
(212) 692-6842
GBennett@mintz.com

Jessica Catlow
(212) 692-6843
JCatlow@mintz.com

Health

Karen S. Lovitch
Managing Member, Health Law Practice
(202) 434-7324
KSLovitch@mintz.com

Stephen M. Weiner
Chair, Health Law Practice
(617) 348-1757
SWeiner@mintz.com

BOSTON

Dianne J. Bourque
(617) 348-1614
DBourque@mintz.com

Thomas S. Crane
(617) 348-1676
TSCrane@mintz.com

Deborah A. Daccord
(617) 348-4716
DADaccord@mintz.com

Brian P. Dunphy
(617) 348-1810
BDunphy@mintz.com

Garrett G. Gillespie
(617) 348-4499
GGGillespie@mintz.com

Rachel M. Irving
(617) 348-4454
RMIrving@mintz.com

Ellen L. Janos
(617) 348-1662
EJanos@mintz.com

M. Daria Niewenhous
(617) 348-4865
DNiewenhous@mintz.com

Melissa O'Neill Thatcher
(617) 348-3015
MOThatcher@mintz.com

NEW YORK

Stephen C. Curley
(212) 692-6217
SCCurley@mintz.com

Andrew B. Roth
(212) 692-6889
ARoth@mintz.com

Nili S. Yolin
(212) 692-6799
NSYolin@mintz.com

WASHINGTON

Susan W. Berson
Managing Member,
Washington, D.C. Office
(202) 661-8715
SBerson@mintz.com

Michael D. Bell
(202) 434-7481
MDBell@mintz.com

Stephen R. Bentfield
(202) 585-3515
SRBentfield@mintz.com

Theresa C. Carnegie
(202) 661-8710
TCCarnegie@mintz.com

Robert D. Clark
(202) 434-7402
RDClark@mintz.com

Hope S. Foster
(202) 661-8758
HSFoster@mintz.com

Lauren N. Haley
(202) 434-7386
LNHaley@mintz.com

Sarah A. Kaput
(202) 434-7423
SAKaput@mintz.com

Katina W. Lee
(202) 661-8729
KLee@mintz.com

Carrie A. Roll
(202) 434-7350
CARoll@mintz.com

Tara E. Swenson
(202) 585-3504
TESwenson@mintz.com

Jennifer E. Williams
(202) 585-3542
JEWilliams@mintz.com