buckconsultants

xerox

FYI®
For Your Information®

Volume 36 | Issue 19 | March 8, 2013

The wait is over…HHS releases final omnibus HIPAA privacy and security regulations

The Department of Health and Human Services (HHS) published long-anticipated (and long-overdue) omnibus regulations under HIPAA on January 25, 2013. The final rules respond to public comments and implement requirements from HIPAA's privacy, security, enforcement, and breach notification requirements. For example, the rules impose direct liability on business associates for compliance with certain privacy and security rules, expand the definition of business associates to include subcontractors, and significantly alter the standard for determining a breach of unsecured protected health information. In addition, individual rights and protections are clarified. The revisions require prompt action by covered entities (including group health plans) and their business associates to be in compliance by September 23, 2013 (there is an additional grace period for certain provisions).

A long road to the final rules

The Health Insurance Portability and Accountability Act's (HIPAA's) privacy and security rules — the "administrative simplification" requirements — were first announced in 1996. Since then, several rounds of regulations and guidance addressed the safeguards required for an individual's protected health information (PHI).

- The privacy and security rules provided the basic structure of how covered entities (health providers, group health plans, and health data clearinghouses) must protect PHI in all formats.
- The Health Information Technology for Economic and Clinical Health (HITECH) Act extended certain HIPAA provisions and penalties to covered entities' business associates (e.g., third party administrators, contractors, subcontractors, and other vendors), added new breach notification requirements and individual privacy rights, and strengthened enforcement with significantly increased civil monetary penalties for HIPAA violations. (See our April 27, 2009 *For Your Information*.)

- The Genetic Information Nondiscrimination Act of 2008 (GINA) imposed certain privacy requirements in connection with the use of genetic information. (See our October 15, 2009 *For Your Information*.)

- Proposed regulations published in 2011 would have modified the rules regarding the accounting of disclosure of PHI and permit individuals to receive a report showing who accessed their PHI. (See our July 8, 2011 *For Your Information*.)

The omnibus regulations pull together several of these past regulations and create a consolidated set of final rules for covered entities and their business associates to follow. However, the omnibus rules do not appear to include 2011 proposed regulations on accounting of disclosures and an individual's right to receive an access report. Regulators comment that additional guidance on that topic is forthcoming.

While the final rules generally adopt the contents of the remaining prior guidance, that is not the case in all provisions. Covered entities generally must comply with the new rules by September 23, 2013. In some cases, a special transition rule exists for executing revised business associate agreements. This article provides an analysis of the most significant changes in the final rules and a checklist of employer action items.

Changes affecting business associates

"Business associates" are generally entities or people performing activities that involve use or disclosure of PHI for or on behalf of a covered entity. The omnibus rules include several provisions that apply to business associates and covered entities that enter into agreements with them. Specifically, the omnibus rules revise the definition of business associate and increase business associate compliance liability requiring changes to business associate agreements (BAAs).

Definition

A business associate now includes the following additional entities:

- Patient safety organizations that receive reports of patient safety events or concerns from providers and provide analysis of events to reporting providers

- Health information organizations (HIOs), e-prescribing gateways, and other organizations that transmit PHI to a covered entity (or business associate) and that require access to PHI on a routine basis (mere "conduits" that provide courier services such as the US Postal Service, United Parcel Service, or their electronic equivalents are deemed not to have "routine access" and are excepted from the definition of business associate)

- Data storage companies (whether digital, cloud, or hard copy) that maintain PHI, regardless of whether they require regular direct access

- Entities that offer personal health records (PHRs) to individuals on behalf of a covered entity

- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate

Whether an entity is a business associate is role and activity based, i.e., if it creates, receives, maintains, or transmits PHI on behalf of the covered entity. The omnibus rules describe some entities that would not be considered business associates, e.g., plan sponsors receiving PHI from a group health plan and health care providers receiving treatment-related PHI from a covered entity.

> Buck Comment. Covered entities should confirm which entities it considers business associates and refine that determination to reflect the omnibus rule.

Compliance liability and BAAs

Covered entities are required to enter into agreements with their business associates specifying the permitted uses and disclosures of PHI and assigning appropriate obligations and liability to the parties. The omnibus regulations confirm the HITECH Act's extension of direct liability for compliance with certain HIPAA provisions to business associates, such as impermissible uses and disclosures and failure to:

- Provide a breach notification to the covered entity
- Provide access to a copy of electronic PHI
- Disclose PHI where required by HHS to investigate or determine compliance with HIPAA
- Provide an accounting of disclosures
- Comply with the requirements of the security rule

Noncompliance with those rules could subject the business associate to civil and criminal penalties.

Subcontractors. These obligations and the potential liability extend to subcontractors, although the covered entity is not required to enter a direct contract with the subcontractor to establish the business associate relationship. A business associate must have a written agreement with its subcontractor containing satisfactory assurances that the subcontractor will comply with applicable provisions of the privacy and security rules. A business associate that is aware of noncompliance by its subcontractor must respond in the same manner as a covered entity would respond to noncompliance by its business associate, either by taking reasonable steps to cure the breach or by terminating the contract.

Business associate agreements. Changes in the obligations and liability of business associates must be reflected in BAAs. HHS has provided sample BAA language, but notes that its use is not required for compliance and may be

Common business associates

Insurers and HMOs covered by ASO agreements to provide claims processing and medical management decisions

Third party vendors (e.g., COBRA, disease management, utilization review)

Lawyers

Consultants and actuaries

Pharmacy benefit managers

Accountants

Patient safety organizations

Data storage companies (digital or hard copy)

Persons offering PHRs

Data aggregators

HIOs, e-prescribing gateways, and entities transmitting and routinely accessing PHI

changed to reflect the business relationship between the parties accurately. Among other things, BAAs must now state that business associates will:

- Comply with HIPAA's security rule. This means establishing administrative, technical, and physical safeguards to protect electronic PHI (e.g., performing a risk analysis, periodically reassessing and updating security protections, and implementing reasonable and appropriate security policies and procedures)
- Comply with the HITECH Act's privacy provisions (e.g., account for disclosures, follow minimum necessary rule, comply with revised sales and marketing rules)
- Comply with the HIPAA privacy rule to the same extent as the covered entity when carrying out a covered entity's HIPAA obligation
- Report breaches of unsecured PHI to covered entities
- Ensure that subcontractors that create or receive PHI on behalf of a business associate agree to the same restrictions with respect to PHI that apply to the business associate

The parties may wish to add language regarding responsibilities for breach notification and responses to requests received directly from covered individuals.

As noted above, most of the provisions in the omnibus rule are effective on September 23, 2013. However, the regulations provide a transition period for covered entities and business associates to amend their agreements to comply with the new requirements. The transition rule states that existing HIPAA-compliant agreements have up to an extra year to revise their agreements (see table below). But, while the parties will have additional time to conform their agreements, they must be in compliance with all other HIPAA requirements as of September 23, 2013.

Status of business associate agreement	Actions	Compliance date
HIPAA-compliant agreement in effect before 1/25/2013	Renewed or modified on or after 1/25/2013 and before 3/26/2013	If "evergreen" or automatically renewed (i.e., no changes), no later than 9/22/2014 Otherwise unclear; conservatively, by 9/23/2013
HIPAA-compliant agreement in effect before 1/25/2013	Renewed or modified on or after 3/26/2013 and before 9/23/2013	9/23/2013
HIPAA-compliant agreement in effect before 1/25/2013	Renewed or modified on or after 9/23/2013	Earlier of renewal/modification date or 9/22/2014
New agreement executed in 2013 but before 9/23/2013		9/23/2013
HIPAA-compliant agreement in effect before 1/25/2013	Renewed or modified on or after 1/25/2013 and before 3/26/2013	If "evergreen" or automatically renewed (i.e., no changes), no later than 9/22/2014 Otherwise unclear; conservatively, by 9/23/2013
New agreement executed on or after 9/23/2013		Effective date of agreement

Buck Comment. Business associates will need to negotiate and execute the necessary agreements with their subcontractors as soon as possible to meet the September 2013 compliance date.

Notice of privacy practices (NPP)

Covered entities are required to maintain and distribute a notice that describes their HIPAA privacy practices, including uses and disclosures of PHI, and informs people of their individual rights. Group health plans are required to give this notice of privacy practice (NPP) to all new plan enrollees and anyone else requesting it. A reminder notice is required every three years. The required modifications to a plan's NPP include:

- A description of the uses and disclosures of PHI that require an authorization (e.g., use of psychotherapy notes, disclosure of PHI for marketing, and disclosures that constitute a sale of PHI)
- A statement regarding the covered entity's use of PHI for fundraising purposes and the individual's right to opt out of receiving such communications
- A statement that the covered entity is not permitted to use genetic information for underwriting purposes
- A statement regarding the covered entity's obligations to maintain the privacy of an individual's PHI and of the individual's right to receive notification in the event of a breach

If the covered entity is a provider, the NPP must also state that the individual has the right to restrict disclosures of PHI to a health plan if the PHI relates to services for which the individual has paid the provider in full. Notices must be revised by the September 23, 2013 compliance date. HHS has not provided templates or model NPPs, noting that each NPP will vary based on the requirements of the covered entity. In an attempt to balance an individual's right to receive information and the administrative burden on the covered entity, the regulations provide some flexibility in distributing the revised notice. A health plan that currently posts its NPP on its web site must:

- Prominently post the material change or the revised notice on its web site by September 23, 2013
- Provide the revised notice (or information about the material change and how to obtain the revised notice) in its next annual mailing to covered individuals (e.g., open enrollment)

If the health plan does not post the NPP on its web site, it must provide the revised NPP (or information about the material changes and how to get the full NPP) within 60 days of the material revision to the notice.

Buck Comment. Plan sponsors should review their current NPPs and make necessary revisions as soon as possible. In addition, they will need to coordinate with any insured plans or HMOs to ensure that all NPPs are provided on a timely basis.

Individual rights

The HIPAA rule provides certain rights to the individuals for whom the PHI relates (for most group health plans, this means the plan participants). The final regulations expand or change some of these individual rights:

- **Access to electronic records.** HIPAA allows individuals to review or get copies of their PHI when it is part of a "designated record set." The HITECH Act allows people to ask for *electronic* copies of their PHI contained in electronic health records or to request in writing or electronically that another person receive an electronic copy of these records. The final omnibus rules expand an individual's right to access

electronic records or to direct that they be sent to another person to include not only electronic health records but also any records in one or more designated record sets. If the individual requests an electronic copy, it must be provided in the format requested or in a mutually agreed-upon format. Covered entities may charge individuals for the cost of any electronic media (such as a USB flash drive) used to provide a copy of the electronic PHI.

- **Restricted disclosures**. An individual may request that PHI concerning a health care item or service for which the individual has paid the covered entity in full not be disclosed to a health plan for payment, or health care operations. Unlike other requests for restricting otherwise permitted disclosures, the covered entity must honor the restriction regardless of who pays for the item or service (e.g., plan participant, participant's family or friend). The commentary to the final regulations noted that an individual may request this restriction even if using a flexible spending account or health savings account to pay for the services, i.e., disclosure may not be made to another health plan. However, the individual cannot restrict disclosure of information necessary to make the payment.
- **Decedent's PHI.** Generally, the use and disclosure of a decedent's PHI is subject to the same protections as that of a living person. Thus, if an authorization for disclosure is required, it must be obtained from the decedent's personal representative (i.e., executor, administrator, or other person who has authority under applicable law to act on behalf of the decedent or the decedent's estate). The final regulations reflect the changes made by the HITECH Act:
    - The general privacy protections noted above need only be provided for a period of 50 years from the date of death.
    - The rules permit (but don't require) covered entities to disclose a decedent's PHI to a family member or close personal friend who was involved in the individual's care or payment for care prior to the individual's death. However, this permissible disclosure doesn't apply if the covered entity is aware that the decedent wouldn't have wanted the disclosure.
- **Proof of immunization**. The final omnibus regulations provide that covered entities may disclose proof of immunization to a school when legally required for attendance. No HIPAA authorization is required, but the covered entity must receive permission from the adult student, parent or guardian of a child, or other person acting on the student's behalf. The final rules add that permission could be provided orally. The covered entity must document that permission was received.

Genetic information

GINA prohibits discrimination in employment or health coverage based on an individual's genetic information. Under Title I of GINA, a group health plan cannot base premium rates or program eligibility on genetic information, and it is limited in its ability to collect such information or require an individual to provide it. In addition to its nondiscrimination rules, GINA includes new privacy protections under HIPAA. HHS issued proposed regulations in October 2009 to implement those rules. The final rules implement the modifications required by GINA by:

- Including genetic information in the definition of health information
- Adding other GINA defined terms, such as "family members," "genetic information," and "genetic services"
- Prohibiting the use of genetic information for underwriting purposes by all health plans and health plan issuers, except for issuers of long-term care policies; underwriting purposes is broadly defined to include:

- Rules governing eligibility, benefits determination, or coverage under the plan
- Calculations of premium or contribution amounts, including discounts or incentives for participation in health promotion activities
- Application of any pre-existing condition exclusion under the plan or policy
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits

As noted above, the plan must include a statement in its NPP regarding the prohibition against the use of genetic information for underwriting purposes.

Use and disclosure of PHI coupled with financial remuneration

HIPAA generally provides that covered entities and business associates only use or disclose PHI if they have a valid HIPAA authorization. However, HIPAA also contains exceptions to that general rule and allows certain uses or disclosures without an authorization if they meet specific standards. For instance, group health plans can use or disclose PHI for treatment, payment, and health care operations without needing an authorization. The final omnibus regulations generally require an individual's authorization for the use or disclosure of PHI when the covered entity receives direct or indirect financial remuneration in exchange for the information. The rules impose new limits on the use of PHI for marketing and fundraising and create a definition of what constitutes a sale of PHI.

Marketing

An individual's authorization is required for the use or disclosure of PHI for marketing purposes. Marketing is defined as any communication about a product or service that encourages the recipient to purchase the product or use the service. The final rules remove the prior exception that permitted communications in connection with health care operations and require an authorization if the covered entity received any financial remuneration for making the communication. However, there are several exceptions to the broad marketing definition that the final omnibus rules clarify, including:

- Refill reminders or other communications about a drug or biological that the individual is currently taking, so long as the covered entity is only paid to cover the communication costs. Communications about generic equivalents, adherence to properly taking medications, and information on self-administered drugs are also excepted. The regulators note that additional guidance may be forthcoming on this exception
- Descriptions of a health-related product or service to a health plan enrollee, so long as the covered entity isn't paid for providing the description (e.g., a change to the plan, provider network, or items only offered to plan enrollees)
- Communication promoting general health such as a healthy diet or encouraging routine diagnostic tests (e.g., annual mammograms)
- Communication about government and government-sponsored programs

- Communication about treatments and health care operations and recommendations of alternative treatments, providers, and therapies, provided certain conditions are met
- Case management and care coordination where no financial remuneration is given to the covered entity in exchange for a communication

Fundraising

The privacy rules permit a covered entity to use certain PHI in fundraising activities without receiving an authorization from the individual, provided that the entity's notice of privacy practices includes a statement indicating that the entity may contact the individual for that purpose. The final rules expand the type of information that may be used or disclosed to include not only demographic information, health insurance status, and date(s) of service, but also information about the department and provider of service and treatment outcomes. However, the final rules now require that the covered entity provide information regarding the individual's ability to opt out of current and future fundraising activities. In addition, the method of opting out must not be burdensome, may not involve more than a nominal cost, and may not condition treatment or payment on the decision to opt out. The entity may also provide a method for the individual to opt back in, if he or she chooses.

Sale

The final omnibus rules restate that the sale of PHI without an individual's authorization is not permitted. The authorization must note that the covered entity receives payment in return for the disclosure. Sale is a disclosure of PHI where the covered entity or business associate receives direct or indirect remuneration in exchange for the information. The definition of sale is not limited to the transfer of ownership of the data – it can include license, access, or use agreements. Exceptions to the definition include disclosures for public health and certain research purposes — where the only remuneration is the cost of preparing or handling the PHI— to carry out an individual's treatment, to provide health care payments, to satisfy legal requirements, and in connection with the sale or transfer of the covered entity.

Enforcement

HHS actively stepped up its HIPAA enforcement activities in 2011 (see our March 22, 2011 *For Your Information*) and 2012 (see our July 2, 2012 *For Your Information*), imposing significant penalties consistent with those outlined under the HITECH Act. In addition, the Office of Civil Rights published a comprehensive audit protocol organized around modules, representing separate elements of the privacy, security, and breach notification requirements. This activity was a precursor to issuance of the omnibus regulations this year.

Breach

One of the most striking changes in the final omnibus regulations is the change in the definition of "breach" to establish a presumption that any impermissible use or disclosure of PHI is a breach unless the covered entity or business associate can demonstrate a low probability that the PHI was compromised. Under prior guidance, a breach occurred if the disclosure resulted in significant financial or reputational harm to the individual. Noting that the "harm" standard in the prior interim final regulations created a higher threshold for breach notification than was intended, the final omnibus regulations remove the harm standard, which was deemed to be subjective, and now require the entity to conduct a risk assessment that examines the following objective factors:

- Nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification

- Who used or received the PHI
- Whether the PHI was actually acquired or viewed
- Any risk mitigation measures taken

The burden is on the covered entity or business associate, if applicable, to show that no breach occurred.

Breach notice. As under the interim rules, notice of a breach to affected individuals must be provided no later than 60 days after discovery of the breach. If the breach involves more than 500 persons in a state or jurisdiction, notice must be provided to prominent local media. If the breach involves more than 500 individuals, notice must be provided to HHS concurrently with notice to the individuals. In all other instances, notice must be provided to HHS within 60 days after the close of the calendar year in which the breach is discovered.

> Buck Comment. The documentation and notice requirements emphasize the need for every covered entity to train its workforce on HIPAA's privacy and security requirements. In addition, covered entities will need to clearly define the roles and responsibilities of its business associates regarding documentation and breach notification.

No breach notice is necessary if the covered entity or business associate can demonstrate a low probability that the PHI was compromised (or one of the other exceptions to breach applies).

Penalties

The final regulations adopt the provisions set forth in the HITECH interim regulations providing for tiered and increased maximum penalties.

Violation category	Penalty for each violation	All violations of an identical provision in a calendar year
Did not know	$100 - $50,000	$1,500,000
Knew, but reasonable cause	$1,000 - $50,000	$1,500,000
Willful neglect, timely corrected (generally within 30 days after the covered entity knew or should have known about the violation)	$10,000 - $50,000	$1,500,000
Willful neglect, not timely corrected	$50,000	$1,500,000

In response to comments regarding the amount of potential penalties — particularly in instances where the entity did not know or could not have known of the violation — the regulators emphasized that HHS has discretion to assess penalties on a case-by-case basis and will not automatically impose the maximum penalty. Factors such as the nature of the violation, the time period over which it occurred, and the entity's "prior indications of noncompliance" will be taken into account in calculating the final penalty amounts.

Finally, it should be noted that covered entities may be financially responsible for the acts of their business associates (and business associates for the acts of their subcontractors) based on whether one party is the agent of the other. The key factor in determining whether an agency relationship exists — and liability will attach — "is the right or authority of a covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity." Conversely, if the only method to control the relationship is to modify or terminate the business associate agreement, it is generally a clear indication that an agency relationship does not exist.

Buck Comment. Covered entities will need to exercise care in defining their relationships and drafting business associate agreements to avoid the unintended imposition of vicarious liability for the actions of their business associates.

HIPAA checklist for employers

Business associate issues

- ☐ Review HHS model BAA
- ☐ Revise BAAs to include the new direct liability provisions
- ☐ Determine date by which BAAs must be amended to comply with the omnibus rule
- ☐ Prepare an amendment for currently executed BAAs that adds the new provisions
- ☐ Consider changes to policies and procedures for monitoring business associate compliance to reflect the changes to the HIPAA enforcement rules.

Notice of privacy practices

- ☐ Revise NPP to reflect the final omnibus rules
- ☐ Distribute either revised NPP or the "material changes" to your NPP in accordance with the rules (note: that distribution rules differ for website v. paper NPPs)

Policies and procedures

Review and modify, as necessary, HIPAA privacy policies and procedures to confirm:

- ☐ The definition of PHI includes genetic information
- ☐ That access to records can include PHI maintained electronically even if not an electronic health record
- ☐ A procedure is in place related to requested disclosures to third parties
- ☐ A provision is in place regarding handling of immunization records
- ☐ Breach notification reflects the new definition of breach
- ☐ Uses of genetic information are restricted
- ☐ How the plan will use or disclose decedent's PHI to requesting parties in light of new 50-year rule
- ☐ How the plan will use or disclose decedent's PHI to family members and others involved in the care or payment of care
- ☐ They incorporate the new standards related to performing a risk assessment
- ☐ The correct definitions of marketing and sale are being used
- ☐ They include the permitted uses and disclosures related to marketing and sales
- ☐ Authorizations are updated for marketing and/or sale of PHI, if applicable
- ☐ If and how the group health plan will handle fundraising involving PHI (and a system for allowing individuals to opt out of fundraising communication)
- ☐ Permitted uses and disclosures for research are in place

Workforce training

- ☐ Update workforce training to include new provisions in the omnibus rules relevant to the group health plan, necessary changes to the organization's HIPAA policies and procedures, and breach notice training

Volume 36 | Issue 19 | March 8, 2013

Authors
Mary Harrison, JD
Tami Simon, JD

Produced by the Knowledge Resource Center of Buck Consultants at Xerox
The Knowledge Resource Center is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your account executive or email fyi@xerox.com.