HIPAA: Not Just For Doctors Anymore; Beware The Designation 'Business Associate'

May 8, 2013

The final rules implementing the Health Information Portability and Accountability Act ("HIPAA") became effective in March and apply to persons and companies other than those in the health industry. The rules are cumbersome to navigate, but compliance is required by September.

Background

On January 25, 2013, the Department of Health and Human Services ("DHHS") published the final omnibus rule ("Rule") implementing changes to the privacy, security, breach notification, and enforcement regulations under the Health Information Portability and Accountability Act ("HIPAA"). The Rule extends the reach and liability of the HIPAA privacy and security regulations not only for covered entities, but also for business associates as well. In fact, the most significant changes under the Rule apply directly to business associates.

The Rule became effective on March 26, 2013, and covered entities and business associates are expected to be in compliance by September 23, 2013. The Rule can be cumbersome to navigate, particularly for businesses outside the health care industry that may be introduced to HIPAA for the first time. This article provides an overview of the changes the Rule implements that directly apply to business associates, and provides best practice tips on how to move forward with HIPAA compliance before the September deadline.

Who is a Business Associate?

The Rule revises the definition of a "business associate" to include any person or entity that creates, receives, maintains, or transmits protected health information ("PHI") on behalf of a covered entity. The Rule also continues to impose business associate burdens and obligations on any person or entity that is not part of the covered entity's workforce, but that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, including claims processing, data analysis, utilization review, quality assurance, and patient safety activities to a covered entity.

The Rule lists three specific categories of entities that are included within the definition of a business associate. These categories are:

- Health information organizations, e-prescribing gateways, or other persons or entities providing data transmission services to a covered entity that requires access on a routine basis to PHI;
- Any person or entity that offers a personal health record to an individual on behalf of a covered entity; and,
- Any subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate.

Before the Rule was adopted, business associates and their subcontractors were not directly subject to HIPAA, and the only obligation business associates had was to ensure that their subcontractors complied with the terms of the business associate agreement that the business associate had with the covered entity. The

revised definition of a business associate now includes subcontractors of business associates. This means that business associates are required to enter into HIPAA-compliant business associate agreements with their subcontractors. Furthermore, the subcontractors will be required to enter into HIPAA-compliant business associate agreements with their subcontractors, and so forth on down the line. It is not the responsibility of the covered entity to have business associate agreements with the various subcontractors that may be engaged by business associates of the covered entity. This responsibility falls on each business associate for each of its subcontractors.

Examples of Who is and Who is not a Business Associate

With the broad definition of the term 'business associate," it is easy to see how a business dealing with health care providers would be concerned as to whether or not it is now a business associate. The Rule provides concrete examples regarding who is and who is not a business associate.

The Rule reaffirms that the term business associate does not include:

- A health care provider who receives PHI from a covered entity concerning the treatment of a patient;
- A group health plan sponsor;
- A government agency charged with determining eligibility for, or enrollment in, a government health plan; or,
- A covered entity participating in an organized health care arrangement that performs a particular service, function, or activity on behalf of that organized health care arrangement.

In addition to these narrowly defined exclusions, the Rule provides further guidance on persons and entities that are not business associates. First, the so-called "conduit exception" still applies and operates to exclude entities from business associate status that act as "mere conduits" for the transport of PHI, but that do not access the PHI other than on a random or infrequent basis. Examples of persons and entities that would meet the conduit exception include the United States Postal Service, United Parcel Service ("UPS"), telecommunication companies, and internet service providers providing only mere data transmission. But the Rule specifically includes within the business associate designation document storage companies maintaining PHI for covered entities, regardless of whether they actually view the information.

Moreover, the Rule names other types of persons or entities that are not burdened with the status of business associate, such as:

- External researchers, even if a covered entity hires the researcher;
- External or independent Institutional Review Boards; and,
- Banks and other financial institutions that perform payment processing activities on behalf of a covered entity.

What's a Business Associate to Do?

Along with the expanded definition of business associate, the Rule extends some of HIPAA's privacy, security, and enforcement provisions to business associates for the first time. For example, the HIPAA security administrative, physical, technical safeguards and documentation requirements now apply directly to business associates. Business associates must now develop and implement written HIPAA-compliant security policies and procedures.

There are also provisions within the Rule that affect what a business associate can do with PHI. For example, business associates, when using, disclosing, or requesting PHI, must take reasonable steps to limit the amount of PHI to the minimum necessary to accomplish the relevant task. Additionally, a covered entity or business

associate must obtain authorization from an individual before any disclosure of PHI that would constitute a "sale" of the PHI, and such authorization must state that the disclosure is part of a sale of the PHI. A "sale" of PHI means a disclosure of PHI by a covered entity or business associate for which it receives direct or indirect remuneration.

If you are a business associate, or a subcontractor working for a business associate, your first step should be to enter into all necessary HIPAA-compliant business associate agreements. Of course, covered entities have always been, and continue to be, required to enter into HIPAA-compliant business associate agreements. Now you, as a business associate, must enter into HIPAA-compliant business associate agreements with your subcontractors. You should also take this opportunity to review your current business associate agreements with covered entities to ensure they are in compliance with the newly promulgated Rule.

Penalties

The Rule provides that business associates are now directly liable under the HIPAA privacy and security rules for impermissible uses and disclosures of PHI, failure to notify covered entities regarding a breach of unsecure PHI, failure to provide access to a copy of electronic PHI with respect to an individual's request, failure to disclose PHI when required by the Secretary of DHHS, failure to enter into business associate agreements with subcontractors, failure to comply with the minimum necessary rule, and failure to comply with the HIPAA security rule.

There are civil monetary penalties for failure to comply with the Rule. The penalties are ranked on a tiered level based on levels of culpability. If the covered entity or business associate did not know and could not have known of the HIPAA violation, then the penalty range is $100 - $50,000 per incident. If the covered entity or business associate knew, or would have known through reasonable due diligence, that an act or omission would violate the Rule, but did not act with willful intent, then the penalty range is $1,000 - $50,000 per incident. If the covered entity or business associate acted with willful neglect, but corrected its violation within 30 days, then the penalty range is $10,000 - $50,000 per incident. If the covered entity or business associate acted with willful neglect and took no corrective measures within 30 days, then the penalty is $50,000 per incident. There is an annual aggregate cap of $1.5 million for violations of the same provision.

Summary

The Rule has expanded the application of the term "business associate" under HIPAA and imposes new obligations and liability on business associates and their subcontractors if they don't become HIPAA-compliant before September 23. There are potentially severe civil monetary penalties for violations. Business associates and their subcontractors should take steps now to develop and implement HIPAA privacy and security policies and procedures so they will be in place by the September 23, 2013 compliance date.

--