BuchalterNemer
A Professional Law Corporation

Client Alert

February 2013

Now Is The Time To Revise Your Business Associate Agreements and Notice of Privacy Practices

Julie A. Simer, Esq. and Brooke J. Ledger, Esq.

There is a lot of confusion among providers caused by the recent publication of new rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). On January 25, 2013, the HIPAA final omnibus rule ("Final Rule") issued by the U.S. Department of Health and Human Services ("HHS") was published in the Federal Register (78 FR 5565). The Final Rule is actually four rules rolled into one massive 523-page rule. The Final Rule changes the requirements necessary to protect the privacy and security of protected health information ("PHI") under the HIPAA Privacy, Security and Enforcement Rules. The Final Rule strengthens protection for PHI and heightens breach-reporting obligations. For providers, it will require:

1. Revising Existing Notices of Privacy Practice
2. Revising Existing Business Associate Agreements
3. Requiring Business Associates to Execute Business Associate Agreements With Subcontractors

Deadline for Compliance

The date for compliance with the Final Rule is September 23, 2013. However, if a business associate agreement was in effect prior to January 25, 2013, a new business associate agreement is not necessary until the existing agreement is modified or renewed, or September 23, 2014, whichever is earlier. However, this does not mean that a provider has time to waste. Important steps must begin now.

Conduct an Immediate Inventory

The Final Rule expands the definition of "business associate." The term now includes subcontractors of business associates as well as those who create, receive, maintain, or transmit PHI, even if the PHI is never accessed. However, there are some nuances to this rule; for example, a business such as an Internet service provider, which only acts as a conduit for data, does not need to execute a business associate agreement, but a storage company that maintains paper records does. Consequently, there are many types of existing arrangements that now need business associate agreements that did not need them in the past. Therefore, providers must immediately inventory all of their arrangements with entities that have access to PHI and determine (a) whether the arrangement requires a business associate agreement, (b) if a business associate agreement has been executed, and (c) the date any executed business associate agreement will expire or be renewed.

Communicate with Your Business Associates

Once the inventory is complete, it is time to communicate with business associates about the need to conduct an inventory of arrangements with subcontractors. Business associates must execute business associate agreements with any subcontractors who create, receive, maintain, or transmit PHI. The minimum necessary standard applies to the use of PHI by business associates and subcontractors, so they will each need to have policies in place to prevent unnecessary access to PHI.

Review Your Business Associate Agreement

A sample of a new business associate agreement is provided on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

However, before you start using the HHS form, or one prepared by a vendor, consider whether the form provides the necessary protection from liability. Data breaches can result in significant fines and penalties, as well as liability for damages. A provider may choose to include indemnity provisions in the business associate agreement to appropriately place liability upon the business associate in the event the business associate or a subcontractor causes the breach. The form business associate agreement provided by HHS does not address such liability issues.

Also, note that the increased penalties under the Final Rule are assessed "per violation," so penalties can add up quickly when the records of many individuals are lost or disclosed. The business associate agreement should specify how and when the provider will be notified of a breach and who will provide the notice to affected individuals.

Under previous rules, the business associate agreement was required to include a provision that if the business associate agreement could not terminate the contract upon notice of a material breach by the physician, the business associate was required to notify the Secretary of HHS. That provision is no longer required, so physicians will want to act quickly to revise

their business associate agreements to make it clear that the business associate does not have to notify the Secretary under such circumstances.

Revise Your Notice of Privacy Practices

Under the Final Rule, health care providers with a direct treatment relationship with an individual must revise and redistribute their Notice of Privacy Practices ("Notice"). In addition to previously mandated requirements, the Notice must include these statements:

- The right to be notified in the event of a breach of the individual's PHI;
- The right to request that a health plan not be informed of treatment which is paid for in full by the individual, and the covered entity's obligation to comply with such a request;
- That consent is required prior to the use or disclose of an the individual's psychotherapy notes, or the use the individual's PHI for marketing purposes;
- The right to opt out of communications for fundraising purposes;
- A statement that a health plan is prohibited from disclosing genetic information for underwriting purposes (applies to health plans only).

Note that business associates are not required to provide a Notice unless such responsibility is delegated to the business associate, making it a contractual requirement, not a requirement of the Final Rule. Providers must revise and prominently post Notices on or promptly after the effective date of March 26, 2013. Although providers do not need to mail the new Notice to all existing patients, they must post the revised Notice in a clear and prominent location and have copies of the Notice at the delivery site for individuals to request to take with them. Providers are only required to give a copy of the Notice to, and obtain a good faith acknowledgment of receipt from, new patients. Providers may post a summary of the Notice as long as the full Notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up. It is not sufficient to require the individual to ask the receptionist for a copy of the full Notice.

Steps Going Forward

- Conduct a risk assessment to determine the likelihood of a data breach.
- Update compliance policies for obtaining business associate agreements and distributing the Notice of Privacy Practices
- Update an incidence response plan identifying the procedure to be followed in the event of a security breach.
- Set up monitoring and internal audits to avoid lapses in the privacy and security of PHI.

There is no reason to wait until the last minute; the time is now to review business associate agreements and Notices of Privacy Practices to avoid unexpected liability.

Julie A. Simer is a Shareholder in the firm's Health Care Practice Group. She can be reached at 949.224.6259 or jsimer@buchalter.com.

Brooke J. Ledger is an Associate in the firm's Health Care Practice Group. She can be reached at 949.224.6436 or bledger@buchalter.com.