Proskauer

HHS Issues HIPAA/HITECH Omnibus Final Rule Ushering in Significant Changes to Existing Regulations

January 29, 2013

"***Sweeping changes***" is how Leon Rodriquez, of the Department of Health and Human Services Office of Civil Rights (OCR), characterized the effect of the final omnibus Health Insurance Portability and Accountability Act (HIPAA) rule published in the Federal Register on January 25, 2013 at 78 Fed. Reg. 5566 (Omnibus Rule). There can be no disputing that statement. Indeed the 563-page Omnibus Rule makes a long list of significant changes to existing regulations. These include, among others:

- modification to the standard for reporting breaches of unsecured personal health information (PHI);
- extension of HHS enforcement authority over business associates;
- expansion of the definition of the term business associate to include Health Information Organizations, E-prescribing Gateways, entities that provide data transmission services for PHI and which require routine access to such PHI, and personal health record vendors;
- modifications to the requirements for business associate agreements;
- new obligations for business associates to enter into business associate agreements with their own subcontractors;
- the removal of limitations on the liability of covered entities for the acts and omissions of business associates;
- changes to the requirements for notices of privacy practices;

- new limitations on the sale of PHI;
- new limitations on and clarifications concerning the use and disclosure of PHI for marketing;
- relaxation of certain limitations on the use of PHI for fundraising; and
- improvement to the regulations concerning authorizations for the use or disclosure of PHI for research.

Except as noted below with respect to provisions related to the requirements for business associate agreements and arrangements relating to the sale of PHI, the deadline for complying with the amended HIPAA regulations is September 23, 2013. Accordingly, covered entities, business associates, and business associate subcontractors will have to act expeditiously to come into compliance with the Omnibus Rule.

Below, we review the changes implemented in the Omnibus Rule in greater detail, and address some of the action steps that covered entities and business associates should take to comply.

Provisions of the Omnibus Rule

1. Tougher Breach Reporting Standard Adopted

Section 13402 of the HITECH Act requires covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. HITECH requires the Secretary to post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals. The Omnibus Rule substantially alters the definition of breach. Under the August 24, 2009 interim final breach notification rule, breach was defined as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information." The phrase "compromises the security or privacy of [PHI]" was defined as "pos[ing] a significant risk of financial, reputational, or other harm to the individual."

According to HHS, "some persons may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than we intended to set. As a result we have clarified our position that breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised. . . ." To demonstrate that there is a low probability that PHI has been compromised, a covered entity or business associate must perform a risk assessment that addresses, at a minimum, the following factors:

(i) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) the unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) whether the protected health information was actually acquired or viewed; and

(iv) the extent to which the risk to the protected health information has been mitigated.

While these factors are similar to those recommended by HHS in the preamble to the interim final rule for use in assessing the risk of harm, HHS contends that the former "risk of harm" standard resulted in an analysis that was too subjective. Accordingly, HHS indicates that under the Omnibus Rule, the risk assessment analysis should be an objective test focusing on whether PHI has been "compromised." Nevertheless, other than listing the risk assessment factors, the Omnibus Rule does not define the term "compromise" or explain what it means for PHI to be compromised. HHS did note in the preamble, however, that it will issue additional guidance "to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios."

2. Expansion of HHS Enforcement Authority over Business Associates and Related Changes to Requirements for Business Associate Agreements

As expressly required by HITECH, the Omnibus Rule amends 45 C.F.R. § 164.104 to make certain HIPAA privacy and security rules directly applicable to business associates, but only where those rules so provide. The rules that are made applicable to business associates under this provision are: 45 C.F.R. § 164.306 pertaining to security standards, 45 C.F.R. § 164.308 pertaining to administrative safeguards, 45 C.F.R. § 164.310 pertaining to physical safeguards, 45 C.F.R. § 164.312 pertaining to technical safeguards, 45 C.F.R. § 164.316 pertaining to policies and procedures, 45 C.F.R. § 164.502 pertaining to disclosures of PHI, and 45 C.F.R. § 164.504 pertaining to organizational requirements.

The Omnibus Rule also requires business associates to agree in business associate agreements to comply with the requirements imposed on them under HIPAA. In addition, under the Omnibus Rule, business associate agreements now must require business associates to enter into business associate agreements with subcontractors who will receive, create, or transmit PHI on their behalf. HHS has released a new model form business associate agreement that includes revisions pursuant to the requirements of the Omnibus Rule. The model form is available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Notably, the Omnibus Rule provides that business associate agreements that were effective prior to January 25, 2013 are deemed compliant with the preexisting regulations until September 22, 2014, unless they are amended within one year before that date.

3. Expansion of Definition of Business Associate

The Omnibus Rule broadens the definition of business associate to include, in addition to those entities that would qualify as business associates under the preexisting regulations, the following entities: (1) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity. As a result, these entities will be subject to the requirements imposed on business associates under HIPAA including various requirements under the Security Rule, and the new requirement to enter into business associate agreements with subcontractors. They also will be subject to direct enforcement action by HHS. HHS, however, has declined to define the term "Health Information Organization," noting 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."

With respect to what it means to require access to PHI on a "routine basis," HHS distinguishes entities that require access to PHI on a "routine basis" from entities that serve as "mere conduits." HHS cautions, however, that the "mere conduit" exception is intended to be narrow and to apply only to courier services such as the Postal Service "and their electronic equivalents, such as Internet service providers (ISPs) providing mere data transmission services." HHS also notes 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]."

4. New Requirements Related to Business Associate Subcontractors

According to the Omnibus Rule, a subcontractor is "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." The Omnibus Rule provides that there must be an agreement between the business associate and its subcontractor that provides that the subcontractor is subject to the same HIPAA requirements for access and use of PHI as the business associate. In effect, the Omnibus Rule places the subcontractors of business associates in the same position that business associates were in before HITECH made business associates directly subject to certain HIPAA requirements. Specifically, business associates' subcontractors now will be contractually obligated to comply with certain HIPAA requirements, but not directly subject to HHS enforcement authority.

5. Expanded Liability of Covered Entities and Business Associates for Acts of Their Agents

Prior to the promulgation of the Omnibus Rule, 45 C.F.R. § 160.402 established civil monetary penalty liability for covered entities under HIPAA based on the acts and omissions of their agents, including workforce members, but exempted covered entities from liability for the acts of their business associates if the following conditions were met: (1) the relevant business associate agreement requirements; (2) the covered entity did not know of a pattern or practice of the business associate in violation of the business associate agreement; and (3) the covered entity did not fail to act as required by the HIPAA Privacy or Security Rule with respect to such violations. The Omnibus Rule now provides that covered entities will be liable under the "federal common law of agency" for the acts and omissions of their business associates, and eliminates the exception to such liability that was included previously in 45 C.F.R. § 160.402. The Omnibus Rule also provides that like covered entities, business associates may be held liable under the "federal common law of agency" for the acts and omissions of their subcontractors.

The preamble to the Omnibus Rule discusses two contexts in which covered entities and business associates may be held liable for the acts of their agents: (1) when they "delegate out" obligations under HIPAA to another party; and (2) when they retain authority to give interim instructions concerning a particular task, such as where a business associate agreement provides that the business associate must make available PHI based on instructions to be provided by the covered entity. Imposing agency liability in both these contexts would appear to leave little ground uncovered, as it indicates that covered entities and business associates may be liable for the acts of third parties both when they retain control of the performance of a certain task, and when they do not. The preamble, however, does provide a number of examples of situations where a covered entity or business associate will not be subject to agency liability. These include a business associate hired by a small health care provider to perform de-identification. The preamble explains that such an arrangement should not give rise to agency liability because the provider would be unable to provide guidance to the business associate. HHS cites a business associate who performs credentialing for a covered entity where the covered entity lacks the authority to award accreditation as another example of an arrangement that would not give rise to agency liability. The common thread in these two examples appears to be the lack of ability for the business associate to control or direct the performance of its agent.

In sum, the elimination of a bar to liability for the acts of business associates represents a significant expansion of HHS's enforcement authority. Covered entities and business associates will have to consider carefully how decisions to delegate responsibility for tasks such as handling breach notification and their retention of authority to provide instructions to their business associates and contractors with respect to certain tasks will affect their exposure to liability.

6. New Requirements for Notices of Privacy Practices

Notices of Privacy Practices (NPPs) for all covered entities now must include the following information: (1) that the sale of protected health information and the use of such information for paid marketing require authorization from the individual; (2) that other uses and disclosures not described in the NPP will be made only with authorization; (3) that covered entities must notify affected individuals of breaches of their PHI; and (4) that individuals can restrict disclosures to their health plan for services for which they pay "out of pocket."

In addition, NPPs for health plans that underwrite (excluding certain long-term care plans) must state that the plan cannot use or disclose genetic information for underwriting purposes. NPPs for covered entities that intend to contact individuals for fundraising also must note that individuals have a right to opt out of receiving fundraising communications from the covered entity. Finally, entities that maintain psychotherapy notes must note in their NPPs that most uses and disclosures of such notes require authorization.

The Omnibus Rule also eliminates one existing requirement relating to NPPs: whereas NPPs previously had to state that the covered entity may contact individuals to provide appointment reminders or information about treatment alternatives or other health-related benefits, such a statement is no longer required. It is worth noting, though, that authorization will generally be required for the use or disclosure of PHI for marketing activities that are supported by payments from third parties.

The Omnibus Rule also includes important provisions concerning requirements for distributing revised NPPs. Specifically, the Omnibus Rule provides that health plans that post their NPPs on their Web sites must post material changes on their Web sites by the effective date of the change, and provide information about the change in their next mailing to covered individuals. Plans that do not post their NPPs on their Web sites must provide information about any material change to their NPP to covered individuals within 60 days of the material revision to the NPP. These provisions are intended to enable health plans to avoid the cost of having to make a separate mailing of their revised NPPs, which would have been required under preexisting regulations.

Health care providers are not required to mail out revised NPPs. But health care providers must post the revised notice on their Web sites if they maintain one, post the revised notice in a clear and prominent location in their facility if they maintain a physical service delivery site; and make the revised notice available to patients upon request after the effective date of the revision.

7. Limitations on the Sale of PHI

The sale of PHI without authorization is prohibited under the Omnibus Rule. The "sale of [PHI]," however, is defined to exclude disclosures for public health purposes, for treatment and payment for health care, for the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence, to a business associate in connection with the business associate's performance of activities for the covered entity, to a patient or beneficiary upon request, and as required by law. In addition, the disclosure of PHI for research purposes or for any other purpose permitted by HIPAA will not be considered a "sale" if the only remuneration received by the covered entity or business associate is "a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law." Notably, under the Omnibus Rule, an authorization to sell PHI must state that the disclosure will result in remuneration to the covered entity. Notwithstanding the changes in the Omnibus Rule, the disclosure of limited data sets (a form of PHI with a number of identifiers removed in accordance with specific HIPAA requirements) for remuneration pursuant to existing agreements is permissible until September 22, 2014, so long as the agreement is not modified within one year before that date.

8. Limitation on the Use of PHI for Paid Marketing

Under preexisting regulations, covered entities are required to obtain authorization to use or disclose PHI for marketing purposes, but not for activities that constitute treatment or health care operations. Marketing is defined as "a communication about a product or service that encourages recipients . . . to purchase or use the product or service." However, prior to the implementation of the Omnibus Rule, no prior authorization was required to make communications related to treatment and health care operations. The practical effect was that covered entities could use PHI to conduct marketing for a variety of purposes, such as recommending alternative therapies, without obtaining authorization from the patient or beneficiary.

The Omnibus Rule limits the ability of covered entities to make such communications. Specifically, under the Omnibus Rule, covered entities must obtain authorization to use PHI to make any treatment and health care operations communications if they receive financial remuneration for making the communication from a third party whose product or service is being promoted. HHS notes that the authorization requirement applies even when a business associate will receive the remuneration for making a communication, and the covered entity will not receive direct remuneration.

There are several important limitations to this requirement. First, "refill reminders" are excluded, so long as the remuneration for making such a communication is "reasonably related to the covered entity's cost" for making the communication. The preamble notes that permissible costs that can be reimbursed do not include indirect costs, and are limited to labor, supplies, and postage. The preamble also notes that communications about generic equivalents and adherence communications reminding patients to take medication as directed are both considered to be "refill reminders." Additionally, for self-administered drugs and biologics, communications about all aspects of the delivery system (such as a communication about an insulin pump) are considered to be "refill reminders" as well.

Second, face-to-face marketing communications are not subject to the authorization requirement. Permissible face-to-face communications can include handing someone written material such as a pamphlet.

Third, promotional gifts of nominal value are not subject to the authorization requirement.

Additionally, for purposes of determining whether authorization is required to use PHI to make a paid marketing communication, financial remuneration does not include nonfinancial benefits such as in-kind payments, and payments for a purpose other than making a communication, such as payments to implement a disease management program.

HHS also notes in the preamble that authorizations from patients and beneficiaries need not be limited to a single product or service or the products or services of a single entity, but can allow subsidized communications more generally.

9. Relaxation of Restrictions on the Use of PHI for Fundraising

The Omnibus Rule expands the type of information that can be used for fundraising without patient authorization to include the department of service information, the identity of the treating physician, and health insurance status. But providers should note the requirement to describe disclosures that may be made for fundraising in their NPP. In addition, the new rule heightens the requirement for including an opportunity for patients to opt out of receiving future fundraising communications in any such notice. Covered entities also are prohibited from conditioning treatment on any decision with respect to the receipt of fundraising information.

10. Improvements to Requirements for Authorizations Related to Research

The Omnibus Rule includes two noteworthy changes concerning authorizations for the use or disclosure of PHI for research. First, the preamble notes that HHS has changed its position with respect to authorizations for the use of PHI for future research. Previously HHS had taken the position that such authorizations were not valid. HHS now states, however, that such authorizations will be considered valid if they adequately describe future uses. Second, the provisions of the privacy regulations relating to the use of compound authorizations for research have been amended to clarify that when a compound authorization is used, and the provision of research-related treatment is conditioned on the provision of an authorization, the compound authorization must differentiate between conditioned and unconditioned components.

11. Additional Modifications to HIPAA Regulations

The Omnibus Rule includes a number of additional noteworthy changes. Although they are of somewhat lesser import than those highlighted above, they are not inconsequential. They include:

- a provision requiring covered entities to agree, upon request, to restrict disclosures to health plans of PHI when the PHI pertains to items or services for which an individual has paid "out of pocket." As a result, covered entities will have to implement procedures for complying with such requests;

- a requirement for covered entities to provide access to PHI in electronic format upon request if they maintain information in designated record sets electronically;

- a requirement for covered entities to comply with requests by individuals to transmit copies of PHI to third persons when such requests are made in writing;

- a provision allowing covered entities to disclose PHI to family members of a deceased patient who were involved with the patient's care or payment for their care, so long as such disclosure is not contrary to "any prior expressed preference of the individual that is known to the covered entity,"

- establishment of a 50-year limit on the obligation to protect the PHI of deceased individuals;

- a provision allowing covered entities to disclose immunization records to a school if the school is required by law to obtain such records prior to admission and the covered entity obtains and documents the agreement to the disclosure from the parent or individual as applicable; and

- a provision implementing requirements of the Genetic Information Nondiscrimination Act of 2008 (GINA) by prohibiting the use of genetic information for underwriting purposes, such as eligibility determinations and the computation of premiums.

Action Items for Covered Entities and Business Associates

In light of the many significant changes to the HIPAA regulations, covered entities and those who provide services to covered entities as business associates will have to take prompt action to comply. Specifically, covered entities will have to:

- revise their NPPs;

- review and, as necessary, revise their policies and procedures concerning: (1) breach notification; (2) the sale of PHI; (3) the use of PHI for paid marketing activities; (4) the use of PHI for fundraising; (5) requests to restrict disclosure of PHI to health plans from individuals who pay "out of pocket" for services; (6) requests for access to PHI in electronic format; (7) requests to transmit copies of PHI to third persons; (8) disclosure of the PHI of deceased patients to family members; (9) disclosure of immunization records; and (10) authorizations for research;

- develop new forms for business associate agreements;

- review any agreements pertaining to the sale of PHI or the use of PHI for marketing to assess the impact of the new regulations on such agreements; and

- as necessary, develop authorizations for the sale of PHI and the use and disclosure of PHI for paid marketing.

In addition, changes in the regulations with respect to liability for the acts and omissions of business associates should prompt covered entities and business associates to review their current business associate agreements and to consider how they will approach future business associate agreements. For example, covered entities that have delegated responsibility to a business associate for making determinations with respect to, and providing, breach notifications may wish to amend their agreement or to retain those duties in future agreements. Similarly, even where a covered entity has not expressly delegated responsibility to a business associate for making breach determinations, covered entities also should review language in current and future business associate agreements relating to breach notifications carefully. Often, such agreements require business associates to provide notice concerning a breach of unsecured PHI. Such a provision, however, can be construed as providing the business associate with the authority to not inform covered entities of potential breaches on the basis that there has been no "breach." Covered entities may wish to seek language that more clearly delineates the parties' rights and obligations in this area. Finally, both covered entities and business associates should now consider seeking indemnification in their business associate agreements.

Business associates, including Health Information Organizations, E-prescribing Gateways, entities that provide data transmission services for PHI and require routine access to such PHI, and personal health record vendors will have additional work to do as well, including:

- drafting and adopting policies, procedures and related documents if they do not have them in place already;

- performing and documenting risk assessments if they have not done so; and

- reviewing their relationships with subcontractors and entering into business associate agreements with them as necessary.

In short, there is much work for covered entities and business associates to do, and, in large part, that work will have to be completed by September 23, 2013.

Related Professionals

- **Edward S. Kornreich**