

Reproduced with permission from Health Insurance Report, 19 HPPR 40, 03/06/2013. Copyright © 2013 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## The HIPAA Omnibus Final Rule—Data Privacy and Security Implications for Business Associates and Covered Entities



BY MATTHEW FISCHER

**O**n January 17, 2013, the Office for Civil Rights (“OCR”) of the U.S. Department of Health and Human Services (“HHS”) published the HIPAA Omnibus Final Rule (“Final Rule”) which OCR has trumpeted as carrying “the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented.”<sup>1</sup> The changes significantly impact the compliance obligations for covered entities, busi-

ness associates and their subcontractors, particularly with respect to their use and disclosure of protected health information (“PHI”).

The amendments to HIPAA<sup>2</sup> found in the Final Rule are extensive and address complex health care regulatory schemes. This article will focus on the substantial changes to the Privacy Rule<sup>3</sup> and Security Rule<sup>4</sup> (collectively referred to as the “Privacy and Security Rules”) as they affect covered entities and companies servicing the health care industry with respect to their data pri-

<sup>1</sup> January 17, 2013 News Release, U.S. Department of Health & Human Services, <http://www.hhs.gov/news/press/2013pres/01/20130117b.html>

*Matthew Fischer is a partner in the San Francisco office of Sedgwick LLP. His practice focuses on intellectual property and data privacy. He can be reached at [matthew.fischer@sedgwicklaw.com](mailto:matthew.fischer@sedgwicklaw.com).*

<sup>2</sup> References to HIPAA include the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act as incorporated in the American Recovery and Reinvestment Act of 2009 (HITECH).

<sup>3</sup> Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

<sup>4</sup> Standards for Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

vacancy, security and breach notification policies and procedures.

## Compliance Deadlines

Although it was published in the *Federal Register* on January 25, 2013, the Final Rule does not go into effect until March 26, 2013.<sup>5</sup> The deadline for covered entities and business associates to comply with the applicable provisions is September 23, 2013.

## Key Changes for Business Associates

**Expanded Definition.** The definition of a “business associate” has been broadened to encompass entities that create, receive, maintain or transmit PHI on behalf of a covered entity. Expressly included are: Health Information Organizations; e-prescribing Gateways; entities that offer personal health records to individuals on behalf of a covered entity and; entities that provide data transmission services with respect to PHI to a covered entity and that require access on a routine basis to such PHI.

---

**While the changes are intended to remove uncertainty that has pervaded for vendors servicing the health care industry, the Final Rule is not a model of clarity.**

---

While the changes are intended to remove uncertainty that has pervaded for vendors servicing the health care industry, the Final Rule is not a model of clarity. For example, HHS left the term “Health Information Organization” undefined, explaining that the type of entities that may be considered Health Information Organizations continues to evolve. HHS has indicated that it anticipates issuing guidance in the future on its web site on “the types of entities that do and do not fall within the definition of a business associate.”<sup>6</sup>

The comments to the Final Rule explain that data storage providers that maintain PHI constitute business associates regardless of how frequently they view or access the data. While the Final Rule confirms that the previously existing “conduit exception” remains, it clarifies that this narrow exception only applies to those entities that provide mere courier services, such as the U.S. Post Office or an internet service provider that only transmits the data.

---

<sup>5</sup> 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, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. Parts 160 and 164).

<sup>6</sup> 78 Fed. Reg. 5571.

---

**HHS noted in the comments that an entity that maintains PHI on behalf of a covered entity is a business associate and not a conduit, “even if the entity does not actually view the [PHI].”**

---

HHS noted in the comments that an entity that maintains PHI on behalf of a covered entity is a business associate and not a conduit, “even if the entity does not actually view the [PHI].” The distinction between the transitory nature of a transmission service versus an entity that has the ability to regularly access PHI is underscored by the Final Rule’s modification of the definition of a business associate to add entities that “maintain” PHI on behalf of covered entities. This change eliminates prior ambiguity as to whether certain cloud service providers and data storage centers are considered business associates.

**Subcontractors.** The Final Rule expands the definition of business associate to include any subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate. Under the Final Rule a subcontractor is defined as “a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.”<sup>7</sup> Such downstream contractors must now comply with applicable HIPAA Privacy and Security Rules to the same extent as business associates and this obligation continues down the chain so that a vendor that creates, receives, maintains or transmits the PHI on behalf of the subcontractor will be required to enter into a business associate agreement with that subcontractor, and so on.

This extension to subcontractors is effectuated through the requirement that business associates must attain assurances from their subcontractors that they will maintain adequate administrative, physical and technical safeguards to protect PHI, which is no different than the provision requiring covered entities to obtain the same assurances from business associates through a business associate agreement. Likewise, if a business associate learns that its subcontractor has not implemented satisfactory safeguards resulting in a data breach, it must respond in the same manner (i.e., making a reasonable effort to ensure the breach is cured and any harm has been mitigated) as a covered entity that learns of noncompliance by its business associate.

The inclusion of subcontractors within the definition of business associates carries significant consequences for those companies that service health care organizations, particularly those companies that service the health care industry indirectly and have limited understanding of the substantial operational obligations associated with HIPAA’s Privacy and Security Rules.

Many companies will not be on notice that they are subject to the Privacy and Security Rules unless they are compelled to enter into a business associate agreement. Even then, however, they may not realize the specific types of administrative, physical and technical

---

<sup>7</sup> 78 Fed. Reg. 5573.

safeguards that they must have in place to protect PHI unless they consult with an attorney that specializes in data privacy and/or health care law. Those subcontractors that create, receive, maintain or disclose PHI but are not required to sign a business associate agreement are still subject to HIPAA regulations.

While a business associate agreement creates contractual liability between the business associate and a subcontractor, the business associate and the subcontractor are now directly liable to HHS, regardless of whether they ever entered into a business associate agreement. Subcontractors that do not function primarily in the health care space—such as cloud providers and data storage facilities—may not even be aware that they are maintaining or transmitting PHI.

As discussed below, the Final Rule significantly increases the security and privacy measures for business associates and, in turn, for their subcontractors. Certain companies will not have the operational capabilities, nor the financial resources, to meet the business associate obligations. While the Security Rule maintains its pre-existing concepts of flexibility, scalability and technology neutrality which allows business associates and subcontractors to implement security measures that correlate to their size and capabilities, certain aspects of the regulations are mandatory.

---

**Some companies would have to perform a major overhaul of their security and network infrastructures and others may not be able to offer sufficient assurances of compliance to covered entities and business associates in order to work in the health care industry.**

---

For example, companies must be able to track and account for disclosures of PHI, provide a report of attempts to access their information systems, even if unsuccessful, and provide access to specific medical records. Some companies would have to perform a major overhaul of their security and network infrastructures and others may not be able to offer sufficient assurances of compliance to covered entities and business associates in order to work in the health care industry. HHS has stated that it will offer guidance in the future on its website as to “the types of entities that do and do not fall within the definition of a business associate.”

**Expanded Liability.** One of the more noteworthy changes under the Final Rule is that business associates are now directly liable for the failure of their subcontractors to comply with HIPAA Privacy and Security Rules.

The preamble to the Final Rule sets forth two circumstances wherein a business associate assumes liability under the federal common law of agency for the acts and omissions of its subcontractors. The first scenario is when they “delegate out” obligations under HIPAA to a subcontractor. The second is when the business associate retains authority regarding a specific duty, usually pursuant to the terms of a business associate agreement

between the business associate and the covered entity. Whether agency liability applies is a fact specific inquiry in which HHS determines the totality of the circumstances involved in the ongoing relationship between the parties. In short, HHS has made it clear that there is now little difference between business associates and covered entities for liability purposes, regardless of how far downstream PHI travels.

Covered entities are still ultimately accountable for notifying individuals whose PHI has been breached, although they can assign this responsibility to a business associate under a business associate agreement. Nonetheless, if a business associate fails to meet its contractual obligation to notify individuals of a breach, the covered entity will still be liable for such failure.

**Direct Liability of Business Associates for Privacy Rule Violations.** While business associates were required to comply with most of the requirements of the Privacy Rule pursuant to contractual obligations set forth in the business associate agreements, the HITECH Act did not create direct liability for their compliance under the Interim Rule. Under the Final Rule, business associates are directly liable for the following:

- Impermissible uses and disclosures of PHI;
- Failure to enter into a business associate agreement with subcontractors;
- Failure to provide breach notification to the covered entity;
- Failure to provide access to a copy of electronic PHI to either the covered entity, an individual or the individual’s designee;
- Failure to disclose PHI when required by HHS to determine the business associate’s compliance with HIPAA;
- Failure to provide an accounting of disclosures; and
- Failure to comply with the Security Rule requirements.

The Final Rule also applies the “minimum necessary” standard directly to business associates who use, disclose or request PHI from a covered entity or another business associate. As a result, covered entities and business associates disclosing PHI in response to a request from a business associate can therefore reasonably assume that such requests are asking for the minimum necessary for the disclosure. How a business associate applies the minimum necessary standard will vary according to the circumstances, but it must be consistent with the covered entity’s minimum necessary policies and procedures. The Final Rule leaves it to the discretion of the parties to a business associate agreement to determine the extent to which the contract will identify specific minimum necessary provisions to ensure the business associate or subcontractor maintains the required consistency.

**Direct Liability of Business Associates for Privacy Rule Violations.** Business associates and subcontractors are directly responsible for compliance with the Security Rule requirement that they implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of all electronic PHI. The Final Rule maintains the flexibility contained in the Interim Rule with respect to the implemen-

tation of security specifications so that business associates and subcontractors are able to adopt security measures that are proportional to their size, complexity and financial and technical capabilities.

**Enforcement.** Business associates are subject to sizeable civil monetary penalties under the Final Rule, which retains the tiered range of penalties based on increasing levels of culpability found in the Interim Rule (did not know, reasonable cause, willful neglect – corrected, and willful neglect – not corrected), but modified the state of mind requirement for the second tier, reasonable cause.

The new definition of “reasonable cause” covers violations that were caused by (1) circumstances that would make it unreasonable for the covered entity to comply with the violated HIPAA regulation (which existed under the Interim Rule) and (2) where an entity is aware of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations.

The Final Rule clarifies that OCR must investigate any complaint if a preliminary review of the facts indicates a possible (rather than the higher “probable” threshold that was considered) violation due to willful neglect.

### **Breach Notification Rule Revision**

HHS changed the definition of a “breach” so that an impermissible use or disclosure of PHI is now presumed to be a breach unless the covered entity or business associate is able to demonstrate that a low probability exists that the PHI has been compromised based on a risk assessment, or one of the other exceptions to the definition of “breach” applies.

---

**HHS changed the definition of a “breach” so that an impermissible use or disclosure of PHI is now presumed to be a breach unless the covered entity or business associate is able to demonstrate that a low probability exists that the PHI has been compromised based on a risk assessment, or one of the other exceptions to the definition of “breach” applies.**

---

Under the Interim Rule, a “breach” consisted of the “acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the [PHI]”, which was further defined as a “significant risk of financial, reputational, or other harm to the individual.” HHS changed the definition out of concern that the former “risk of harm” standard was too subjective and could be misconstrued and interpreted in a way that HHS had not intended. The more objective standard under the revised definition creates an automatic presumption that a breach occurred and will therefore likely result in more notifications.

Rather than weighing the risk of harm to an individual, the covered entity or business associate must, at a minimum, undertake a risk assessment of the following four objective factors to determine whether there is a “low probability” that the PHI has been compromised:

- *The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification of the information.* Entities should consider whether the PHI involved in the impermissible use or disclosure is of a sensitive nature. For financial information, this would include credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, it may include an analysis of the types of services and information involved, as well as the amount of detailed clinical information disclosed (e.g., treatment plan, diagnosis, medication, medical history information, test results).

- *The unauthorized person who used the PHI or to whom the impermissible disclosure was made.* An important consideration would be whether the unauthorized person who received the PHI is obligated to protect its privacy and security. Under both the Interim Rule and Final Rule, PHI impermissibly disclosed to another entity obligated to abide by the Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 is not PHI and thus not considered a breach.

- *Whether the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.* For example, if a forensic analysis shows that PHI stored in a stolen laptop that was later acquired was never accessed, viewed, acquired, transferred, or otherwise compromised, then it would be reasonable for an entity to conclude that the PHI was not actually acquired by an unauthorized individual even though the opportunity existed

- *The extent to which the risk to the PHI has been mitigated.* Covered entities and business associates should attempt to mitigate the risks to the PHI following any impermissible use or disclosure. Mitigation may be achieved by obtaining satisfactory assurances from the recipient of the PHI that it will not be further used or disclosed (e.g., through a confidentiality agreement) or will be destroyed. The extent and efficacy of the mitigation should be considered when determining the probability that the PHI has been compromised.

While the Final Rule outlines the above four factors to be considered in determining whether a breach has occurred, it does not provide a definition for the terms “compromise” or “low probability” nor provide any further criteria for undertaking such an analysis. HHS stated that it plans to promulgate guidelines on the risk assessment factors associated with data breaches, but there is no certainty that such guidance will be made available before the September 23, 2013 compliance deadline.

Another change to the breach notification rules worth noting is the elimination of the exception for limited data sets that do not contain birth dates and ZIP

codes.<sup>8</sup> Accordingly, the impermissible use or disclosure of *any* limited data set now requires a covered entity or business associate to either notify affected individuals or conduct an objective risk assessment based on the above four factors to determine if notification is necessary.

## Increased Individual Rights Regarding Access to and Restrictions on Disclosure of PHI

The Final Rule grants individuals increased access to their electronic PHI while also enhancing their ability to restrict disclosure of their PHI. Covered entities will need to modify their Notice of Privacy Practices to reflect these new individual rights.

**Increased Access.** Individuals have had the right under the Interim Rule to obtain an electronic copy of PHI contained in an electronic health record used or maintained by a covered entity. The Final Rule expands this right to requests for PHI contained in designated record sets and the covered entity must provide the individual access to the PHI in the electronic form and format requested, so long as it is readily producible in that form and format, and if it is not, in a form and format agreed to by the covered entity and the individual. If the individual refuses a copy of the PHI in electronic format, then the covered entity must provide the information in hard copy.

If the individual makes a signed, written request for a covered entity to transmit a copy of the individual's PHI to another person clearly designated by the individual, then the covered entity must do so. Covered entities will likely need to modify their applicable documents and procedures for transmissions to third parties in order to adhere to these new specifications.

---

**A covered entity now has 30 days to provide access to, or a copy of, requested PHI, with a 30-day extension available if the covered entity alerts the individual within the original 30 day timeframe.**

---

The Final Rule also eliminates the 60-day deadline for covered entities to respond to an individual's request to access or receive a copy of PHI. A covered entity now has 30 days to provide access to, or a copy of, requested PHI, with a 30-day extension available if the covered entity alerts the individual within the original 30 day timeframe.

**Restrictions on Disclosure of PHI.** The Interim Rule currently requires a covered entity to comply with an individual's request to restrict uses or disclosures of the

---

<sup>8</sup> A "limited data set" is defined under the Privacy Rule as PHI that excludes certain direct identifiers of the individual or of relatives, employers or household members of the individual, including but not limited to, names, telephone numbers, social security numbers, postal and email addresses, medical record numbers, photos, etc. 45 C.F.R. Part 164.514(e).

individual's PHI for purposes of treatment, payment or health care operations (provided it is not otherwise required by law) and the PHI pertains solely to a health care item or service for which the individual, or a person on the individual's behalf, has paid in full. The Final Rule clarifies that this requirement only applies to requests to restrict disclosure of PHI to a health plan. Covered entities must therefore implement procedures to ensure that the health plan is not mistakenly given access to restricted PHI for payment or health care operations purposes.

## Notice of Privacy Practices

The Privacy Rule requires most covered entities to prepare and disseminate a Notice of Privacy Practices ("NPP") that summarizes the entity's permitted uses and disclosures of PHI, privacy practices and legal obligations and delineates individual's rights regarding their PHI. The Final Rule modifies the content requirements of NPP so that they must include the following additional statements:

- other uses and disclosures not described in the NPP will be made only with the individual's written authorization, which may be revoked;
- the sale of PHI and the use of such information for paid marketing require authorization from the individual;
- covered entities must notify affected individuals of breaches of unsecured PHI;
- individuals can restrict disclosures to their health plan for services for which they pay out of pocket in full;
- if the covered entity engages in fundraising activities, it may contact individuals to raise funds, but they have the right to opt-out of receiving such communications;
- health plans that engage in underwriting activities are prohibited from using or disclosing PHI that is genetic information for such purposes;
- individuals have the right to request a restriction of disclosures of PHI, but covered entities are not required to agree to such a request.

The Final Rule states that the necessary revisions to NPPs to include the above statements constitute "material changes," which in turn trigger distribution requirements for health plans. Those that post their NPPs on their website must prominently post a notice of the material changes or a copy of the revised NPP on their website by the effective date of the change and provide either information about the changes or a copy of the revised NPP in their next annual mailing to individuals. Health plans that do not post their NPPs on their websites must provide a copy of the revised NPP, or information about the changes and how to request a copy of the NPP, within 60 days of the change.

## Additional Changes Pertinent to Covered Entities

Some of the other significant changes encompassed in the Final Rule that impact covered entities but do not specifically target the Privacy and Security Rules include:

- A prohibition against health plans using or disclosing genetic information for underwriting purposes.
- A prohibition against the sale of PHI without an individual's authorization confirming whether the PHI can be further exchanged for payment by the entity receiving the information.
- A requirement for authorization for all treatment and health care operations communications in which the covered entity receives direct or indirect payment for transmitting the communication from a third party whose product or service is being marketed.
- An expanded range of PHI that a covered entity may use or disclose for fundraising and the requirement that covered entities provide individuals the ability to opt-out of fundraising communications.
- The ability of covered entities to combine conditioned and unconditioned authorizations for research, so long as the authorization "clearly differentiates" between the conditioned and unconditioned research components and provides an opt-in mechanism in connection with the unconditioned research activities.

### **Considerations for Compliance with the Final Rule Modifications**

The numerous substantive changes to the HIPAA regulations encompassed within the Final Rule merit close attention from covered entities and companies providing services to the health care industry, which would be well advised to verify how, if at all, specific changes apply to them and to start taking immediate action to ensure compliance by September 23, 2013.

Covered entities will want to revise their NPPs to include the various statements now required and decide the means by which they will notify individuals of the "material changes" to the NPPs. They will also want to evaluate, and revise as necessary, their policies, procedures and any existing agreements or contract terms regarding a number of content changes, including, but not limited to: breach notification; the sale of PHI; the use and disclosure of PHI for paid marketing; requests of individuals who pay in full for health care services to restrict disclosures of PHI to health plans; individuals' requests for access to or copies of electronic PHI and;

requests to provide PHI to third parties. Additionally, covered entities will want to review and amend their business associate agreements to bring them in line with the expanded obligations for business associates and their subcontractors.

Business associates should review and update their HIPAA Privacy and Security Rule policies and procedures, particularly the HIPAA regulations that now apply to business associates. To that end, they should make sure they have implemented sufficient administrative, physical and technical safeguards to protect PHI in proportion to their size and complexity. They should also modify breach notification policies and procedures to address the altered definition of a breach and the new objective risk assessment standard for determining whether a breach occurred.

As is the case with most covered entities, business associates should have cyber insurance and have identified in advance a computer forensic company that can assist in determining whether a data breach has occurred and, if so, help mitigate the harm. Business associate agreement templates for both covered entities and subcontractors should be revised to include new applicable provisions under the Final Rule and existing business associate agreements should be amended to include the new Final Rule provisions if necessary.

Companies that service others in the health care industry but are unsure if they themselves fit within the definition of a business associate or subcontractor should consult an attorney to determine their status and, if they do, whether they fall within an established exception, such as the conduit exception. If an entity determines that it is either a business associate or subcontractor, then it should undertake the above-referenced steps to advance toward HIPAA compliance.

If companies have any doubt about the need to take prompt action to comply with the Final Rules, they need only look to OCR's increasing enforcement efforts and HIPAA compliance audits over the past few years. Companies operating in the health care sphere can expect continued investigations, enforcement measures and audits from OCR in 2013, with the potential for substantial monetary penalties and settlements for those who do not meet applicable HIPAA Privacy and Security Rule requirements.