New HIPAA/HITECH act omnibus rule: What must be done to comply?

February 28, 2013

From international law firm Arnold & Porter LLP comes timely views on current regulatory and legislative topics that weigh on the minds of today's physicians and health care executives.

See Also

BLOG: Obama administration releases new Affordable Care ...

HHS proposes new guidelines for Medicaid, CHIP, health ...

BLOG: New reviews related to physician services in OIG's ...

Health care professionals and others working with personal medical information face considerable compliance risks and responsibilities under the omnibus final rule governing "protected health information" (PHI) that the Department of Health and Human Services issued in January 2013 (the Final Rule). The Final Rule sets standards and authorizes substantially increased penalties for violations of HHS' regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act. Particularly in light of those increased penalties, HIPAA covered entities (health plans, health care clearinghouses, and most health care providers) and their "business associates" — which are now directly subject to HHS regulations — should be actively reviewing their new responsibilities under the Final Rule.

Among the most significant aspects of the Final Rule are provisions that:

- Make subcontractors (and sub-subcontractors, sub-sub-subcontractors, etc.) of HIPAA business associates themselves "business associates" and thus directly subject to most provisions of the HIPAA Privacy Rule, as well as the HIPAA Security Rule and HHS' Breach Notification Rule;
- Eliminate the "risk of harm" standard that HHS previously prescribed as a criterion for determining when it is necessary to notify individuals about a breach of security affecting their PHI; and
- Require amendments to Notices of Privacy Practices, business associate agreements, and a variety of policies and procedures entailed in complying with the Privacy Rule.

With limited exceptions, compliance with the Final Rule's provisions is required by September 23, 2013.

Covered entities: What steps are needed?

1. Revisions to privacy policies

Each covered entity should revise its internal privacy policy to reflect the new requirements of the Final Rule, including, but limited to, provisions that:

- *Prohibit the sale of PHI* without an individual authorization (with limited exceptions) — noting that a "sale" of PHI includes any disclosure of PHI in exchange for remuneration, even if the ownership of the PHI remains with the "seller";

- *Prohibit using PHI without an authorization to make certain types of communications newly deemed to constitute "marketing" under the Final Rule* if payment is received from a third party whose product or service is promoted in the communication (with narrow exceptions such as for refill reminders where the payment is limited to the cost of making the communication);
- *Prohibit using PHI without an authorization to make fundraising communications*, unless each communication provides a means for the recipient to opt out of receiving any further such communications and the opt-out mechanism entails no more than "nominal cost" for the recipient; and
- *Require giving individuals access to electronic copies of their PHI* that is in electronic form.


Nancy L. Perkins

2. Amendments to notices of privacy practices

The Final Rule requires new statements in each covered entity's Notice of Privacy Practices (NPP). For example, the NPP now must include statements that:

- Certain uses and disclosures of PHI require an individual authorization, including uses and disclosures for marketing purposes; disclosures that constitute a "sale" of PHI; and most uses and disclosures of psychotherapy notes (the latter need be included only where relevant).
- No uses or disclosures may be made without an individual authorization for a purpose that is not explicitly described in the NPP.
- Individuals have the right to be notified of a security breach that compromises the privacy of their PHI.

- Individuals who receive fundraising communications have the right to opt out of receiving any further such communications.
- Individuals have the right to require a health care provider to withhold from any health plan/insurer information pertaining to treatment the individual paid for out of pocket (applicable only to provider NPPs).
- No use or disclosure of genetic information may be made for insurance underwriting purposes (applicable only to health plan NPPs).

3. Amendments to business associate agreements

Reflecting the fact that business associates are now directly subject to the Privacy and Security Rules and to incorporate the breach notification requirements applicable to business associates, the Final Rule requires updating of business associate agreements (BAAs) to include provisions requiring the business associate to:

See Also

BLOG: Obama administration releases new Affordable Care ...

HHS proposes new guidelines for Medicaid, CHIP, health ...

BLOG: New reviews related to physician services in OIG's ...

- Comply with all applicable requirements of the Privacy Rule and all requirements of the Security Rule with respect to electronic PHI (rather than simply to implement safeguards to ensure the security of such PHI);
- Comply with the Privacy Rule's provisions governing the covered entity when acting to fulfill the covered entity's Privacy Rule obligations (such as preparing or distributing NPPs or notices to individuals of breaches of the security affecting their PHI).
- Enter into written, HIPAA-compliant BAAs that conform to the Privacy and Security Rules' specifications with any subcontractors that create or receive PHI on behalf of a business associate;
- Report to the covered entity any breach of "unsecured" PHI without "unreasonable delay" and in no event later than 60 days after discovering the breach;

HHS has prepared a sample revised business associate agreement that provides some guidance on this newly required content.

4. Amendments to security breach incident response plans

As noted, the Final Rule eliminates the "risk of harm" standard that HHS previously prescribed for determining whether individuals and HHS must be notified about a breach of security affecting "unsecured" PHI. Specifically, notifications previously were not required unless such a security incident posed a "significant risk of financial, reputational, or other harm" to the individual. Under the Final Rule, however, notifications are *uniformly* required unless, following an investigation, it can be determined that there is a "low probability" of any compromise to the security of the PHI involved. Each such investigation must include a risk assessment that analyzes:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.

The required assessment should consider all these factors (and others as relevant) in combination, and the analysis must be documented in writing. This documentation will be essential to defending a decision not to provide notifications.

5. Training of employees and agents

Covered entities should train their workforce members, including employees, agents, and any others working under their control, on all of the new requirements and restrictions imposed by the Final Rule.

Business associates

Who are now "business associates"?

The Final Rule does not change the basic concept of who is a "business associate" — which, in relation to a covered entity, means a person who (other than as a member of the covered entity's workforce) either (i) performs health care functions "on behalf of such covered entity," or (ii) provides certain services, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to the covered entity, and needs access to PHI to perform those functions or services. Under the Final Rule, however, *subcontractors* of business associates are also defined as "business associates." Specifically, when a business associate delegates to a third party a function, activity, or service that involves the creation, receipt, maintenance, or transmission of PHI, the subcontractor is itself a "business associate."

Under the HITECH Act, all business associates are liable not only for breach of their BAA obligations, but also are directly liable for violations of the Privacy Rule, Security Rule and Breach Notification Rule. And as HHS emphasized when issuing the Final Rule, whether an entity is a "business associate" does *not depend on the existence of a BAA*. Therefore, a party may become a "business associate" even if the covered entity/business associate for whom it agrees to perform functions or services never mentions the obligation to enter into a BAA.

This means that an entity could potentially be a business associate without knowing it. For example, a data storage company might receive files from a business associate that contain PHI, but the business associate might fail to mention the PHI. The storage company, by performing a function for the business associate that permits access to PHI (even if that access is not exercised) would meet the definition of a "business associate" and be directly liable for violations of the HIPAA/HITECH rules, whether or not it was aware of that legal consequence.

See Also

BLOG: Obama administration releases new Affordable Care ...

HHS proposes new guidelines for Medicaid, CHIP, health ...

BLOG: New reviews related to physician services in OIG's ...

This suggests the need for all entities to be proactive about determining their own "business associate" status.

What new obligations are required of business associates?

The Final Rule codifies the obligations of business associates that were prescribed by the HITECH Act, which should be documented in written policies maintained by each business associate. At a minimum, those policies should include:

1. Privacy policy

The privacy policy should document the business associate's obligations to:

- Comply with the terms of all of BAAs the business associate has entered into, including the agreement not to use or disclose PHI in a manner that would be impermissible if done by the covered entity/primary business associate;
- Notify covered entities/primary business associates of breaches of "unsecured" PHI;
- Provide access to electronic PHI to either the covered entity/primary business associate or an individual (or such individual's designee);
- Maintain and provide, upon request, an accounting of disclosures of PHI;
- Disclose PHI when required by HHS to investigate or determine the business associate's compliance with the HIPAA Rules;
- Abide by the requirement to use and disclose only the "minimum necessary" amount of PHI needed to accomplish a particular purpose;
- Train all workforce members and agents on their privacy and security obligations.

2. Security policy

The security policy should include all the elements required by the HIPAA Security Rule, including:

- Mechanisms to implement all "required" and appropriate "addressable" specifications for protection of electronic PHI.
- Standards to ensure adequate and effective:
- administrative safeguards
- physical safeguards
- technical safeguards

3. Security breach incident response policy

The security breach incident response policy should cover all the basic elements of a HIPAA covered entity's breach response plan, tailored to the business associate's specific circumstances and taking into account the amount, type and form of PHI maintained by the business associate.

Timing

How soon must all the above-referenced steps be accomplished? As noted, compliance with most of the provisions of the Final Rule is required by September 23, 2013. For executing new or updated BAAs, however, HHS has provided additional time. Specifically, the Final Rule provides that any BAA that (i) complies with the current Privacy and Security Rules, (ii) was entered into prior to January 25, 2013 (the publication date of the Final Rule), and (iii) is not renewed or modified between March 26, 2013 (the Final Rule's effective date) and September 23, 2013 (the Final Rule's general compliance date), will be deemed in compliance with the Final Rule until the earlier of:

1. the date the BAA is renewed or modified on or after September 23, 2013, and
2. September 22, 2014

Essentially, this means that, absent of any reworking of a preexisting, currently compliant BAA, the BAA will be deemed in compliance with the Final Rule for a full year after the Final Rule's general compliance date.

A lot of work lies ahead for covered entities and business associates — especially business associates that are newly defined as such under the Final Rule. These entities should take proactive steps, in coordination with legal counsel, to meet the Final Rule's requirements in a timely manner.

Nancy L. Perkins, JD, can be reached at Arnold & Porter LLP, 555 12th St. NW, Washington, DC 20004-1206; 202-942-5065; email: nancy.perkins@aporter.com