HHS Finalizes HIPAA Privacy and Data Security Rules, Including Stricter Rules for Breaches of Unsecured PHI

Executive Summary

- HHS has issued final regulations that address recent legislative changes to the HIPAA privacy and data security rules. Compliance by employers will be required by September 23, 2013 at the earliest.
- A new standard will apply in determining what qualifies as a breach of unsecured protected health information (PHI). The new rule will presume a breach has occurred unless the plan can demonstrate a low probability the PHI has been compromised.
- New terms are required for business associate agreements (BAA). For most agreements that require revisions, amendments won’t be required until September 23, 2014.
- Additional language will be required for the plan’s notice of privacy practices. To the extent that the plan’s privacy notice already meets the regulation’s requirements, the plan is not required to revise and distribute another privacy notice on account of the final rules.
- The regulations codify other requirements related to access to PHI, requesting restrictions on use of PHI, and using genetic information for underwriting purposes.

The U.S. Department of Health and Human Services (HHS) has issued final omnibus regulations that incorporate legislative changes to the HIPAA privacy and data security rules from the 2009 HITECH law, as well as the Genetic Information Nondiscrimination Act of 2008 (GINA). We discussed the proposed HIPAA regulations in our Alert of July 14, 2010 and the GINA rules in the Alert of October 9, 2009.

Please join us for a related webcast presentation:

New HIPAA Privacy Requirements -
What’s In Store for Employer Health Plans and Their Business Associates
February 26, 2013
2:00 to 4:00 pm Central Time
Register Now

Changes to the rules will principally apply to healthcare providers, but will also impact employer group health plans. For example, the final rules impose enhanced obligations upon some subcontractors of plans’ business associates. Some plans will be required to modify their HIPAA business associate agreements and the privacy
notices they issue to enrollees.

A significant portion of the regulations don't directly impact group health plans. Rather, they address matters such as the prohibited sale of protected health information (PHI) and the use of PHI for marketing and fundraising purposes. We won't discuss any of those topics here.

We'll focus on changes to the contracting requirements that apply to a health plan's service providers, known as "business associates," as well as changes to the model HIPAA privacy notice and the breach notification requirements. The new rules are effective March 26, 2013 with a compliance date of September 23, 2013 for most of the new rules.

**Notification Requirements for Breaches of Unsecured PHI**

In August 2009, HHS issued interim regulations that require health plans to notify individuals if there is a breach of unsecured PHI maintained by a health plan or a business associate. Those interim rules defined a breach as instances when PHI was compromised only if there was a significant risk of harm to the individual.

In response to numerous comments submitted by privacy advocates, HHS concluded the risk of harm threshold was too subjective. Instead, HHS has now tightened the definition to presume that any impermissible acquisition, access, use, or disclosure of PHI is a breach unless the health plan or business associate demonstrates that there is a low probability that the protected health information has been compromised. For each potential breach, this new rule requires a formal risk assessment of at least the following factors:

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

Fortunately, the new rules exclude from the definition of "breach" unintentional or inadvertent disclosures of PHI to workforce members (e.g., a member of a health insurer's staff) or people authorized to access PHI where the information is not retained, used or further disclosed in violation of the HIPAA rules.

**So What Do We Mean by Unsecured PHI?**

HHS previously issued guidance that identifies two methods for securing PHI (rendering PHI "unreadable, unreadable or indecipherable" to unauthorized people). Prior guidance endorsed encryption as one such method (defined as use of an algorithmic process to transform data into a form where there is a low probability of assigning meaning without a confidential process or key). For disposing of PHI, the guidance recommends destruction in a manner consistent with guidelines recognized by the National Institute of Standards and Technologies.

**What Happens if There is a Breach of Unsecured PHI?**

The law requires that the health plan notify each affected individual within 60 days of discovery of a breach. If the breach is from a business associate, the business associate must notify the health plan when it knows of the breach. For purposes of this rule, the business associate is deemed to know of the breach on the first day it would have known of the breach by exercising reasonable diligence. Health plans are required to track
incidences of breaches and report them to HHS once a year.

The notification to individuals affected by a breach must be made by first class mail (or email if preferred by the individual) and must detail the following:

- The circumstances of the breach, including the date of the breach and date of discovery;
- The type of PHI involved;
- The steps people should take to protect themselves;
- The action taken by the health plan to mitigate any harm.

If the breach involves more than 500 individuals in a state or jurisdiction, the health plan must immediately notify HHS of the breach and provide notice to prominent media outlets serving the area, such as newspapers, radio, and television stations serving the area. Better yet, HHS publicly posts a list of health plans that are involved with breaches of more than 500 individuals. That information is available on HHS's "Wall of Shame" which may be accessed via this link.

**Requirements for Business Associates**

Prior to HITECH, the HIPAA rules did not directly apply to a health plan's business associates. Rather, the health plan was required to place business associates under contracts that compelled the business associates to maintain the confidentiality of the plan's PHI. Business associates were *contractually* liable to the plan if there was a breach but were not subject to direct oversight by the regulatory agency that enforces the HIPAA rules, HHS.

As a result of HITECH, the HIPAA privacy and security rules *directly* apply to business associates, as do HIPAA's civil and criminal penalties. Thus, business associates must develop formal policies and procedures to demonstrate compliance with the HIPAA rules, as well as designate their own privacy and security officials.

**HHS Pushes HIPAA Requirements Downstream**

Noting Congress's intent that HIPAA's protections should broadly apply, HHS has included a business associate's subcontractors in the definition of "business associate" under the final privacy and data security regulations. This means that the HIPAA confidentiality obligations and enforcement regime would extend to these subcontractors (even though they do not have a direct relationship to the health plan), to the extent that the subcontractors create, maintain or transmit PHI on behalf of the business associate.

For example, suppose a utilization review vendor (UR vendor) contracts with a self-funded plan's third party administrator. Under current law, the plan must place the third party administrator (TPA) under a business associate agreement with the plan (we might call the TPA a "direct" business associate, in that it has contracted for services directly with the plan). That agreement requires the TPA, to the extent it intends to share PHI with a subcontractor (such as the UR vendor) to obtain assurances from the subcontractor that it will keep the PHI just as confidential as the TPA is required to keep it. Under the current HITECH law, the TPA is subject to the HIPAA requirements and penalties to the same extent as the plan, but the subcontractor is not. In this example, the UR vendor's obligations are dictated solely by its agreement with the TPA. However, HHS's final regulations change that.

Under the final rules, the UR vendor would *also* be considered a business associate and, as such, required to comply with the privacy and security rules to the same extent as the health plan and its direct business associates, such as the TPA.
Fortunately under the final rule, it is the plan's direct business associate, not the health plan, that would be required to obtain a written contract from the subcontractor, under which the subcontractor acknowledges that it is subject to the same restrictions and conditions on the use of PHI that apply to the direct business associate. In other words, the direct business associate must enter into a contract with business associate subcontractors that handle PHI, in the same manner that health plans are required to enter into contracts with their business associates. The subcontractor would also, in turn, be required to obtain a written contract with any sub-subcontractor with whom it shared PHI.

According to HHS, an agent or other person who acts on behalf of the plan's business associate would be covered by HIPAA even if there is no formal contract between the business associate and the agent or other person. In the example above, then, the result would be the same even if the UR vendor did not have a formal written contract with the TPA; the UR vendor would nevertheless be considered a business associate and subject to all the rules that apply to business associates.

Because direct business associates are liable for HIPAA breaches by their subcontractors, business associates need to identify all agents and subcontractors with access to PHI and ensure there is a written agreement in place with appropriate indemnification language that protects the direct business associate in the event the subcontractor commits a HIPAA violation.

**Changes to Business Associate Agreements**

Going forward, HHS has made the following changes to its model business associate agreement provisions:

- Business associates must ensure that any agent or subcontractor that creates or receives PHI for the business associate agrees to the same restrictions and conditions that apply to the business associate with respect to the information described in the business associate agreement (see discussion above).
- Business associates must report breaches of unsecured PHI as required by the HHS regulations.
- If the business associate agrees to carry out a HIPAA privacy obligation of the health plan, such as distribution of the HIPAA privacy notice, then the business associate must comply with the HIPAA requirements and would be liable for failing to do so. However, the health plan itself remains directly liable to HHS for failing to meet the obligation.

Because of the new reporting requirements that apply directly to business associates, such as the requirement to report breaches of unsecured PHI, HHS has deleted the requirement that a health plan report to HHS when a termination of a business associate contract is not feasible.

Fortunately, a transition rule applies to health plans that have existing contracts in place with business associates or subcontractors as of January 25, 2013. Under this special rule, agreements that are in place prior to that date and are not renewed or modified between March 26 and September 23, 2013 would not have to be amended until September 23, 2014 (or, if the earlier, the date the agreement is renewed or modified on or after September 23, 2013).

As a practical matter, many business associate agreements entered into after 2009 already address these topics. This appears to moot the requirement for any amendments for compliant business associate agreements that automatically renew.

**Changes to Privacy Notice**

Health plans are required to distribute to covered employees a notice of the plan's privacy practices with respect to PHI. The notice must be distributed at enrollment and upon request thereafter. The notice must
be re-issued within 60 days after a material change to its contents. In any event, the responsible party must notify covered individuals every three years that the notice exists, and how they may obtain a copy. Many health plans include the notice in the initial and annual enrollment packets, a practice that we endorse.

HHS has made the following additions to the privacy notice1:

- A description of the types of disclosure that require an individual authorization, such as a release of PHI for sale, and marketing activities, or if the information that is released is psychotherapy notes.
- A statement that other uses and disclosures of PHI not mentioned in the privacy notice will only be made with the individual's authorization.
- A statement of the right to restrict disclosures of protected health information to a health plan where the individual pays out of pocket in full for the healthcare item or service (only applies to notices from health providers, not health plans).
- A statement of the obligation to notify affected individuals following a breach of unsecured PHI.

The current rules require that the plan issue a new privacy notice within 60 days of a material revision. Because the HHS-mandated changes to the privacy notice are "material," health plans that post the privacy notice on the plan's website must post a compliant notice by September 23, 2013. Coincident with the plan's next annual enrollment period after the effective date of final regulations, these plans must provide enrollees with a copy of the new notice or information about the change and how to obtain the revised notice.

Plans that do not post the privacy notice on the plan's website must provide the revised notice or information about the change and how to obtain the revised notice within 60 days of September 23, 2013 (i.e., by December 22, 2013).

To the extent that the plan's privacy notice already meets the regulations requirements, HHS has clarified that the plan is not required to revise and distribute another privacy notice on account of the final rules. This is good news for employers who have already updated their privacy notices in response to the proposed regulations issued in 2010.

**Individuals' Rights to Get Copies of Electronic PHI**

The final rules require health plans to provide copies of electronic PHI within 30 days to individuals who request copies.

**Right to Request Restriction**

Under HITECH, an individual can restrict disclosure of PHI for payment or healthcare operations when the person pays the provider the full out-of-pocket cost. If an individual reimburses the out-of-pocket expenses through an account-based plan, such as a health FSA, the individual may not restrict a disclosure necessary to effectuate that payment.

**GINA**

The final privacy rule incorporates changes required by GINA that prohibit health plans from using or disclosing genetic information for underwriting purposes, including health risk assessments under wellness programs. For a background on these rules, see our Alert of October 9, 2009. Long-term care plans are exempt from these rules.

**New Penalties for Noncompliance**
HITECH increased the penalties for noncompliance with the HIPAA privacy and data security requirements. As a reminder, the penalty amounts are:

- $100 per violation if the person does not know of the violation, up to $25,000 per year for identical violations;
- $1,000 per violation due to reasonable cause, up to $100,000 per year for identical violations;
- $10,000 per violation due to willful neglect that are corrected, up to $250,000 per year for identical violations; and
- $50,000 per violation due to willful neglect that are not corrected, up to $1.5 million per year for identical violations.

The final rules contain a list of mitigating and aggravating factors that HHS will weigh when it determines penalty amounts, such as:

- The number of individuals affected;
- The time period during which the violation occurred;
- The nature and extent of the harm resulting from the violation, including whether the violation caused physical harm, financial harm, reputational harm or hindered an individual's ability to obtain healthcare;
- The history of prior compliance or noncompliance with the HIPAA rules;
- Whether the health plan or business associate had financial difficulties that affected its ability to comply; and
- Whether the imposition of a civil money penalty would jeopardize the ability of the health plan or business associate to continue to provide, or to pay for, healthcare.

If HHS fails to act, the law allows State Attorneys General to bring civil lawsuits to enforce penalties.

Mark Holloway, J.D.
Health Reform Advisory Practice

1The rules also require healthcare providers who engage in fundraising to include a statement about an individual's right to opt out of receiving fundraising communications.

Not Legal Advice: Nothing in this Alert should be construed as legal advice. Lockton may not be considered your legal counsel and communications with Lockton’s Compliance Services group are not privileged under the attorney-client privilege.

Circular 230 Disclosure: To comply with regulations issued by the IRS concerning the provision of written advice regarding issues that concern or relate to federal tax liability, we are required to provide to you the following disclosure: Unless otherwise expressly reflected herein, any advice contained in this document (or any attachment to this document) that concerns federal tax issues is not written, offered or intended to be used, and cannot be used, by anyone for the purpose of avoiding federal tax penalties that may be imposed by the IRS.