Bloomberg BNA

Pension & Benefits Daily ™

View From Groom: Get Ready for Sweeping Changes in HIPAA Privacy Regulations

BY CHRISTY TINNES AND VIVIAN HUNTER TURNER

On Jan. 25, 2013, the Department of Health and Human Services published an omnibus Health Insurance Portability and Accountability Act (HIPAA) privacy regulation that initiated sweeping changes to the landscape of health information privacy. The new final rule applies certain parts of the HIPAA Privacy and Security Rule to business associates, expands an individual's right to access their protected health information, and requires revisions to the Notice of Privacy Practices. The final HIPAA regulation is effective March 26, 2013, with a compliance date of Sept. 23, 2013, and provides a transition period for business associate agreements, as discussed in more detail below.[1]

[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. 5,566 (Jan. 25, 2013) (13 PBD, 1/18/13; 40 BPR 183, 1/22/13).

Christy Tinnes (ctinnes@groom.com) is a principal at Groom Law Group in Washington. She is involved in all aspects of health and welfare plans, including ERISA, HIPAA portability, HIPAA privacy, COBRA, and Medicare. She represents employers designing health plans as well as insurers designing new products. Vivian Hunter Turner (vturner@groom.com) is an associate in the Health and Welfare practice at Groom. Her practice includes a broad array of issues relating to HIPAA portability, HIPAA privacy, compliance with state and federal insurance regulations, and ERISA.

Civil and Monetary Penalty

Prior to the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the maximum fine imposed for violations of HIPAA was $100 for each violation, with the total amount imposed on a covered entity for all violations of an identical requirement or prohibition not to exceed $25,000. The new final rule adopts the following two-tier penalty scheme, as outlined under the HITECH Act, with a maximum penalty greatly increased to $1,500,000 in a calendar year:

Covered Entity Liability For Business Associate Conduct

Under the new final rule, a covered entity may be liable for the acts of a business associate that is an ''agent'' of the covered entity. The preamble to the regulations indicates that the analysis of whether a business associate is an agent is a fact-specific determination that should take into account the terms of the business associate agreement and whether an agency relationship exists under federal common law. The preamble specifies that the essential factor in determining whether an agency relationship exists is the right of the covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity and goes on to list several factors that should be considered in any analysis to determine the scope of agency:

- the time, place, and purpose of a business associate agent's conduct;
- whether a business associate agent engaged in a course of conduct subject to a covered entity's control;
- whether a business associate agent's conduct is commonly performed by a business associate to accomplish the service provided on behalf of a covered entity; and
- whether or not the covered entity reasonably expected that a business associate agent would engage in the conduct in question.

Practice Tip—Drafting the Business Associate Agreement

The business associate agreement can play a key role in framing and documenting the intentions of the covered entity and business associate, which may be useful in analyz-

 ISSN

ing whether the parties intended the business associate to be an ''agent'' of the covered entity. Consider the extent that a business associate agreement allows a covered entity to give interim instructions or directions to the business associate and the avenues that the covered entity has to control the business associate. While not determinative, also consider an express statement that the business associate is not an agent of the covered entity.

Direct Liability for Business Associates

Before the HITECH Act, the HIPAA Privacy and Security Rules did not apply directly to business associates of covered entities. However, under the new final rule, some of the Privacy Rule requirements and all of the Security Rule's requirements apply directly to business associates. This means that a business associate must comply with these requirements in the same manner as a covered entity. Further, the new final rule provides that business associates may be civilly and criminally liable for violations of these provisions.

Practice Tip—Business Associates and HIPAA

As a practical matter, business associates of every size will now have to be prepared to undertake the formal administrative safeguards related to electronic protected health information, such as performing a risk analysis, designating a security official, adopting written policies and procedures, and conducting employee training. The new final rule provides some relief in that it continues to provide that covered entities and business associates have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard.

Violation Category	Each Violation	Maximum Penalty for Violations of an Identical Provision in a Calendar Year
The covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision.	$100-$50,000	Up to $1,500,000
Violation is due to reasonable cause and not to willful neglect.	$1,000-$50,000	$1,500,000
Violation was due to willful neglect and was timely corrected.	$10,000-$50,000	$1,500,000
Violation was due to willful neglect and was not timely corrected.	At least $50,000	$1,500,000

Business Associate Agreements

The new final rule includes changes to the content of business associate agreements that will apply to existing business associate agreements. In addition, under the new final rule, business associates are now also required to have business associate agreements in place with any subcontractors that also use protected health information. The Department of Health and Human Services has published sample business associate language on its website.

Practice Tip—Sample Business Associate Agreement

While the Department of Health and Human Service website has sample business associate agreement language, a covered entity, business associate, or subcontractor likely will want different terms in their business associate agreements, depending on their roles. Entities that have dual roles, such as a business associate that enters into agreements with both covered entities and subcontractors, may want two different templates.

The new business associate agreement regulations apply as of Sept. 23, 2013. However, the new final rule adopts a transition provision to grandfather certain existing contracts until they are otherwise renewed. The additional transition period is available if, prior to Jan. 25, 2013, the covered entity or business associate had an existing contract or other written arrangement with a business associate or subcontractor that complied with the prior provisions of HIPAA and such contract or arrangement was not renewed or modified from March 26, 2013, until Sept. 23, 2013. Existing business associate agreements are considered compliant with the modifications to HIPAA until either the covered entity or the business associate has renewed or modified the contract following the compliance date of the modifications, or until Sept. 23, 2014, whichever is sooner. In cases where the contract renews automatically, i.e., evergreen contracts, such contracts are eligible for the extension regardless of the date that the contract automatically rolls over.

Breach Analysis

The HITECH Act requires covered entities to provide notification to affected individuals and the Secretary of the Department of Health and Human Services following the discovery of a breach of unsecured protected health information. The new final rules replace the prior ''harm threshold'' in the security breach rules and now define a ''breach'' to mean the unauthorized acquisition, use, or disclosure of protected health information that compromises the security or privacy of such information. The new final rule clarifies that an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates under a risk assessment that there is a low probability that the protected health information has been compromised.

In conducting the risk assessment, the regulations provide that covered entities should consider:

- the nature and extent of the protected health information involved,
- the unauthorized person who used the protected health information or to whom the disclosure was made,
- whether the protected health information was actually acquired or viewed, and
- the extent to which the risk to the protected health information has been mitigated.

  ISSN

If the covered entity determines that a breach has occurred, it must notify the individuals involved without unreasonable delay and in no case later than 60 days following the discovery of a breach. The covered entity must notify the Department of Health and Human Services and in some cases the media if the breach involves more than 500 residents in a state. The notice must include, to the extent possible:

- a description of the breach;
- a description of the types of information that were involved in the breach;
- the steps affected individuals should take to protect themselves from potential harm;
- a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
- contact information for the covered entity.

Practice Tip— Reporting the Breach Internally

The new final rule clarifies that a breach should be treated as discovered by a covered entity or business associate as of the first day on which such breach is known or should reasonably have been known. It is important to note that the breach is treated as discovered by the covered entity at the time the workforce member or other agent has knowledge of the breach. Covered entities and business associates should review and update their HIPAA training materials and HIPAA policies and procedures to stress the importance of reporting breaches and provide clear guidance on how and to whom breaches should be reported internally.

Revisions to Definition of Marketing/Sale Of Protected Health Information

The new final rule generally treats most subsidized communications as marketing and requires authorization for communications where the covered entity receives financial remuneration from a third party whose product or service is being marketed. Further, under the new final rule, where a business associate, as opposed to the covered entity itself, receives financial remuneration from a third party in exchange for making a communication about a product or service, such communication also requires prior authorization from the individual. In addition, the new final rule prohibits any remuneration (financial or in-kind) in exchange for protected health information, unless the covered entity obtains authorization.

Practice Tip—Marketing Materials

Plans should review communications that appear to promote a product or service and analyze the content and any direct or indirect remuneration involved under the marketing rules. In addition, if plans provide protected health information to a third party, such as a data warehouse, they should ensure they are not receiving any remuneration, including in-kind remuneration such as the computer to store and send the data.

Modifications to HIPAA under GINA

The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits discrimination based on an individual's genetic information in both health coverage and employment. The new final rule applies the GINA prohibition on using and disclosing genetic information for underwriting to all health plans that are covered entities, including those to which GINA does not expressly apply, such as HIPAA excepted benefits. The new final rule does include an exception for long term care policies.

Practice Tip—GINA Compliance

Health plans should carefully review how they use or disclose family history to ensure they are in compliance with both GINA and now the new HIPAA privacy rules.

Quick Reference Chart

Contract Type	Compliance Date
■ Contracts or arrangements entered into prior to Jan. 25, 2013, and **not** renewed from March 26, 2013, until Sept. 23, 2013	The business associate agreement is compliant until the earlier of renewal/ modification of contract **or** Sept. 23, 2014
■ Contracts or arrangements entered into prior to Jan. 25, 2013, and renewed or modified from March 26, 2013, until Sept. 23, 2013	Sept. 23, 2013
■ New contract entered into Jan. 25, 2013, or later	Later of Sept. 23, 2013, or date of new contract
■ Evergreen contracts (contracts that renew automatically without any change in terms or other actions by the parties)	Sept. 23, 2014

*Note that the transition provision only applies to requirements to amend business associate agreements and not to any other compliance obligations under HIPAA.

Changes to Notices of Privacy Practices

Covered entities currently are required to provide individuals with a Notice of Privacy Practices (NPP) that describes how protected health information will be used and disclosed and an individual's rights with respect to their protected health information. Under the new final rule, the NPP must be revised to include the following:

- a statement indicating that most uses and disclosures of psychotherapy notices, uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization;
- a statement that other uses and disclosures not described in the NPP will be made only with authorization from the individual;
- a statement regarding fundraising communications and an individual's right to opt out of receiving such communications, if a covered entity intends to contact an individual to raise funds for the covered entity;
- a statement of the right of affected individuals to be notified following a breach of unsecured protected health information; and

■ a statement regarding an individual's right to restrict protected health information if they have paid out of pocket in full for services.

The new final rule requires providers to deliver their NPP by Sept. 23, 2013. The new final rule requires a health plan that currently posts its NPP on its website to: (1) prominently post the material change or its revised notice on its website by Sept. 23, 2013, and (2) provide the revised notice in its next annual mailing to individuals. Health plans that do not post their NPP on their websites are required to provide the revised NPP within 60 days of the effective date – or Nov. 23, 2013.

Practice Tip—Notice of Privacy Practices

Health plans should add updating their privacy notices to their list of notices typically provided at enrollment, which for most plans occurs in the fall. Plans that post their Notice of Privacy Practices online will have more flexibility and can simply update their online posting and deliver updated Notice of Privacy Practices with their enrollment materials or other annual mailing.

Access of Individuals To Protected Health Information

Under the HIPAA Privacy Rule, individuals have a right to review or obtain copies of their protected health information to the extent such information is maintained in the designated record set of a covered entity. The new final rule strengthens the Privacy Rule's existing right of access to the extent that a covered entity maintains electronic health records. Under the new final rule, an individual has the right to obtain from the covered entity a copy of his or her information in an electronic format requested by the individual, if it is readily producible or, if not, in a reasonable electronic form and format as agreed to by the covered entity and the individual.

The new final rule also modifies the deadlines for a covered entity to provide access to protected health information. The HIPAA Privacy Rule currently permits a covered entity 60-days to provide access to protected health information maintained off-site and provides a one-time 30-day extension. Under the new final rule, the time frame is reduced and now provides a covered entity 30-days to provide access to protected health information maintained off-site while retaining the 30-day extension period. The preamble to the new final rule says that the department believes 30 days is ''appropriate and achievable . . . given the increasing expectation and capacity to provide individuals with almost instantaneous electronic access to protected health information.''[2]

Practice Tip—Electronic Access

Covered entities that rely on business associates to fulfill the access requirement should make sure business associates understand these new rules for electronic access and the new time frames. Covered entities may want to specify these new requirements in their updated business associate agreements.

Conclusion

The new final rules are dense and nuanced and make significant changes regarding privacy and security protections initiated under the initial passage of HIPAA in 1996. Covered entities should consider taking the following steps to bring themselves into compliance:

1. Review HIPAA policies and procedures to integrate revisions mandated by the new regulations, including but not limited to the new breach risk assessment, electronic access requirements, and marketing restrictions.

2. Review vendors that have executed business associate agreements and confirm whether new vendors should be added to the list (for business associates, this may mean new business associate agreements with subcontractors). Review business associate agreements in light of the new regulations and consider whether existing contracts should be amended.

3. Review the Notice of Privacy Practices and make conforming changes based on the new regulations.

4. Review and update HIPAA training materials and make sure that the appropriate workforce has been trained on the new regulations.

5. Review and update the HIPAA security assessment related to electronic protected health information (for business associates this is a new requirement since they are now directly liable under the HIPAA security standards).

[2] 78 Fed. Reg. 5,637.

  ISSN