Health Care Industry News
Headlines You Need to Know

meade | ensslin
Prompt. Efficient. Results.

March 6, 2013

Top Health Care Entities Know When To Seek Counsel

ATTORNEY AT LAW
Tammy Meade Ensslin
World Trade Center
333 West Vine Street
Suite 300 East
Lexington, Kentucky 40507

Phone: 859-368-8747
Fax: 859-317-9729
tensslin@meadeensslin.com

Revised HIPAA Rules for Business Associates Become Effective March 26, 2013

Legal Alert: On January 17, 2013, the U.S. Department of Health and Human Services (HHS) moved forward with additional rules to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The new rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law. In the past, the HIPAA rules have focused on health care providers, health plans and other entities that process health insurance claims. The new changes recently announced expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors. According to HHS, some of the largest breaches have involved business associates.

Some of the key provisions include:

Definition of "Business Associate"

The final rule added the following to the definition of business associate (45 CFR §160.103):

1. A health information organization, e-prescribing gateway, or other entity that provides data transmission services to a covered entity and requires access on a routine basis to protected health information (PHI). The preamble to the final rule clarifies that an entity that is a mere *conduit* (such as the U.S. Postal Service, UPS or other courier service) does not require access to PHI, and therefore is not included.
2. An entity that offers a personal health record (PHR) *on behalf of* a covered entity. However, if the PHR is not offered on behalf of a covered entity, the PHR vendor is not a business associate.
3. A subcontractor. The new rule provides that if a business associate subcontracts part of its function requiring access or use of PHI to another organization, that subcontractor is also subject to HIPAA. Accordingly, there must be an agreement between the business associate and its subcontractor that contains the elements required to be included in business associate agreements and describes the subcontractor's permitted uses and disclosures of PHI (which may not include uses and disclosures not permitted to the business associate).

The final rule also clarifies that a business associate includes a person or entity that creates, receives, *maintains*, or transmits PHI on behalf of a covered entity. The word "maintains" has been added to the definition to recognize entities that maintain PHI on behalf of a covered entity, such as physical storage facilities or companies that store electronic PHI in the cloud--even if they do not access or view the PHI—are business associates of the covered entity, as opposed to mere "conduits" (which transport information but do not access it other than infrequently which are excepted from the definition of "business associate"). *This clarification is significant and likely will require covered entities to enter into business associate agreements with additional contractors.*

The final regulations also clarify that when a covered entity discloses information to a health care provider concerning the treatment of an individual, the health care provider is *not* regarded as a business associate of the covered entity. Also, when a group health plan or insurer discloses information to the plan sponsor, or when a government agency determines eligibility for a benefit plan, the plan sponsor and government agency are not business associates.

Liability under HIPAA

Another critical portion of the new rule addresses liability of the business associate and their subcontractors. Under the new rule, business associates--and their subcontractors--are now directly liable both for violations of the Security Rule and for uses and disclosures of PHI in violation of the Privacy Rule. Business associates also have the following responsibilities:

1. To keep records and submit compliance reports to HHS, when HHS requires such disclosure in order to investigate the business associate's compliance with HIPAA, and to cooperate with complaint investigations and compliance reviews (45 CFR §160.310(a), (b));
2. To disclose PHI as needed by a covered entity to respond to an individual's request for an electronic copy of his/her PHI ((45 CFR §160.502(a)(4));
3. To notify the covered entity of a breach of unsecured PHI (45 CFR §160.410(a));
4. To make reasonable efforts to limit use and disclosure of PHI, and requests for PHI, to the minimum necessary (45 CFR §160.501(b)(1));
5. To provide an accounting of disclosures (76 Fed. Reg. 31426 (May 2011); and
6. To enter into agreements with subcontractors that comply with the Privacy and Security Rules (45 CFR §314(a)(2)(iii); §164.504(e)(5)).

Also, penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation.

Business Associate Agreements

In addition to the provisions previously required by the Privacy Rule and the Security Rule, business associate agreements between covered entities and business associates now must require that the business associate comply with the Security Rule obligations for *electronic PHI* and report breaches of unsecured PHI to the covered entity. Also, if the business associate is to carry out any part of a covered entity's obligation under the Privacy Rule, the business associate must comply with the Privacy Rule with respect to that activity. If the business associate subcontracts any of its activities, it must enter into an agreement with its subcontractor that complies with the requirements for business associate agreements, and it may not permit the contractor to use or disclose PHI in a manner that would not be permissible to the business associate.

Expansion of Patient Rights

Individual rights are also expanded under the new rule. Patients can ask for a copy of their electronic medical record in an electronic form. And, when individuals pay by cash they can instruct their health care provider not to share information about their treatment with their health plan. The final rule sets new limits on how information is used and disclosed for marketing and fundraising purposes and prohibits the sale of an individuals' health information without their permission. The final rule also reduces burden by streamlining individuals' ability to authorize the use of their health information for research purposes and makes it easier for parents and others to give permission to share proof of a child's immunization with a school.

Timeline to Comply

The rules become effective on March 26, 2013, and compliance is required by September 23, 2013. If covered entities and business associates have business associate agreements now in effect, the existing agreements are grandfathered in for a period of one year after the required compliance date (September 23, 2013) to allow time for modification of the agreements to comply with the final regulations.

For assistance in updating your business associate agreements, to ensure compliance with the new rule, or for other questions regarding HIPAA compliance, please contact me at your convenience.

The final rule is based on statutory changes under the HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and the Genetic Information Nondiscrimination Act of 2008 (GINA) which clarifies that genetic information is protected under the HIPAA Privacy Rule and prohibits most health plans from using or disclosing genetic information for underwriting purposes.

For additional information on Health Care Law issues, please contact TAMMY MEADE ENSSLIN at 859-368-8747.