What We Need to Do to Comply with the Final HIPAA Rule: A Summary of the Privacy Obligations for Health Care Providers, Health Plans, Business Associates and their Subcontractors

03.18.13

By: Cheryl Camin Murray

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) published the highly anticipated Omnibus Rule, which makes extensive changes (as promulgated by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)) to the privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA). The Omnibus Rule is effective March 26, 2013. However, the deadline for compliance with the Omnibus Rule is not until September 23, 2013.

Covered entities, such as health care providers and health plans, as well as their vendors and contractors, referred to as "business associates" must comply with the Omnibus Rule. So, what needs to be done? A number of action items should be taken by September 23rd, some of which include:

Notice of Privacy Practices:

Notice of Privacy Practices need to be updated to include:

(i) A description of the types of uses or disclosures that require an authorization.

(ii) If a covered entity uses protected health information (also referred to as "PHI") for fundraising activities, a statement that the covered entity may contact the individual to raise funds and the individual has the right to opt out of such communication.

(iii) If a covered entity is a health plan and intends to use PHI for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing PHI that is genetic information for such purposes.

(iv) A statement that a covered entity (that is a health care provider) is not required to agree to an individual's request for a restriction, except in the case of a request to restrict the disclosure of PHI to a health plan if (a) the disclosure is for the purpose of carrying out payment or health care operations; and (b) the PHI pertains solely to a health care item or service for which the individual has paid the covered entity in full.

(v) An explanation that the covered entity is required to notify affected individuals following a breach of unsecured protected health information.

Generally, under the HIPAA, if there is a material change to the notice, then the health plan must provide the revised notice (or information about the material change and how to obtain the revised notice) to the individuals then covered by the plan within 60 days of the revision to the notice. For a health plan that posts the notice on its website, it must also post the change or its revised notice on its website by the effective date of the change. The revised notice, required under the Omnibus Rule, or information about the material change and how to obtain the revised notice, must be provided within 60 days of the compliance date (i.e. September 23, 2013) and, therefore, for most participants would be included in the health plan's annual enrollment materials. If the health plan posts its notice on a website, then the health plan must post the revised notice by September 23, 2013.

Business Associates

The definition of a business associate has been expanded to include a health information organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI. In addition, personal health record companies and subcontractors of business associates are included in the definition of business associate. Based on this revised definition, arrangements with business associates should be re-evaluated to determine who falls within the description of a business associate.[1]

Business Associate Agreements and Subcontractor Agreements should be revised to comply with the Omnibus Rule. Business Associate Agreements should include provisions that require the business associate (i) to comply with various sections of the HIPAA Security Standards; and (ii) to notify the covered entity if there is a breach of unsecured PHI. In addition, business associates must enter into written Business Associate Agreements with their subcontractors. Business Associate Agreements that are already in place are grandfathered and don't have to comply with the Omnibus Rule until September 23, 2014. However, for new Business Associate Agreements, they must meet the requirements under the Omnibus Rule by September 23, 2013.

In addition, business associates are now subject to civil monetary penalties for HIPAA violations. In addition, they are required to perform risk analyses of the potential risks and vulnerabilities of electronic PHI transmitted, created, maintained or received by the business associate.

Authorization, Marketing, Fundraising, and Access

The final privacy rule further defines the limits on the use of patient information, without authorization, for marketing and fundraising and prohibits the sale of protected information without specific authorization. Patients who pay for medical services out of their own pockets can now restrict the use of their health information by their insurance companies or health plans. In addition, the Omnibus Rule changes the format of authorizations used for research purposes.

Also, an individual will have expanded access to his or her own PHI. In particular, if an individual requests an electronic copy of the PHI maintained electronically in a designated record set, the covered entity must provide such access in the requested electronic form.

Breach

A very important change is to the definition of "breach". Currently, the definition of a breach means "the acquisition, access, use, or disclosure of protected health information in a manner not permitted, which *compromises the security or privacy of the protected health information*." This definition has not changed. However, before the passage of the Omnibus Rule, the definition of "compromises the security or privacy of the protected health information," meant "poses a significant risk of financial, reputational, or other harm to the individual." This definition and the "significant risk of harm" threshold have been removed from the Omnibus Rule.

Now an impermissible acquisition, access, use, or disclosure of unsecured PHI is presumed to be a breach unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

(i) The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the PHI or to whom the disclosure was made;
(iii) Whether the PHI was actually acquired or viewed; and
(iv) The extent to which the risk to the PHI has been mitigated.

The new standard would require notice to HHS, to the patients and to the media of any improper disclosure of protected health information, unless it is shown that there is a "low probability" that patient privacy was compromised as a result of the incident. This standard increases the probability that a breach would have to be reported and is expected to require more-frequent notice to the government, patients, and media, as well as increased investigations by HHS.

Both covered entities and business associates are subject to these breach notification requirements. A current research study indicates that 62 percent of breaches of patient privacy that amount to HIPAA violations were related to conduct by business associates. These business associates, which can include data processing firms, law firms, accounting firms, information technology consultants, billing and collection companies, cloud computing providers, and many other vendors that contract with health care companies are legally prohibited from breaching patient privacy, even inadvertently.

For business associates, just as for health care providers and other covered entities, fines may be no more than $50,000 per violation and can increase to a maximum penalty of $1.5 million. Each organization's policies and procedures for handling potential breaches should include this new definition of breach and the risk assessment process.

Policies, Procedures and Training

HIPAA policies, procedures, and compliance programs will need to be updated to comply with all of the new requirements under the Omnibus Rule. These policies and procedures should be monitored and reviewed regularly to ensure that they

continue to fit the operations and changing structure of your organization as well as future changes in applicable federal and state law.

HIPAA training programs should be modified and employees, consultants and volunteers should be re-trained on the new requirements. Such training should be properly documented. As soon as possible, these steps should be taken in order to ensure that your organization is in compliance by the applicable deadline.

---

[1] Also, organizations that are organized health care arrangements or hybrid entities, which are covered entities with business associate components, should re-evaluate the structure of their organization and the integration of their components based on the new requirements of the Omnibus Rule.

Contact:
Cheryl Camin Murray | 214.745.5142 | cmurray@winstead.com