VENABLE® LLP

Articles

July 2013

What Your Nonprofit Needs to Do about HIPAA – Now

AUTHORS

Thora A. Johnson
Peter P. Parvis
Jennifer Spiegel Berman
Molly E. G. Ferraioli
Jessica E. Kuester

DOWNLOADABLE FILES

- What Your Nonprofit Needs to Do about HIPAA – Now

RELATED PRACTICES

Healthcare

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

Whether your nonprofit entity is an employer that provides health insurance to your employees, an organization in the growing health care industry, a hospital, or other medical provider—or you provide services to any of those entities—you need to know about changes to the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which were made by the final omnibus HIPAA rule issued by the U.S. Department of Health and Human Services (HHS) on January 25, 2013 (the "Final Regulations"). These Final Regulations implement changes made under the Health Information Technology for Economic and Clinical Health Act (HITECH). Nearly every organization in the health care industry (and every service provider to those organizations) is affected by these changes.

Among other things, the Final Regulations:

- Directly subject Business Associates,[1] including their Subcontractors (or "downstream" Business Associates), to the HIPAA security rule and many aspects of the HIPAA privacy rule.
- Require amended Business Associate Agreements between Covered Entities and Business Associates to reflect the changes made by the Final Regulations and, for the first time, Business Associate Agreements between Business Associates and their Subcontractors.
- Require Covered Entities to notify affected individuals, the federal government, and the media (in certain circumstances) of any "breach" of Unsecured PHI.
- Expand an individual's right to receive electronic copies of his or her PHI and restrict disclosures to a health plan concerning treatment for which an individual has paid out of pocket in full.
- Permit additional categories of PHI to be used in fundraising, enhance the limitations on the use of PHI for marketing, and prohibit the sale of PHI without individual authorization.
- Significantly strengthen the authority of the federal government to enforce the HIPAA privacy and security rules.

Below is a list of action items for Covered Entities and Business Associates to consider in preparing for the compliance deadline (generally, September 23, 2013). Following the list of action items is a more detailed summary of the changes made by the Final Regulations.

Action Items for Covered Entities and Business Associates (including Subcontractors)

Except for updating "grandfathered" Business Associate Agreements, Covered Entities and Business Associates, including Subcontractors, have until September 23, 2013 to come into compliance with the Final Regulations. To do so, Covered Entities and Business Associates, including Subcontractors, must:

- Review their current privacy and security compliance program;
- Enter into, or amend, as appropriate, Business Associate Agreements to reflect the Final Regulations;
- Educate Business Associates (including Subcontractors), as necessary, about their responsibility (and the responsibility of their Subcontractors) to safeguard PHI so as to mitigate chances of agents causing upstream liability;
- Conduct a HIPAA security risk analysis and prepare/update a risk management plan. As part of this process, consider implementing encryption and destruction technologies in order to minimize the risk that PHI will be considered Unsecured PHI and, thus, able to be "breached;"
- Create processes to discover breaches of Unsecured PHI;
- Prepare/update a policy about how to handle breaches of Unsecured PHI;

- Draft/update the other HIPAA security and privacy policies;
- Update forms to reflect changes to individual rights;
- Conduct HIPAA training on the updated policies; and
- Update and distribute a Notice of Privacy Practices, as applicable.

Delayed Compliance Deadline for Grandfathered Business Associate Agreements

If a compliant Business Associate Agreement was in place before January 25, 2013, and it is not otherwise renewed or amended after March 25, 2013 (i.e., it is a "grandfathered Business Associate Agreement"), then it generally does not need to be updated to comply with the Final Regulations until September 22, 2014. Agreements that renew automatically through evergreen clauses qualify for this extended compliance date.

Changes Impacting Business Associates (including Subcontractors)

Business Associates, including Subcontractors, will be directly liable (and not simply contractually liable pursuant to their Business Associate Agreements) for complying with certain provisions of HIPAA, including:

- All of the administrative, physical, and technical standards of the HIPAA security rule in the same manner as Covered Entities.
- The use and disclosure requirements of the HIPAA privacy rule in the same manner as Covered Entities.

> **CAUTION:** As of September 23, 2013, entities that create, receive, maintain, or transmit PHI on behalf of a Business Associate (in other words, Subcontractors) will be required to comply with all of the HIPAA provisions that apply to Business Associates because they will, in fact, be treated as Business Associates under the Final Regulations.

Moreover, Covered Entities can be held directly liable for the acts and omissions of their Business Associates that are acting within the scope of their agency. Importantly, this is the case even if the act or omission violates a provision of the Business Associate Agreement. For this purpose, the Final Regulations rely on the federal common law of agency (rather than potentially disparate state laws). An agency relationship is established where a Covered Entity has the right or authority to control its Business Associate's conduct in the course of performing a service on behalf of the Covered Entity. Similarly, Business Associates can be held directly liable for the acts and omissions of their Subcontractors.

As such, care will need to be taken as Business Associate Agreements are updated or put in place. Where a Business Associate is acting as a Covered Entity's agent, consideration should be given to whether indemnification provisions are appropriate.

Covered Entities and Business Associates Must Provide Notice of a Breach Involving "Unsecured" PHI

Since September 23, 2009, Covered Entities have been required to notify affected individuals within 60 days after a "breach" of Unsecured PHI is discovered. (A breach is deemed "discovered" on the first day that the "breach" is known or should reasonably have been known.) Covered Entities are also required to provide notice to HHS and, in certain circumstances, to the local media.

The threshold for determining whether an unauthorized use or disclosure of PHI constitutes a "breach" for this purpose will change as of September 23, 2013. Under interim final breach notification rules, the security and privacy of Unsecured PHI is deemed to be "breached" where the unauthorized use or disclosure of such information poses a significant risk of financial, reputational or other harm to the individual or individuals whose PHI was compromised.

As of September 23, 2013, the unauthorized acquisition, access, use or disclosure of Unsecured PHI will be presumed to be a breach for purposes of the breach notification rule, unless it can be demonstrated that there is a "low" probability that the PHI has been compromised. While certain

exceptions apply to this rule, it is likely to increase the frequency with which potential breaches are reported.

> **CAUTION:** State law may also require notice of certain breaches of health-related information. Additionally, entities that are not considered Covered Entities or Business Associates subject to HIPAA (and this notice requirement), but who maintain personal health records for consumers, are subject to Federal Trade Commission rules requiring them to provide similar notices of breaches involving such personal health records.

Individual Rights and Obligations Related to the Use and Disclosure of PHI

Rights of Individuals to Access Their PHI in Electronic Format

If an individual requests an electronic copy of his or her PHI that is maintained electronically (whether or not in an electronic health record), the Covered Entity must provide the individual with access to the electronic information in the electronic format requested by the individual. If the requested format is not readily producible, the PHI can instead be provided in a readable electronic form as agreed to by the Covered Entity and the individual. Individuals making such a request may be charged for certain (but not all) labor costs and supplies for creating the electronic media (for example, the physical media, such as a CD or USB), if the individual requests that the electronic copy be provided on portable media. The interaction of these rules with permissible charges under state law must be considered.

Mandatory Compliance with Restrictions Requested on Certain Disclosures of PHI

Health care providers must comply with an individual's request for restrictions on the disclosure of his or her PHI if:

- The disclosure would otherwise be made to a health plan;
- The disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and
- The PHI pertains solely to a health care item or service for which the health care provider has been paid in full by the individual or person other than the health plan on the individual's behalf.

The Use of PHI in Fundraising and Marketing, and the Sale of PHI

The Final Regulations made significant changes to the rules regarding fundraising, marketing, and the sale of PHI.

The Final Regulations now permit the use of additional categories of PHI in the fundraising activities of Covered Entities. Specifically, Covered Entities may use department of service, treating physician and outcome information for their fundraising purposes. Fundraising communications (whether in person, over the phone, or written) must, however, provide individuals with clear and conspicuous instructions on how to opt out of receiving future fundraising solicitations. A Covered Entity's Notice of Privacy Practices must be reviewed to ensure that it includes a statement that an individual has a right to opt out of receiving fundraising communications.

Covered Entities and Business Associates are prohibited from using or disclosing PHI without authorization—even if for treatment and health care operations—where the Covered Entity (or Business Associate) receives direct or indirect payment for such use or disclosure. HIPAA's marketing restrictions have certain exceptions, including a communication made to provide refill reminders or otherwise communicate about current prescriptions where any financial remuneration received is reasonably related to the cost of making the communication.

Finally, the sale of PHI is prohibited unless an authorization is provided.

Using or Disclosing the "Minimum Necessary" PHI

With certain exceptions, Covered Entities and Business Associates must use "reasonable efforts" to

limit their uses or disclosures of, or requests for, PHI to the minimum amount that is necessary to accomplish the intended purpose. Under HITECH, a Covered Entity is automatically deemed to comply with the minimum necessary standard if it limits its use and disclosure of PHI to a "limited data set"—which is essentially de-identified information, except that dates relating to the individual (such as birth dates and dates of hospital admission and discharge) can be included. The Final Regulations provide no further guidance on this issue but promise it in the future.

Rights of Individuals to Get Enhanced Accounting of Disclosures of Electronic PHI

HITECH requires that Covered Entities that use or maintain an electronic health record will need to account for disclosures of electronic PHI for the purpose of treatment, payment, and health care operations. (Accountings for disclosures of non-electronic PHI do not need to include disclosures for treatment, payment, and health care operations.) Individuals will have the right to request an accounting of all such disclosures made in the three-year (rather than the otherwise applicable six-year) period prior to the accounting request. The Final Regulations did not address this requirement, which will not be effective until final regulations are issued on the accounting rules.

Significantly Enhanced HIPAA Enforcement Provisions

HITECH considerably increased the civil monetary penalties that may be assessed under HIPAA against Covered Entities and (now) Business Associates. Specifically, penalties for violations are determined with a tiered approach:

Violation Due to:	**Penalty Range (per Violation):**
Unknown cause	$100-$50,000
Reasonable cause and not willful neglect	$1,000-$50,000
Willfull neglect (violation corrected within 30 days)	$10,000-$50,000
Willful neglect (violation not corrected within 30 days)	At least $50,000

A $1.5 million annual cap applies for violations of an identical privacy or security requirement.

The Final Regulations revised the factors that can be considered in determining the penalty amount and amended the definition of reasonable cause. For purposes of assessing penalties, any act or omission that a Covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, violated the HIPAA privacy or security rules will be deemed to be a violation due to reasonable cause, provided the Business Associate did not act with willful neglect.

HITECH requires HHS to perform periodic audits of Covered Entities and Business Associates to ensure that they are complying with the HIPAA privacy and security rules. Under the Final Regulations, when a preliminary review of the facts in either a compliance review or a complaint investigation indicates a possible violation due to willful neglect, HHS must conduct a review to determine whether the Covered Entity or Business Associate is in compliance. HHS may conduct investigations in other circumstances in its discretion. Additionally, HHS is no longer required to resolve investigations or compliance reviews through informal means, meaning that in certain circumstances, HHS may assess penalties without negotiating with impacted Covered Entities and/or Business Associates.

Although not part of the Final Regulations, HITECH also gives state attorneys general the ability to bring civil actions on behalf of residents of their states, and clarifies that an individual who obtains or discloses PHI from a Covered Entity without authorization may be subject to criminal prosecution for a violation of HIPAA.

HIPAA Glossary

The world of HIPAA includes a vocabulary of its own. Key terms that may aid in your understanding include the following:

Business Associate

Generally, a person or entity that performs functions or activities on behalf of, or certain services for, a Covered Entity that involve the use or disclosure of PHI.

Examples include third party administrators, pharmacy benefit managers, claims processing or billing companies, and persons who perform legal, actuarial, accounting, management, or administrative services for Covered Entities and who require access to PHI. They also include certain information technology providers, health information organizations, most entities that provide data or document transmission and storage services with respect to PHI to a Covered Entity, and Subcontractors that create, receive, maintain, or transmit PHI on behalf of a Business Associate.

Business Associate Agreement

A contract between a Covered Entity and a Business Associate or between a Business Associate and a Subcontractor that governs each party's rights and obligations under HIPAA. Business Associate Agreements are required under the privacy rule.

Covered Entities

Health care providers that transmit health information in electronic form in connection with certain transactions; health plans (including employer-sponsored plans); and health care clearinghouses.

We specifically note that employers who sponsor self-insured group health plans will need to take the action items noted in this article on behalf of their health plans. For employers who sponsor fully-insured group health plans, the majority of these obligations will ordinarily fall on the insurance carrier.

Protected Health Information or PHI

Generally, "individually identifiable health information" that is transmitted or maintained in any form or medium, with limited exceptions. "Individually identifiable health information" includes demographic and health information that relates to an individual's health conditions, treatment or payment and can reasonably be used to identify the individual.

Subcontractor

Generally, a person to whom a Business Associate delegates a function, activity, or service. A Subcontractor becomes a Business Associate under HIPAA when it creates, receives, maintains or transmits PHI on behalf of the Business Associate when performing such delegated function, activity, or service.

Unsecured PHI

PHI that is not rendered unusable, unreadable, or indecipherable to an unauthorized person through encryption or destruction, pursuant to guidance published by HHS.

Click here to view the PDF version of this article.