New Rules, New Notices, New Agreements—Final HIPAA/HITECH Act Regulations Require Action by Employer-Sponsored Group Health Plans

March 2013

Self-insured employer group health plans must revise HIPAA Notices of Privacy Practices (HIPAA Notices), amend business associate agreements, and make changes to their HIPAA data security and privacy practices under final regulations issued by the Department of Health and Human Services (HHS) on January 25, 2013. The final HIPAA/HITECH Act1 regulations will have the greatest impact on self-insured employer group health plans that are covered entities under HIPAA and their employer plan sponsors, while responsibility for HIPAA compliance for fully insured group health plans will fall on the health insurance issuer or health maintenance organization (HMO).

This Aon Hewitt bulletin discusses the final HIPAA/HITECH Act regulations, which:

- Lower the standard for determining whether a breach of unsecured protected health information (PHI) has occurred, thereby increasing the possibility that a health plan will have to issue a notice of the breach;
- Identify new provisions that must be included in business associate agreements under the final regulations, which make business associates and their subcontractors directly liable for noncompliance with the HIPAA data security regulation (Security Rule) and portions of the HIPAA privacy regulation (Privacy Rule);
- Require that health plans add new disclosures to their HIPAA Notices and distribute the revised HIPAA Notices or a summary of the changes;
- Modify the requirements for obtaining individual authorizations as a pre-condition for certain marketing communications and the sale of PHI by a health plan; and
- Require health plans to provide copies of electronically maintained PHI to individuals upon request in the electronic form and format requested.

Compliance with the final regulations is required by September 23, 2013, except that health plans have until September 22, 2014, to amend certain business associate agreements under a transitional compliance rule. Health plans that fail to comply with the final regulations by the applicable compliance date may be subject to HHS’s enforcement efforts and the new tiered civil money penalty scheme established by the HITECH Act.

Due to the broad scope of the final regulations, the significance of the guidance, the relatively short time period allowed for health plans to become fully compliant, and the enhanced civil money penalties for noncompliance, health plans and their plan sponsors need to promptly undertake the following activities:

- Review and amend business associate agreements;

---

1 Health Information Technology for Economic and Clinical Health (HITECH) Act
Re-visit previous HIPAA data security risk assessments;
Review and update the health plan’s HIPAA privacy and security policies and procedures;
Modify the health plan’s unsecured PHI breach identification and notification policies and procedures;
Revise and disseminate the health plan’s HIPAA Notice or the changes to the HIPAA Notice; and
Update the health plan’s HIPAA privacy and data security training materials, and conduct supplemental HIPAA training.

Lower Standard Applies for Determining a HIPAA Breach

The final regulations apply a lower standard for determining whether a breach of a health plan’s unsecured PHI has occurred. In the event of the discovery of a breach of unsecured PHI, the HITECH Act requires that a health plan provide notification to affected individuals, HHS, and in some instances, the public media. “Unsecured PHI” is PHI that has not been encrypted or destroyed so as to render it unusable, unreadable, or indecipherable to unauthorized individuals. The HITECH Act also requires business associates to notify the applicable health plan after the business associate’s discovery of a “breach” of the health plan’s unsecured PHI.

Effective for data security incidents occurring on or after September 23, 2013, the final regulations lower the standard for determining whether a breach has occurred by replacing the previous standard, which required a “significant risk of harm to an individual,” with a new standard that essentially places the burden of proof on the health plan or issuer. The final regulations presume that an unauthorized acquisition, access, use, or disclosure of PHI is a breach unless the health plan or business associate, as applicable, demonstrates that there is a “low probability the PHI has been compromised.” The required demonstration must be based on a risk assessment of at least four specified factors:

- The nature and extent of the PHI involved, including the types of identifiers and 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.

According to HHS, health plans and business associates must address each of the factors listed above separately when evaluating the probability of whether PHI has been compromised, along with other factors when necessary. Health plans and business associates must then analyze the overall probability that the PHI has been compromised by considering all four factors in combination. If a health plan’s or business associate’s evaluation of these factors shows there is a low probability that PHI has been compromised, no breach notification is required.

A risk assessment must be performed following an impermissible use or disclosure of PHI unless the data security incident falls within one of the enumerated exceptions to the definition of a breach or the incident involved “secured PHI” (i.e., PHI that has been encrypted or destroyed so as to render it unusable, unreadable, or indecipherable to unauthorized individuals). HHS expects that the risk assessment performed by the health plan or business associate, as applicable, will be thorough, completed in good faith, and reach reasonable conclusions. Moreover, HHS expects that the risk assessment will be
documented sufficiently to enable the health plan or business associate to show that there is a low probability the PHI was compromised.

**Significant Changes Impacting Business Associates**

The final regulations made a number of significant modifications to the Privacy Rule and the Security Rule that affect: the determination of what entities or persons are business associates; the HIPAA compliance obligations of business associates; and the content of business associate agreements.

**Expanded Definition of a “Business Associate”**

The final regulations expand the definition of “business associate” to include a business associate’s subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate. A subcontractor is a person or entity to which a business associate delegates a function, activity, or service other than in the capacity of a member of the business associate’s workforce. HHS emphasized in the preamble that the classification of subcontractors as business associates is intended to apply “down the chain” of subcontractors (i.e., to multiple tiers of subcontractors) as far as the PHI flows so that an individual’s PHI remains adequately protected by all parties that have access to the PHI to perform functions, activities, or services on behalf of the health plan.

The final regulations further expand the definition of “business associate” to encompass: 1) a health information organization, an e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a health plan and requires access to such PHI on a routine basis; and 2) a person that offers a personal health record to one or more individuals on behalf of a health plan.

The final regulations also added the word “maintain” to the “business associate” definition to clarify that an entity (e.g., a paper or electronic/digital health record storage firm) that “maintains” PHI on behalf of a health plan may be a business associate even if the entity does not view the PHI or only views such PHI on a random or infrequent basis.

**Direct Liability of Business Associate for Compliance**

The final regulations apply the Security Rule’s administrative, physical, and technical safeguard standards, as well as the Security Rule’s policy and procedure requirements, and select portions of the Privacy Rule to business associates in the same manner that they apply to a health plan. A business associate that fails to comply with these Security Rule standards and Privacy Rule provisions will be subject to direct liability under the HIPAA/HITECH Act civil and criminal enforcement rules.

**Business Associate Agreements With Subcontractors Now Required**

The final regulations provide that a business associate may only permit a subcontractor to create, receive, transmit, or maintain PHI on its behalf if the business associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the PHI. Such assurances must be in the form of a business associate agreement between the business associate and the subcontractor (and not between the health plan and the subcontractor).
New Business Associate Agreement Content Requirements

Under the final regulations, business associate agreements, including agreements between business associates and their subcontractors, must include new covenants providing that the business associate will:

- Use appropriate safeguards and comply with the applicable provisions of the Security Rule (i.e., the applicable administrative, physical, and technical safeguards, and policy and procedure requirements of the Security Rule) to protect electronic PHI;
- Ensure that any subcontractor it engages to create, receive, maintain, or transmit PHI on its behalf agrees, by entering into a business associate agreement, to comply with the same conditions and restrictions under the Security Rule and the Privacy Rule that apply to the business associate with respect to the protection of PHI;
- Report to the health plan any use or disclosure of PHI not permitted under the terms of the business associate agreement of which it becomes aware (including any data security incident or breach of unsecured PHI); and
- To the extent the business associate is to carry out a health plan’s obligations under the Privacy Rule (e.g., provide an accounting of PHI disclosures to an individual upon request), comply with the Privacy Rule requirements that would apply to the health plan in the performance of those obligations.

HHS posted updated sample business associate agreement provisions which reflect these new requirements on its website on January 25, 2013.

Transitional Compliance Rule for Business Associate Agreements

The final regulations provide a transitional compliance rule for business associate agreements that applies only to those health plans (with respect to their business associates) or business associates (with respect to their subcontractors) that: 1) prior to January 25, 2013, had entered into and were operating under a written contract or other arrangement which complied with HIPAA’s business associate agreement requirements then in effect; and 2) the contract or other arrangement is not renewed or modified from March 26, 2013 until September 23, 2013. Contracts or other arrangements that meet these conditions will be deemed compliant with the final regulations until the earlier of: 1) the date the contract or other arrangement is modified or renewed on or after September 23, 2013; or 2) September 22, 2014.

HIPAA Notices—New Content and Distribution Rules

The final regulations require that health plans include statements in their HIPAA Notices that indicate that receipt of a written authorization from the individual is a pre-condition for most uses and disclosures of psychotherapy notes (when such notes are maintained by the health plan), uses and disclosures of PHI for marketing purposes, and disclosures that constitute the sale of PHI. Additionally, the final regulations require that a health plan’s HIPAA Notice state that: 1) the health plan is prohibited from using or disclosing an individual’s PHI which is genetic information for underwriting purposes; and 2) the health plan is required to notify affected individuals following a breach of unsecured PHI.

HHS states in the preamble that the additions to a health plan’s HIPAA Notice required by the final regulations represent material changes. The Privacy Rule, as currently in effect, requires that a materially
changed HIPAA Notice be distributed within 60 days after the changes are made to all individuals then covered by the health plan. For those health plans that have previously posted their HIPAA Notice on a qualifying website, the final regulations replace the current 60-day distribution requirement with a new distribution rule under which the health plan is expected to: 1) prominently post its materially changed HIPAA Notice or a description of the change on its website by the effective date of the material change; and 2) provide the materially changed HIPAA Notice or information about the material change and how to obtain the revised HIPAA Notice in its next annual mailing to individuals then covered by the health plan (e.g., in annual enrollment materials).

**Authorizations—New Rules Involving Marketing and Sales of PHI**

The Privacy Rule generally conditions the use or disclosure of PHI for purposes of “marketing” on receipt of an individual’s authorization. The final regulations make two noteworthy modifications to the Privacy Rule’s definition of “marketing” that change the circumstances in which an authorization will be required as a pre-condition for certain marketing-related communications. As a result of those modifications:

- Refill reminders or other communications about a drug or biologic currently prescribed for the individual *will not* constitute “marketing” (and therefore will be exempt from the Privacy Rule’s authorization requirement) if the financial remuneration received (if any) by the health plan from a third party in exchange for making the communication is reasonably related to the health plan’s cost of making the communication.
- Communications for purposes of treatment or health care operations that fall into one of three categories will be excluded from the definition of “marketing” (and therefore will be exempt from the Privacy Rule’s authorization requirement) only if the health plan does not receive any financial remuneration in exchange for making the communications. The three categories are: 1) communications pertaining to the treatment of an individual by a health care provider; 2) communications to describe a health-related product or service (or payment for the product or service) that is provided by the health plan making the communication; and 3) communications for case management or care coordination to the extent not considered treatment.

The final regulations also prohibit the disclosure of an individual’s PHI by a health plan or business associate that constitutes a “sale of PHI” unless an authorization has been obtained which expressly states that the disclosure will result in remuneration to the health plan. For purposes of the new prohibition, the “sale of PHI” is defined as a disclosure of PHI by a health plan or business associate for which the health plan or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

**Expansion of Individual Rights—Access to PHI in Electronic Form**

The final regulations modify the PHI access rule for individuals to require a health plan that maintains PHI electronically in a designated record set to provide an individual, upon request, with access to the individual's PHI in the electronic form and format requested if it is readily producible in that form and format. Otherwise, the health plan will be required to provide access to the PHI in a readable electronic format. Otherwise, the health plan will be required to provide access to the PHI in a readable electronic format.

---

2 A “designated record set” in the health plan context is a group of records (i.e., items, a collection, or grouping of information that includes PHI which is maintained, collected, used, or disseminated by or for a health plan) that is: 1) the health plan’s enrollment, payment, or claims adjudication record system; or 2) used by the health plan to make decisions about individuals.
form and format agreed to by the requesting individual. HHS’s expectation is that the electronic copy of the PHI will be digital information provided in a machine readable standard format (e.g., Microsoft Word or Excel, text, HTML, or PDF) that can be processed and analyzed on the recipient’s computer.

If the individual’s PHI access request directs the health plan to transmit a copy of the PHI (whether in paper or electronic form) directly to another designated person, the health plan must comply with the request, provided that the individual’s request: 1) is in writing and signed by the individual; and 2) clearly identifies the designated person and where to send the copy of the PHI.

A covered entity will be allowed to include in its cost-based fee for providing the electronic PHI the cost of electronic media (e.g., a compact disc (CD) or universal serial bus (USB) flash drive) if the individual requests that the PHI be provided on portable media.

Resources


The HHS sample business associate agreement provisions are available at: http://hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Aon Hewitt’s bulletin on the final regulations’ guidance regarding the protection of genetic information that is PHI is available at: http://img.en25.com/Web/AonHewitt/HIPAA2.pdf


For additional information regarding the final regulations, please contact your Aon Hewitt Legal Consultant.
About Aon Hewitt

Aon Hewitt is the global leader in human resource solutions. The company partners with organizations to solve their most complex benefits, talent and related financial challenges, and improve business performance. Aon Hewitt designs, implements, communicates and administers a wide range of human capital, retirement, investment management, health care, compensation and talent management strategies. With more than 29,000 professionals in 90 countries, Aon Hewitt makes the world a better place to work for clients and their employees. For more information on Aon Hewitt, please visit www.aonhewitt.com.