Maniaci Insurance Services, Inc.
500 Silver Spur Road
Suite 121
Palos Verdes, California 90275
(310) 541-4824
http://www.maniaciinsurance.com

Significant Changes for Health Care Providers, Health Plans, and Their Business Associates and Subcontractors in Final HIPAA Privacy Regulations

Date: 02.04.2013

The Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services published its long-awaited final privacy and security regulations ("Final Rule") under the Health Insurance Portability and Accountability Act ("HIPAA") on January 25, 2013. The Final Rule becomes effective March 26, 2013, and, in general, covered entities and business associates are required to comply by September 23, 2013.

The Final Rule addresses four key areas: (i) changes made by the Health Information for Economic and Clinical Health Act ("HITECH Act"); (ii) the HIPAA enforcement rule; (iii) updates to the data breach notification regulations; and (iv) changes made by the Genetic Information Nondiscrimination Act. Some significant changes are summarized below.

Business Associates and Subcontractors

One of the most significant changes under the HITECH Act is that it makes Business Associates ("BAs") directly liable under certain provisions of the HIPAA privacy and security rules ("HIPAA Rules"). In addition, the Final Rule provides further guidance concerning which entities are BAs, resulting in the *treatment of certain subcontractors of BAs as BAs themselves, directly subject to the HIPAA Rules.* The Final Rule, for example, clarifies that a BA is a person who performs functions or activities on behalf of, or certain services for, a covered entity or another BA that involve the use or disclosure of protected health information ("PHI").

Importantly, the Final Rule establishes that a person becomes a BA *by definition*, not by the act of contracting with a covered entity or otherwise. Therefore, direct liability for the BA under the HIPAA Rules and HITECH Act for impermissible uses and disclosures and other provisions attaches immediately when a person creates, receives, maintains, or transmits PHI on behalf of a covered entity or BA and otherwise meets the BA definition. As a result of some of these changes, covered entities and BAs should consider re-examining their relationships with their subcontractors to ensure they obtain the appropriate, satisfactory assurances concerning the PHI they make available to those subcontractors. For more information about identifying BAs and subcontractors, see Final HIPAA Regulations: "Business Associates" Include Subcontractors, Data Storage Companies (Cloud Providers?).

The Final Rule also clarifies the BAs are *directly liable* under the HIPAA Rules for:

1. uses and disclosures of PHI not permitted under HIPAA;
2. a failure to provide breach notification to the covered entity;
3. a failure to provide access to a copy of electronic PHI to the covered entity, the individual, or the individual's designee (as specified in the business associate agreement ("BAA"));
4. a failure to disclose PHI to the Secretary of Health and Human Services to investigate or determine the BA's compliance with the HIPAA Rules;
5. a failure to provide an accounting of disclosures; and
6. a failure to comply with the HIPAA Security Rule.

BAs remain contractually liable for the other provisions of BAAs.

In attempting to minimize this liability, the Final Rule also confirms that OCR does not endorse any "certification" process for compliance with the HIPAA Rules or HITECH Act. Thus, BAs and subcontractors should not rely on such programs that may be available. However, it is critical that BAAs be updated to reflect new requirements and to allocate certain liabilities and responsibilities. A transition rule under the Final Rule permits covered entities and BAs to continue operation under certain existing contracts for up to one year beyond the compliance date (September 23, 2013). A qualifying BAA will be deemed compliant until the earlier of (i) the date such agreement is renewed or modified on or after September 23, 2013, or (ii) September 22, 2014. The transition rule applies only to the language in the agreements, the parties must operate as required under the HIPAA Rules in accordance with the applicable compliance dates.

Breach Notification Rule

The Final Rule retains many requirements from the interim final breach notification rule. However, it removes the "risk of harm" standard in exchange for a more objective standard for determining whether a "breach" has occurred. (Thus, inquiry into whether there is a significant risk of harm to privacy and security is no longer appropriate.) The Final Rule establishes a presumption that impermissible uses and disclosures of PHI are breaches, unless an exception applies. Covered entities can rebut that presumption (removing the notification requirement) by engaging in a risk assessment to determine whether there is a low probability that PHI has been compromised. However, because of the presumption, covered entities may avoid the risk assessment and provide notification.

A risk assessment would examine at least the following four factors:

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.

If no exception applies and, after reviewing all of these factors, the covered entity cannot demonstrate that there is a low probability of compromise to the PHI, notification is required. The OCR cautioned that, when working through these factors, many forms of health information can be sensitive, not just information about sexually transmitted diseases, mental health diseases or substance abuse. In addition, the OCR confirmed that violations of the minimum necessary rules also could result in breaches requiring notification.

OCR clarified other aspects of the breach notification rule:

- The time for notification begins to run when the incident is known to have occurred, not when it has been determined to be a breach. However, a covered entity is expected to make notifications after a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual(s).
- The obligation to determine whether a breach has occurred and to notify individuals remains with the covered entity. However, covered entities can delegate these functions

to third parties or BAs.
- Written notification by first-class mail is the general, default rule. However, individuals who affirmatively agree to receive notice by e-mail may be notified accordingly. In limited cases, individuals who affirmatively agree to be notified orally or by telephone may be contacted though those means with instructions on how to pick up the written notice.
- Notices of Privacy Practices must include a statement that covered entities must notify affected individual following a breach.

Enforcement Rule

The Final Rule implements the changes HITECH Act made to the enforcement provisions of the HIPAA rules, including penalty amounts, which now also apply to BAs. The HITECH Act penalty scheme can be summarized as follows:

- "Did not know" penalty - amount not less than $100 or more than $50,000 per violation when it is established the covered entity or BA did not know and, by exercising reasonable diligence, would not have known of a violation;
- "Reasonable cause" penalty - amount not less than $1,000 or more than $50,000 per violation when it is established the violation was due to reasonable cause and not to willful neglect;
- "Willful neglect-corrected" penalty - amount not less than $10,000 or more than $50,000 per violation when it is established the violation was due to willful neglect and was timely corrected;
- "Willful neglect-not corrected" penalty - amount not less than $50,000 for each violation when it is established the violation was due to willful neglect and was not timely corrected.

A penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year.

In addition, OCR made clear in the Final Rule that it *will* investigate a complaint and it *will* conduct a compliance review when the circumstances or its preliminary review suggests willful neglect is possible. Willful neglect is defined at 45 CFR § 160.401 as the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." The term not only presumes actual or constructive knowledge a violation is virtually certain to occur, but also encompasses a conscious intent or degree of recklessness with regard to compliance obligations. The proposed regulations provided examples of where willful neglect may be found:

- A covered entity disposed of several hard drives containing electronic PHI in an unsecured dumpster, in violation of § 164.530(c) and § 164.310(d)(2)(i). HHS's investigation reveals the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard PHI during the disposal process.
- A covered entity failed to respond to an individual's request that it restrict its uses and disclosures of PHI about the individual. HHS's investigation reveals the covered entity does not have any policies and procedures for consideration of restriction requests it receives and refuses to accept any requests for restrictions from individual patients who inquire.
- A covered entity's employee lost an unencrypted laptop that contained unsecured PHI. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 *et seq.*

Genetic Information Nondiscrimination Act

The Genetic Information Nondiscrimination Act (GINA) prohibits discrimination on the basis of an individual's genetic information. GINA also contains privacy protections for genetic information that requires HHS to modify the HIPAA Rules. The protections require (i) clarification that genetic information is health information and (ii) health plans, health plan issuers and issuers of Medicare supplemental policies be prohibited from using or disclosing genetic information for underwriting purposes. The Final Rule implements these protections by incorporating certain definitions from GINA and other provisions relating to health plans (health

care providers are generally not subject to these provisions). In addition, the Final Rule requires a change to the Notice of Privacy Practices for health plans. Namely, if a covered health plan will be using PHI for underwriting purposes (such as in a wellness program), the plan's Notice of Privacy Practices must include a statement that PHI that is genetic information may not be used for this purpose.

Action Needed

The Final Rule includes substantial changes to the HIPAA Final Rules for covered health care providers and health plans, as well as their BAs. These entities will need to review these regulations carefully and make appropriate adjustments in their policies and procedures, workforce training, privacy and other notices, systems, as well as their agreements. Most of this will need to be completed by September 23, 2013, although a transition rule will allow a one-year extension until September 23, 2014 to amend certain existing business associate agreements.

Please contact your UBA Partner Firm if you have any questions about health care reform.

Jackson Lewis LLP