PUBLICATION

HHS Overhaul of HIPAA: Summary of New Obligations for Covered Entities and Business Associates [Ober|Kaler]

January 13, 2013

This client alert was reprinted in the Spring 2013 issue of the Maryland State Bar Association's Section of Labor and Employment Newsletter.

On January 17, 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 Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA), as well as under the general authority of HHS. The Final Rule, published in the *Federal Register* on January 25, 2013, will be effective on March 26, 2013. Thankfully, 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.

This client alert provides an overview of the principal changes in the Final Rule. Look for a complete review and analysis of the Final Rule in the coming days.

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 status of “conduits” as business associates. Since the inception of HIPAA, service providers such as the post office and telephone companies 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. As technology has evolved, 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.

Downstream Contractors

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. Under the Final Rule, each entity would be directly responsible for compliance with the business associate requirements under the Security Rule and the Privacy Rule, even if the parties fail 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. The 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.

Privacy Rule Obligations

The HITECH Act was not specific on the Privacy Rule direct obligations of business associates. The Final Rule specifies that these responsibilities are for limiting uses and disclosures of PHI to what is provided in the business associate agreement or the Privacy Rule; for disclosing PHI to HHS for an investigation of the business associate's HIPAA compliance; for disclosing PHI to the covered entity or the subject individual in response to a request for an electronic copy of the individual's PHI (discussed below); for making reasonable efforts to comply with the minimum necessary requirements of the Privacy Rule, and finally, for entering into a business associate agreement with a subcontractor.

Transition Provisions

In recognition of the time that will be necessary to renegotiate existing business associate agreements, the Final Rule grandfathers existing 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, have complied with HIPAA 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

Effective Date

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.

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 compliance review, or from independent inquiry by HHS, indicates the possibility of willful neglect as to HIPAA compliance. 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.

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. 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, such as those 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.

Upstream Vicarious Liability

As discussed above, 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. If a business associate or downstream contractor is an agent of the entity with which it contracted under federal common law, civil monetary penalties imposed on the downstream contractor for a HIPAA violation, so long as it is within the scope of the agency, will be attributable to the upstream party with which it contracted. 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 contractor'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, the Final Rule will require an authorization for treatment communications and for communications presently permitted as an exception to the marketing requirement of an authorization under the definition of *health care operations*, ***if*** the covered entity (or, under the Final Rule, a 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 to the covered entity or business associate 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 making the communication and *indirect* means that it was channeled through a third party to the covered entity or business associate making the communication. Financial remuneration does not include “in-kind” or other nonfinancial subsidies for this purpose.

HHS reasoned that the Proposed Rule, which 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, participants in or benefits available in a provider or health plan network (i.e., the exceptions to the definition of *marketing* in the definition of *health care operations*) was impractical to implement, requiring a judgment as to whether a communication pertained to treatment or health care operations and requiring two separate processes for subsidized communications, depending on the answer. 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 that if a covered entity or business associate received direct or indirect remuneration in exchange for the disclosure of PHI, a so-called “sale” of PHI, an authorization be obtained from each subject individual. Exceptions were specified in the Act for public health activities, research, treatment, the sale or other business consolidation of a covered entity, business associate services requested by the covered entity, fees charged for providing an individual with access to the individual's PHI, and other purposes designated by HHS. 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. Remuneration, for this purpose, includes in-kind value.

In the case of a transfer for public health purposes, the remuneration can be a cost-based fee to cover the costs of preparing and transmitting the data. A similar limitation applies to research. Cost-based fees, however, may include direct and indirect costs, so long as there is no profit factor. Disclosures for treatment and payment activities are exempted, to make it clear that these activities do not constitute a sale. 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. The definition of costs for research purposes applies to the foregoing exemptions, where reasonable cost is specified.

Research

The Final Rule permits covered entities to combine conditional and unconditional authorizations for research if they differentiate between the two activities and allow for an opt-in of unconditional research activities. 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. This change brings HIPAA in line with Common Rule requirements related to biospecimens and databases. The only exception applies to authorizations related to psychotherapy notes, which may be combined only with another authorization for the use or disclosure of psychotherapy notes.

Disclosures About a Decedent to Family Members and Others Involved in Care

Previously, a covered entity could disclose information about a decedent only to a personal representative. Under the Final Rule, a covered entity also is 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.

Disclosures of Student Immunization to Schools

Under the Final Rule, covered entitiesmay send immunization records directly to a school without written authorization. Instead, a covered entity may provide immunization records to a school upon the assent by a parent, guardian or person acting *in loco parentis*. These disclosures must comply with state law regarding the provision of immunization records. Covered entities must document their discussions related to disclosure for student immunization records.

Fundraising

The Privacy Rule permitted a covered entity to use or disclosure 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.

The Final Rule clarifies what constitutes *demographic information*. It does not modify what constitutes *fundraising communication* and current opt-out requirements, however. Under the Final Rule, covered entities are provided 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, a covered entity could use a toll-free number, email address, other opt-out mechanism or a combination of methods. In addition, under the Final Rule HHS 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

Covered entities that did modify their Notice of Privacy Practice after the passage of HITECH are now required to make changes and to distribute the new Notices based on changes required under the Final Rule. For example, the Final Rule requires that a covered entity include uses and disclosures of PHI, but not specify a list of all situations in which an authorization is required. Instead, covered entities can list categories that require authorization, such as:

- psychotherapy notes (if applicable)
- marketing purposes
- sale of PHI

The Notice must also include a statement that other uses and disclosure not described in the Notice of Privacy Practices will be made only with authorization from the individual. The Notice of Privacy Practices must also include a statement related to fundraising communications and the individual's right to opt out, and the new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service. Finally, the Notice of Privacy Practice must include a statement related to a breach of unsecured PHI, although an entity-specific statement is not required.

Right to Request a Restriction of Uses and Disclosures

The Final Rule creates a new right to restrict certain disclosures of PHI to a health plan where the individual or a family member or other person pays out of pocket in full for the health care item or service. Covered entities will be required to develop methods to create notation in an individual's medical record related to restrictions so that information is not sent to or accessible to health plans. Covered entities still can submit restricted information for required Medicare and Medicaid audits under the "required by law" requirement of the Privacy Rule.

Access of Individuals to Protected Health Information

Access

The Final Rule amends the Privacy Rule to allow individuals to request electronic copies of their PHI that is maintained in an electronic health record (EHR) or other electronic designated record set. Covered entities must provide an electronic, "machine readable copy," which means digital information stored in a standard format enabling the PHI to be processed and analyzed by a computer. HHS provides flexibility as to the exact format, acknowledging that systems may vary, but requires the covered entity to accommodate individual requests for specific formats, if possible.

Third Parties

Under the Final Rule, if an individual requests a covered entity send PHI directly to another individual, the covered entity must transmit the copy as requested. This request must:

- be in writing and signed by the individual, and
- clearly identify the designated person and where to send the copy of the PHI.

If a covered entity already requires that access request be in writing, the covered entity can use the same request to access the individual's PHI or require a separate written request. Covered entities will need to implement policies and procedures to verify the identity of the person who requests PHI and safeguards to protect the information that is used or disclosed.

Fees

Under the Privacy Rule, covered entities can charge reasonable cost-based fees. The Final Rule allows the labor cost for copying PHI to be separately identified in both paper and electronic form as a factor in cost-based fees. HHS acknowledged that the labor cost for search and retrieval of PHI in electronic form are more than negligible. Covered entities may also include the supply cost for both paper and electronic copies, including CDs or USB flash drives, along with postage for sending portable media at the request of the individual. Fees related to maintaining systems, infrastructure and storage are not considered reasonable, cost-based fees. Covered entities should check state law related to fee restrictions and requirements.

Timeliness

The Final Rule removes the 60-day timeframe for retrieval of records held off site, leaving covered entities with 30 days to provide access to records to individuals in all circumstance with a one-time 30-day extension. This change was made due to the increase reliance on electronic records and to encourage covered entities to provide access to records sooner. Covered entities should check state law related to more stringent timeliness requirements and modify current policies and procedures.

Modifications to the Breach Notification Rule (Or, “Goodbye, Harm Standard”)

The Interim Final Breach Notification Rule (the Breach Rule), published August 24, 2009, has been finalized mostly without change with one significant exception – the definition of a *breach* was “clarified” through the removal of the “harm standard” and a shift to a more objective test of whether PHI has been “compromised.” Importantly, this means two things: First, that following the clarification, more breaches will need to be disclosed and reported. Second, because these changes are characterized as a “clarification,” the changes to how covered entities and business associates analyze and report breaches take effect immediately. In fact, the clarification begs the question of whether entities that had relied on a lack of perceived harm to avoid making a breach report will need to reanalyze those incidents and perhaps make (late) disclosures. Most sections of the Interim Final Rule were adopted with minor, or no, changes. Each section of the Breach Rule adopted with noteworthy changes or guidance is addressed below.

Definition of *Breach* (including the harm standard)

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

In short, OCR 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, OCR clarifies its “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."

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.

In practice, the two changes function together. The following regulatory language was eliminated:

(1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

And the following new section of text was *added*:

(2) 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.

It is worth noting that this change 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 above-delineated risk assessment.

The Final Rule's preamble provides ample discussion of each of the new risk assessment factors, along with examples. It is clear from the examples, however, that the OCR intends for the vast majority of breaches to be disclosed. In each explanation/example (which are too voluminous to list here) the guidance provided simultaneously refuses to provide "bright line" rules while also indicating that the standard of a "low probability that the protected health information is compromised" will be very difficult to meet. Finally, it is worth noting that the Final Rule does not provide a definition for *compromised* (which may make entities' determination of the likelihood of compromise difficult indeed).

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 noted 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.

Notifications to the Media

The Breach Rule's treatment of media notifications is finalized with only a minimal change; since the definition of *state* was broadened to include American Samoa and the Northern Mariana Islands, the Breach Rule no longer references them directly. In addition, OCR 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.

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 or circumstances – a statement that may indicate more stringent enforcement activities to come.

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 rather large 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 apparently 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. Each regulatory section adopted with noteworthy changes or guidance is discussed below.

Extension of Required Protections to All Health Plans Subject to the HIPAA Privacy Rule

As noted above, 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.

Prohibition on use of Genetic Information for Underwriting

The underwriting prohibition is adopted without modification, save for the exemption of issuers of long-term-care insurance discussed above. Helpfully, the Final Rule includes several examples of how the prohibition would apply.

Notice of Privacy Practices

The Final Rule adopts the provision obligating health plans that perform underwriting to include in their Notice of Privacy Practices a statement that the health plan is prohibited from using or disclosing genetic information for underwriting purposes. This change does not apply to issuers of long-term-care policies who for now, are exempted from the underwriting prohibition.

Response to Additional Public Comments

In addition to the above specific changes, OCR explained, in response to a public comment, that providers should understand that it is the responsibility of the health plan to abide by the underwriting prohibition. Providers who, for instance, are asked for information that meets the definition of *genetic information* are not obligated to confirm or ensure that the information will not be used for underwriting purposes. OCR noted, however, that the information requested by health plans remains subject to the minimum necessary standard.