OBER | KALER
Attorneys at Law

HITECH and HIPAA: The Final Rule

March 13, 2013

www.ober.com

Welcome

- Housekeeping
- Today's speakers
- Overview of the topic
- Discussion
- Questions

Welcome

- Download the slides for today's program by clicking the PDF link in the upper left corner of your screen.
- You may also download our bulletin "HHS Overhaul of HIPAA: Summary of New Obligations for Covered Entities and Business Associates."
- Also on the left is a Q&A box where you may type your questions. We'll look at those questions at the end of the program and answer as many as we can.
- At the end of the program, you'll receive an email with a link to a survey. Please take a moment to fill that out and give us your feedback.

Meet Today's Speakers

James B. Wieland

Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

Sarah E. Swank

Principal, Ober|Kaler
seswank@ober.com
202.326.5003

Joshua J. Freemire

Associate, Ober|Kaler
jjfreemire@ober.com
410.347.7676

Compliance Dates

On January 25, 2013, the Department of Health and Human Services (HHS) posted Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (the Final Rule) under the authority of the HITECH Act and the Genetic Information Nondiscrimination Act (GINA).

- The Final Rule will be effective on March 26, 2013.
- However, in general covered entities and business associates will have an additional six months, until September 23, 2013, to come into compliance.
- The Final Rule does not address the Proposed Rule on Accounting for Disclosures, published May 31, 2011.
- The Enforcement Rule changes are effective on March 26, 2013. The additional 180 days afforded for most of the provisions in the Final Rule apply only to modified standards or implementation specifications.

Business Associates: Conduits

In addition to formalizing the inclusion of Patient Safety Organizations and Health Information Organizations (Health Information Exchanges, E-Prescribing Organizations and similar organizations) as business associates, the Final Rule provides important clarification about the application of the business associate rules to entities that serve as "conduits."

- Since the inception of HIPAA, service providers such as the post office and telephone companies that act as "conduits" have been exempt from the business associate requirements as their access to Protected Health Information (PHI), if any, has been on an incidental, as opposed to a routine, basis.

Business Associates: Conduits

- As technology has evolved, however, the application of this test, never a “bright line,” to important health care industry service providers such as cloud service providers of storage or software, has been unclear.
- The Final Rule articulates a brighter line test. A “conduit,” whether of paper or electronic PHI, only provides transmission services, including any temporary storage of PHI incidental to the transmission service. By contrast, a service provider that provides storage is a business associate, even if the agreement with the covered entity does not contemplate any access or access only on a random or incidental basis. The test is persistence of custody, not the degree (if any) of access.

Business Associates: Downstream Contractors

- Downstream entities that work at the direction of or on behalf of a business associate and handle protected health information are required to comply with the applicable Privacy and Security Rule provisions, just like the "primary" business associate and are subject to the same liability for failure to do so.
- This specifically does not require the covered entity to have a contract with the subcontractor; rather, that obligation remains on each business associate.
- A "subcontractor" is an entity to which a business associate delegates a function, activity, or service involving the covered entity's PHI, other than in the capacity of a member of the workforce of such business associate.
- A hospital contracts with a billing company. The billing company contracts with a shredding company to dispose of its billing records. The shredding company contracts with a trucking company to bring the hospital's paper billing records to its shredding facility.

Business Associates: Downstream Contractors

- Under the Final Rule, each of these entities would be directly responsible for compliance with the business associate requirements under the Security and Privacy Rules, even if the parties failed to enter into a written business associate agreement. The trucking company's responsibility would likely be based on custody, even if it did not view the records, as discussed above. Under the Final Rule, the hospital would only be required to enter into a business associate agreement with the billing company. Each business associate or downstream subcontractor would be required to obtain written "satisfactory assurances" from its immediate subcontractor.
- In the event of a breach of the security of unsecure PHI, the chain of reporting would follow the chain of contracting in reverse: trucking company to shredding company; shredding company to billing company; billing company to hospital.

Business Associates: Privacy Rule Obligations

The Final Rule specifies the Privacy Act obligations of a Business Associate, not addressed in detail in the HITECH Act. Business Associates are obligated to:

- Limit uses and disclosures to what is permitted under the Privacy Rule, subject to what is allowed under the Business Associate Agreement. This specifically includes compliance with the minimum necessary standards;
- Provide breach notification to the covered entity;
- Provide a copy of electronic PHI to either the covered entity, the individual or to the individual's personal representative, as specified in the business associate agreement;
- Disclose PHI to the Secretary in an investigation of the Business Associate's compliance with HIPAA;
- Provide an accounting of disclosures;
- Comply with the security rule.

Business Associates: Privacy Rule Obligations

Comments by the Secretary indicate that permitted disclosures by a business associate for its own management and administration or for legal purposes do not create a business associate relationship with the recipient. These disclosures "are made outside the entity's role as a business associate."

In that case, however, unless the disclosure is required by law, the business associate must obtain satisfactory assurances that the recipient will hold the information as confidential, will use or disclose it only for its intended purpose or as required by law, and will report a breach of confidentiality to the business associate.

Business Associates: Transition Provisions

In recognition that it will take time to renegotiate existing business associate agreements, the Final Rule grandfathers certain business associate agreements for up to one year beyond the compliance date, up to September 23, 2014.

- In order to qualify, the business associate agreement must have been in existence prior to the publication of the Final Rule (January 25, 2013), have complied with HIPAA prior to the publication date and not be renewed or modified during the grandfather period.
- An automatic renewal, under a so-called evergreen clause, does not constitute a renewal or modification for purposes of the availability of the grandfather period.

Enforcement Rule: Investigation and Resolution of Violations

The Final Rule reflects the requirement of the HITECH Act that HHS will investigate a possible HIPAA violation if, as HHS states, a preliminary review of the facts available from a complaint or a compliance review, or information from an independent inquiry by HHS, indicates the possibility of "willful neglect."

- The investigation may proceed directly to an enforcement action, particularly but not only, in the case of willful neglect.
- However, the Final Rule offers reassurance that, absent indications of willful neglect, HHS still will seek compliance through informal, voluntary action in appropriate cases.

Enforcement Rule: Violations Due to Reasonable Cause

Of the four tiers of penalties specified in the HITECH Act, the required state of mind for the "lowest" tier (entity did not know, and in the exercise of reasonable diligence would not have known of the violation) and for the "highest" two tiers (willful neglect) are unchanged under the Final Rule.

- The state of mind for second tier, violations due to reasonable cause not amounting to willful neglect, was not specified in the HITECH Act.
- The second tier is important as a practical matter, because it likely covers many common violations by otherwise generally compliant covered entities and business associates. These would include, for example, violations that occur due to human error, despite workforce training and appropriate policies and procedures.
- The Final Rule modifies the definition of reasonable cause to specify the state of mind; reasonable cause covers violations in which the entity exercised ordinary business care and prudence to comply with the provision that was violated or in which the entity knew of the violation but lacked "conscious intent or reckless indifference" associated with a violation due to willful neglect.

Enforcement Rule: Upstream Vicarious Liability

Under the Final Rule, compliance obligations flow downstream between parties with direct contractual relationships: Covered Entity to Business Associate, Business Associate to Subcontractor, and so on.

- Civil Monetary Penalties imposed on the downstream contractor for a HIPAA violation will be attributable to the immediate upstream party with which it contracted, so long as:
  - The business associate or downstream contractor is an agent (as determined under the Federal common law of agency) of the entity with which it contracted, *and*
  - The underlying conduct was within the scope of the agency.
- The Final Rule summarizes HHS's view of federal common law of agency. Determinations will be based on the right or authority of the upstream entity to control the downstream entity's conduct in the course of performing the service, even if that right was not actually exercised with respect to the violation for which the CMP is imposed.

Marketing

In a significant departure from the Proposed Rule, an authorization for treatment communications and for communications previously permitted without an authorization under health care operations is required ***if*** the covered entity or business associate receives financial remuneration from the third party whose product or service is subject to the communication.

- Financial remuneration consists of direct or indirect payment from, or on behalf of, the third party whose product is the subject of the communication.
- An exception, in accordance with the HITECH Act, is made for subsidized refill reminders or communications about a currently prescribed drug or biological, as long as the subsidy is reasonable in amount.
- Direct means the payment is paid directly to the entity and indirect means that it was channeled through a third party.
- Financial *remuneration* does not include "in-kind" or other nonfinancial subsidies for this purpose (contrast with p*ayment* for the sale of PHI, discussed later).

Marketing

The Proposed Rule required notice and an opt-out for subsidized treatment communications (defined as those sent to an individual) and an authorization for subsidized health care operations communications (defined as those sent to a population of individuals) about:

- treatment or treatment alternatives,
- health-related products or services available from the covered entity, or
- participation in or benefits available in a provider or health plan network.

These exceptions mirror those found in the definition of marketing in the definition of *health care operations*).

The proposed rule required a judgment as to whether a communication pertained to treatment or health care operations and required two separate processes for subsidized communications – impractical and cumbersome to implement.

- New Rule: In the absence of direct or indirect remuneration, no authorization is required for either the treatment or the health care operations communications. In addition, the exception for face-to-face communications or gifts of nominal value continues, without reference to remuneration from a third party.

Sale of PHI

The HITECH Act required an authorization if a covered entity or business associate received direct or indirect remuneration in exchange for the disclosure of PHI, a so-called "sale." The HITECH Act refers to "payment," distinguishing a sale from "marketing," discussed earlier.

- The HITECH Act specified exceptions for:
  - public health activities,
  - research,
  - treatment,
  - the sale or other business consolidation of a covered entity,
  - business associate services requested by the covered entity, and
  - fees charged for providing an individual with access to the individual's PHI, other purposes designated by HHS.

Sale of PHI

- The Final Rule defines sale of *PHI* as "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information."
- Disclosure includes granting access directly or through licenses or lease agreements, not just transfers of title.
- Remuneration, for this purpose, includes non-financial, in-kind value.
- As to disclosures to a business associate, the Final Rule makes it clear that a business associate may recoup reasonable cost-based fees from third parties for preparing or transmitting records on behalf of the covered entity or where otherwise permitted by law, and that remuneration paid by the business associate to a subcontractor for activities performed on behalf of the business associate does not require an authorization.

Research

- Covered entities permitted to combine conditional and unconditional authorizations for research if they:
  - Differentiate between the two activities.
  - Allow for an opt-in of unconditional research activities.

Research

- Future research studies may now be part of a properly executed authorization, which includes all the required core elements of an authorization.
- Under the prior rule, covered entities could not combine or condition authorizations for purposes other than research that involves treatment, while a separate authorization was needed for future research or to create or build a central research database or repository.

Research

- Preparatory to research
- Solely on decedents' information
- Subject signs an Authorization
- IRB (or privacy board) waiver or alteration of Authorization
- PHI is de-identified
- Limited data set with data use agreement (DUA)

Research

- Other obligations apply because of new Business Associate requirements.
- Breach notification
- Sale of PHI
- Recent enforcement actions include research

NOTE: Common Rule might shift informational risk away from IRBs to Investigators and apply HIPAA-like protections to non-covered entities.

Disclosures Related to Decedent

- Previously, a covered entity could disclose information about a decedent only to a personal representative.
- Covered entity permitted to disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death***, unless inconsistent with any prior expressed reference*** of the individual that is known to the covered entity.
- This change does not change the authority of a decedent's personal representative.
- The PHI of individuals deceased for fifty years or more is not protected under HIPAA.

Immunizations

- Send immunization records directly to a school without written authorization.
- Need assent by a parent, guardian or person acting in *loco parentis.*
- Must comply with state law regarding the provision of immunization records.
- Document their discussion.

Fundraising

- Previously, permitted a covered entity to use or disclose PHI to a business associate or related foundation for fundraising purposes without an individual's authorization.
- Permitted PHI included:
  - Demographic information related to an individual.
  - Dates of health care provided to an individual.
- Demographic information include: name, address, other contact information, age, gender, and insurance status, **not diagnostic information.**
- Had to include fundraising in Notice of Privacy Practices and tell individual how to opt out of future fundraising.

Fundraising

- Now expands demographic information to include:
  - Treating physician
  - Outcome
  - Department (limited diagnostic information)

Fundraising

- Flexibility to decide the method to allow for individuals to opt out and opt back into the use of PHI in fundraising activities.
  - For example, toll-free number, email address, other opt-out mechanism or a combination of methods
- Leaves the decision as to the scope of the opt-out related to future fundraising communications to the covered entity.
- Many covered entities found campaign-specific opt-outs difficult to track for compliance purposes.
- HHS strengthened the standard related to further communications after individuals opt out from reasonable efforts to an outright prohibition.

Notice of Privacy Practices (NPP)

- Include statements regarding certain uses and disclosures requiring authorization.
  - Psychotherapy notes (where appropriate)
  - Marketing
  - Sales of PHI
  - Right to restrict disclosures to health plans (provider only)
  - Right to be notified of breach (but not an entity specific statement)
- Include a general statement that all uses and disclosures not described in NPP also require authorization.

Notice of Privacy Practice (NPP)

- Changes in rule are “material”
- For health plans that post on website, post revised NPP by effective date and in next annual mailing.
- If no website, health plans must provide within 60 days of material revision.
- For providers, must post and make available upon request and still provide to and seek acknowledge-ment from new patients.
- Can send by e-mail if individual agrees.

Notice of Privacy Practices

- Health plans that perform underwriting must include in their NPP a statement that the health plan is prohibited from using or disclosing genetic information for underwriting purposes.
- Does not apply to issuers of long term care policies who for now, are exempted from the underwriting prohibition.

Access - Electronic

- Must have reasonable safeguards in place to protect transmission of ePHI, but …
- If an individual wants information by unencrypted e-mail, entity can send if they advise the individual that such transmission is risky.
- Must have a secure mechanism – can't force individuals to accept unsecure.
- An electronic "machine readable copy"
  - Digital information stored in a standard format enabling the PHI to be processed and analyzed by a computer.
- Covered entities must accommodate individual requests for specific formats, if possible.

Access - Fees

- Fees charged are restricted to labor costs – cannot include costs of retrieval, or portion of capital costs.
- Charge can include supplies provided to individual upon request.

Access - Third Parties

- Individual may request a covered entity send PHI directly to another individual.
- Request must be
  - be “in writing” and signed by the individual
  - clearly identify the designated person and where to send the copy of the PHI
- Information must be protected and entity must implement reasonable policies and procedures to send it to the right place (e.g., type e-mail correctly).
- “In writing” can be electronic.

Access - Timeliness

- Change to 60 days
- Preamble urges entities to make information available sooner when possible.
- Remember to review state law requirements.

Modifications to the Breach Notification Rule

The Interim Final Breach Notification Rule was finalized without change with one significant exception – the definition of a *breach* was "clarified" through the removal of the "harm threshold," replacing it with a more objective test of whether PHI has been "compromised."

- The standards for the objective test are clearly derived from the interim harm threshold articulated in the Interim Final Rule. However, it is likely that more breaches will need to be disclosed and reported.
- Covered Entities and Business Associates should bear in mind that the HITECH Act itself has three exceptions:
  - Two are for 'intra entity" disclosures, such as inadvertent access by a member of the Covered Entity or Business Associate's workforce.
  - The third is available when the unauthorized person to whom the PHI was disclosed "would not reasonably have been able to retain the information."

Modification to the Breach Notification Rule: Definition of Breach

Of the 85 public comments received on the definition of *breach*, 70 addressed the harm threshold. Of those 70 comments, 60 supported the existing standard, but 10 (from members of Congress and consumer advocacy organizations) argued for its modification or elimination.

The Secretary explained that it believes that the "language [defining *breach* and explaining the harm standard] used in the Interim Final Rule and its preamble could be construed and implemented in manners we had not intended."

As a result, in the Final Rule, the Secretary clarifies the "position that breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information is compromised." That is, the burden of proof is unambiguously on the Covered Entity or Business Associate.

Modification to the Breach Notification Rule: Definition of Breach (including the harm standard)

This clarification was undertaken in two steps:

- First, language was added to the definition of a *breach* to "clarify that an impermissible use or disclosure of protected health information is presumed to be a breach" unless the responsible entity can demonstrate that "there is a low probability that the protected health information has been compromised."
- Second, the harm standard was removed and modifications were made to the risk assessment portion of the Breach Rule to require the use of a more objective risk assessment.

Modification to the Breach Notification Rule: Definition of Breach

The objective standard is as follows:

- Except as provided in [the existing exceptions to the definition of breach], an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that here is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
    - (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    - (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
    - (iii) Whether the protected health information was actually acquired or viewed; and
    - (iv) The extent to which the risk to the protected health information has been mitigated.

Modification to the Breach Notification Rule: Definition of Breach (including the harm standard)

The Final Rule also eliminates the existing regulatory exception for limited data sets that do not contain any dates of birth or zip codes. In the event of a breach including a limited data set, whether the data set contains dates of birth or zip codes is immaterial (though the type of information disclosed may play a role in the new assessment).

Modification to the Breach Notification Rule: Notification to Individuals

The Final Rule retains the Interim Final Rule's requirements for breach notifications without modification, but, provides some clarification on some of the finer points of when a breach is "discovered," the timeliness of notification, methods of notification, the content of the notice, and other sub-topics. Important clarifications include:

- The Final Rule notes that a covered entity that is *acting as a business associate* (by, for instance, providing billing or other services to another covered entity) should respond to a breach as a business associate. In these situations, the obligation to disclose will rest with the covered entity whose PHI is compromised.
- The Final Rule clarified several points regarding alternative notice and made explicit that notice *has not been given* if a written notice is returned as undeliverable. Covered entities responding to a breach with more than 10 notifications returned as undeliverable may take some reasonable time to search for correct, current addresses for the affected individuals, but must provide substitute notice "as soon as reasonably possible" and within the original 60-day time frame for notifications.

Modification to the Breach Notification Rule: Notification to the Media

- The Secretary clarified several points regarding media notifications, including:
  - Covered entities are not obligated to incur the cost of any media broadcast regarding the breach in question.
  - Media outlets are not obligated to publicize each and every breach notice they receive (and a failure to publicize does not render the notice provided insufficient).
  - Entities must deliver a press release directly to the media outlet being notified. Posting a general press release on a website, for instance, is insufficient.

Modification to the Breach Notification Rule: Response to Additional Public Comments

Though it did not result in a change to any regulatory text, the Final Rule noted that "[b]ecause every breach of unsecured protected health information must have an underlying impermissible use or disclosure under the Privacy Rule, OCR also has the authority to impose a civil money penalty for the underlying Privacy Rule violation, even in cases where all breach notifications were [timely, compliantly] provided."

This statement clarifies that every breach carries with it the potential for OCR enforcement and civil penalties, regardless of the size, circumstances, or response of the responsible entity.

Modifications to the HIPAA Privacy Rule Under GINA

The Final Rule finalizes proposed regulatory provisions implementing changes to HIPAA as a result of the Genetic Nondiscrimination Act of 2008 (GINA). These rule changes were first proposed in October 2009.

- The Proposed Rule is, for the most part, adopted without changes, with one exception: the Proposed Rule's expansion of entities covered by the changes (which included all health plans subject to the Privacy Rule) has been modified to exclude issuers of long-term-care policies.
- This change reflects the fact that several comments were received indicating that long-term-care insurance may become financially infeasible without a reliance on genetic information to predict future health conditions.

Modifications to the HIPAA Privacy Rule Under GINA

The Final Rule adopts the expanded application of the GINA provisions to all health plans subject to HIPAA but notably excludes issuers of long-term-care insurance.

- OCR responded specifically to claims that such an expansion was beyond its authority, noting that it has broad authority to regulate the use and disclosure of health information, including genetic information, in the interest of individuals' privacy.
- The current decision to exclude long-term-care issuers, however, may not be permanent; the Final Rule notes that OCR will be conducting additional studies of the issue, including a study by the National Association of Insurance Commissioners (NAIC), and will reassess the inclusion of long-term-care issuers in the future.

Questions?

Type your questions

into the Q&A window on the left.

More questions? Contact us.

James B. Wieland

Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

Sarah E. Swank

Principal, Ober|Kaler
seswank@ober.com
202.326.5003

Joshua J. Freemire

Associate, Ober|Kaler
jjfreemire@ober.com
410.347.7676