SEYFARTH SHAW LLP
ATTORNEYS

Management Alert

Final HIPAA Regulations Issued

After much anticipation, the Department of Health and Human Services (HHS) has issued its omnibus set of final regulations modifying and clarifying the privacy, security and enforcement provisions under the Health Information Portability and Accountability Act (HIPAA). Although the final regulations will require group health plans to make some changes to remain in compliance with HIPAA, many of the changes may not come as a surprise because they were previously announced in proposed regulations or interim final regulations (IFRs). *[Click here to view prior alerts explaining this guidance.]* This alert focuses on changes to previous guidance.

Important Dates

Compliance Date. Group health plans and business associates must comply with the final regulations by **September 23, 2013.**

Transition Period for Agreements in Place as of January 25, 2013. Covered entities and business associates with HIPAA compliant business associate agreements (BAAs) in place as of January 25, 2013 (that are not renewed or modified between March 26, 2013 and September 23, 2013) will be deemed to comply with the new regulations for up to 12 months. The deemed compliance period ends the earlier of **September 22, 2014**, or the date the BAA is renewed or modified on or after September 23, 2013.

In addition, covered entities with data use agreements in place with recipients of limited data sets may continue to operate under existing agreements until the earlier of September 22, 2014, or the date the agreement is renewed or modified on or after September 23, 2013.

I. Rules for Business Associates

Background

Before the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the HIPAA privacy, security and enforcement rules did not apply directly to business associates, although many business associates had contractual obligations under a business associate agreement (BAA). HITECH provided that business associates were separately and directly liable for violations of the security rules for electronic PHI and for uses and disclosures of protected health information (PHI) that do not comply with the BAA or the HIPAA privacy rules. Proposed regulations suggested expanding the definition of business associate and modified the privacy, security and enforcement rules to apply to business associates.

Changes

The final rule substantially conforms to the proposed rules. Accordingly, the definition of business associate has been expanded to include: (i) health information organizations, e-prescribing gateways or other persons that provide data transmission services routinely for PHI; (ii) a person that offers personal health records on behalf of a covered entity; and (iii) a subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate. These business associates will need to implement policies and procedures to comply with the security rules.

New Requirements

Business Associates will have direct liability for:

1. Violations of the security rules.
2. Uses and disclosures of PHI that are not in accord with its BAA or the privacy rules.
3. Failing to disclose PHI to HHS when required.
4. Failing to disclose PHI as necessary to comply with an individual's request for an electronic copy.
5. Failing to make reasonable efforts to limit PHI to the minimum necessary.
6. Failing to enter into a BAA with subcontractors.

Under the final regulations, BAAs will be required to provide that the business associate will:

- Comply with the security rules with respect to electronic PHI;
- Ensure that any subcontractors agree to comply with the same restrictions and conditions that apply to the business associate;
- Report security incidents and breaches of unsecured PHI to the covered entity; and
- To the extent the business associate will carry out a covered entity's obligations under the privacy rule, comply with the requirements of the privacy rule that apply to the covered entity.

In addition, the final regulations recognize that a data use agreement may qualify as a business associate's satisfactory assurance that it will appropriately safeguard the covered entity's PHI when the PHI disclosed for a health care operations (HCO) purpose is a limited data set.

Covered entities will not need to enter into BAAs with the business associate's subcontractors. The business associates, however, will need to have BAAs with their subcontractors. On January 25, 2013, HHS published sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While the sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

II. Breach Notification Rules

Background

HITECH required covered entities to provide notification to affected individuals, to the Secretary of HHS, and in some cases, to the media following the discovery of a breach of unsecured PHI. The IFRs issued in 2009 defined a "breach" to mean "the acquisition, access, use, or disclosure of PHI in a manner not permitted [by the privacy rule] which compromises the security or privacy of the protected health information." The IFRs provided that whether an event "compromises the security or privacy of the protected health information" meant that it poses a significant risk of financial, reputation or other harm to the individual. In order to determine whether there was a significant harm to the individual, covered entities and business associates were required to perform a "risk assessment" considering a number of factors set forth in the rules. The IFRs contained three exceptions which had also been enumerated in HITECH.

New Requirements

Risk Assessment Factors:

1. What PHI was disclosed?
2. Who used or received the PHI?
3. Was the PHI actually viewed?
4. Did the covered entity or business associate take steps to mitigate the consequences of the use or disclosure?

Changes

1. Definition of Breach. The final regulations provide that an impermissible use or disclosure of PHI is **presumed to be a breach** unless the covered entity or business associate demonstrates that there is **a low probability that the PHI has been compromised** (or one of the exceptions to the definition of breach applies[1]).

2. Risk Assessment. Instead of assessing the risk of harm to the individual, covered entities and business associates must now assess the probability that the PHI has been compromised. The final regulations identify specific factors to consider, including:

[1]Both the IFRs and the final regulations include three exceptions which encompass situations which do not constitute breaches: (i) an unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further impermissible uses or disclosures; (ii) an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or BA to another authorized person; or (iii) a disclosure of PHI where a covered entity or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (*e.g.,* a list of diagnoses only vs. a list containing names or ID numbers as well);
- The unauthorized person who used the PHI or to whom the disclosure was made (*e.g.,* disclosure within the covered entity or to another covered entity vs. to a non-covered entity);
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated (*e.g.*, assurances such as through a confidentiality agreement were obtained that the recipient will not further use or disclose PHI).

If after evaluating all of the factors, a covered entity or business associate determines that there is a low probability that the PHI was compromised, breach notification is not required.

The final rules do not exempt disclosures between covered entities, or disclosures between a covered entity and a business associate. Each impermissible disclosure must be evaluated as to the probability that the PHI has been compromised based on the risk assessment using the listed factors. The fact that the recipient of a disclosure is a covered entity or business associate is one consideration with respect to assessing the risk. In addition, the exception for a limited data set has been removed and a risk assessment must be performed even if the impermissible use or disclosure involved only a limited data set.

3. Safe Harbor Remains Unchanged. As mentioned above, notice must be provided where there is a breach of unsecured PHI. If PHI is secured, notification is not required in the event of a breach of such information. In order to secure PHI, the information must be rendered unusable, unreadable or indecipherable to unauthorized individuals. Guidance issued by the Secretary of HHS lists encryption and destruction as the two technologies and methodologies for securing PHI.

4. Notice to HHS. The final regulations make it clear that for breaches of unsecured PHI involving less than 500 individuals, notice must be given to HHS within 60 days after the end of each calendar year for breaches discovered (not that occurred) during the preceding calendar year. This correction will be helpful where breaches occur during a calendar year but are not discovered until after the reporting deadline.

III. Marketing

Background

The HIPAA privacy rules require covered entities to obtain a valid authorization for any use or disclosure of PHI for marketing purposes. "Marketing" was defined as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. The following communications, however, were permitted to be made without an authorization:

- Group health plan communications related to its covered health-related products or services;
- Communications made for treatment of an individual; or
- Communications for case management or care coordination for an individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

HITECH provided that marketing communications are impermissible if the covered entity receives payment in exchange for making the communication. The proposed regulations revised the definition of marketing by excluding: (i) communications regarding prescription refills if remuneration was related to the cost of making the communication, (ii) communications to describe health related products or services under a plan, as long as no financial remuneration was received in exchange for making this communication, and (iii) written communications from a health care provider for treatment of an individual as long as certain notice and opt out conditions were satisfied if the provider received financial remuneration.

New Requirements

Privacy Notices will have to:

1. Inform individuals that they will be notified in case of a breach of their unsecured PHI.
2. Explain that an authorization is required before any use or disclosure of psychotherapy notes; use or disclosure of PHI for marketing purposes where a third party receives compensation; and/or sale of PHI.
3. If a health plan will use or disclose PHI for underwriting purposes, include a statement that genetic information will not be used for such purposes.
4. If a health plan will use or disclose PHI for fundraising, include a statement that an individual may opt out of receiving related communications.
5. Contain a statement that the plan must agree to restrictions on disclosures of PHI relating to an item or service for which the individual paid for in full out of pocket.

Changes

The final regulations require authorizations for all treatment and HCO communications where the covered entity receives financial remuneration from a third party whose product or service is being marketed. According to the final regulations, marketing does not include:

- Prescription refill reminders, provided that the covered entity's financial remuneration is reasonably related to the covered entity's cost of making the communication;
- **Except where the covered entity receives financial remuneration**, communications made:
  - → by a provider for the treatment of an individual;
  - → by a plan to describe a health-related product or service under the plan, including communications about participating network providers, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan enrollees that add value to but are not part of the benefit plan, or
  - → by a provider or a plan for case management or care coordination, like treatment alternatives, to the extent the activities do not fall within the definition of treatment.

IV. Genetic Information

Background

The Genetic Information Non-Discrimination Act of 2008 (GINA) prohibited discrimination based on an individual's genetic information in both health coverage and employment contexts. In addition, GINA contained privacy protections for genetic information and required the Secretary of HHS to revise the privacy rules to clarify that genetic information is health information and to prohibit group health plans and insurance issuers from using or disclosing genetic information for underwriting purposes. Proposed regulations issued in 2009 added various definitions to HIPAA and a prohibition on health plans using or disclosing PHI that is genetic information for "underwriting purposes" even if the individual signs an authorization.

Changes

1. Underwriting Purposes. HIPAA allows covered entities and business associates to use or disclose PHI for HCO. As defined, HCO includes underwriting activities, which means that PHI can typically be used for underwriting. The final regulations add a definition of "underwriting purposes" that provides a health plan may not use or disclose PHI that is genetic information for underwriting purposes. For these purposes, "underwriting purposes" means:

- Rules for determining eligibility or benefits under a plan (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment (HRA) or participating in a wellness program);
- The computation of premium or contribution amounts under the plan (including discounts, rebates, or premium differential mechanisms in return for activities such as completing an HRA or participating in a wellness program);
- The application of any pre-existing condition exclusion under the plan; and
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

The final regulations allow health plans to continue to provide incentives for completing HRAs or for participating in wellness programs in manners that do not involve the disclosure of genetic information. For example, information about an individual's use of tobacco, alcohol and drug use is not genetic information and thus, may be used by health plans for underwriting purposes. Further, the DOL has issued guidance which makes clear that plans may continue to collect family health history through the use of HRAs that are not tied to any reward.

2. Long-Term Care Plans. Although the nondiscrimination provisions of GINA do not apply to excepted benefits, the final regulations apply the prohibition on using and disclosing PHI that is genetic information for underwriting to all health plans that are subject to the privacy rules, except long-term care policies. Notably, although long-term care plans are not subject to the underwriting prohibitions, they are bound by the other privacy rules and must protect genetic information from improper uses and disclosures.

To-Do List

1. By the compliance date, covered entities should update their privacy policies and procedures to reflect the new regulations, including GINA's prohibition on using genetic information for underwriting purposes, the new definition of marketing, when an authorization is required, the new definition of breach of unsecured PHI and the new risk assessment procedures.

2. Within a reasonable period of time after the compliance date, covered entities should retrain their workforce members on the updated policies and procedures. Although business associates are only required by law to train their workforce on the security rules, they are contractually obligated to comply with the HIPAA privacy rules and, as a practical matter, should also train their workforce on the privacy rules.

3. By the compliance date, covered entities should revise their privacy notices as indicated above. Revised notices must be posted on a health plan's website by the effective date of the revisions and provided to covered individuals in the next annual mailing. If a plan does not maintain a website, revised notices must be provided (or information as to how to obtain a revised notice) to covered individuals within 60 days of the revision.

4. Covered entities should identify their business associates and make sure BAAs are in place. For those business associates who do not have agreements, covered entities will need to enter into new BAAs containing the new provisions by September 23, 2013. For those BAAs currently in effect, update the existing BAAs for changes prompted by these final rules by the end of the transition period.

5. Business associates should identify their subcontractors and enter into BAAs with them.

6. Covered entities and business associates who have unsecured PHI should consider taking advantage of the safe harbor to secure as much PHI as posible, thus potentially avoiding the breach notification requirements.

7. By the compliance date, covered entities and business associates should implement new risk assessment procedures, and ensure that all assessments are properly documented.

By: *Joy Sellstrom* and *Nicole Bogard*

Joy Sellstrom is senior counsel *Nicole Bogard* is a partner in Seyfarth's Employee Benefits & Executive Compensation practice group. If you would like further information, please contact your Seyfarth attorney, Joy Sellstrom at *jsellstrom@seyfarth.com* or Nicole Bogard at *nbogard@seyfarth.com*.