KING & SPALDING

Client Alert

Healthcare and FDA & Life Sciences Practice Groups

January 24, 2013

OCR Issues Long-Awaited Omnibus HIPAA/HITECH Rules
Significant Changes for Business Associates and Breach Analysis

The wait is finally over. On January 17, 2013, the U.S. Department of Health & Human Services (HHS), Office for Civil Rights (OCR), issued the final "omnibus" rule modifying the HIPAA Privacy, Security, Breach Notification and Enforcement Rules (Final Rule). The rulemaking comes nearly two and half years after the release of the proposed rule and implements statutory amendments to the federal health privacy framework enacted under the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Nondiscrimination Act of 2008 (GINA). It also addresses comments received regarding the interim final enforcement and breach notification rules, and makes other modifications to enhance the effectiveness of the HIPAA rules, while at the same time seeks to reduce their burden on regulated entities.

The Final Rule is effective March 26, 2013, but covered entities and business associates have until September 23, 2013 to come into compliance with the new standards and implementation specifications. As discussed below, OCR has also provided a longer transition period for existing business associate agreements to come into compliance.

The Final Rule includes substantive and non-substantive (technical) changes to the HIPAA Rules. We highlight below the more significant substantive changes.

Breach Notification

Revised Definition of "Breach." The interim final rule for breach notification for unsecured protected health information (PHI) published by OCR in 2009 defined a "breach" to mean generally the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which "compromises the security or privacy" of the PHI. OCR further clarified this definition using a "harm standard;" specifically, the impermissible acquisition, access, use or disclosure must pose a significant risk of financial, reputational, or other harm to an individual. After considering public comments (including from members of Congress) to the interim final rule,

For more information, contact:

Gina Cavalier
+1 202 626 5519
gcavalier@kslaw.com

Robert Keenan
+1 404 572 3591
rkeenan@kslaw.com

Preeya Noronha Pinto
+1 202 626 5547
ppinto@kslaw.com

Tracy Weir
+1 202 626 2923
tweir@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

however, OCR determined that the "harm standard" was too subjective and would lead to inconsistent interpretations and results across covered entities and business associates with regard to when a breach occurs and the notification requirements that are triggered.

In the Final Rule, instead of an assessment of the risk of harm to an individual, OCR requires covered entities and business associates to assess the probability that PHI has been compromised. This assessment must consider at least the following four objective factors:

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

Covered entities and business associates must consider all of these factors in combination in order to evaluate the overall probability that the PHI has been compromised. If the evaluation fails to demonstrate that there is a low probability that the PHI has been compromised, then breach notification is required. In other words, there is now a *presumption* that an impermissible use or disclosure of PHI is a breach unless a covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised.

Removal of Exception for Limited Data Sets. The Final Rule removes the exception to the breach definition for limited data sets that do not contain any dates of birth and zip codes. Any impermissible use or disclosure of such limited data sets is presumed to constitute a breach unless a covered entity or business associate can demonstrate that there is a low probability that PHI has been compromised.

Clarification to Breach Notification Provision. The Final Rule modifies the breach notification requirements to the Secretary of HHS to require that the Secretary must be notified of all breaches affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were "discovered," and not in which the breaches "occurred."

Business Associates

Direct Application of HIPAA to Business Associates. Consistent with the proposed rule, the Final Rule implements HITECH by applying requirements of the Privacy and Security Rules directly to business associates. Under the Final Rule, business associates will have direct liability under the Privacy Rule for violations of the business associate agreement obligations set forth in the Privacy Rule, and for uses and disclosures of PHI that are otherwise impermissible under the Privacy Rule, including violations of the Rule's minimum necessary requirement. In addition, the Final Rule applies all of the requirements of the Security Rule directly to business associates. Business associates will be subject to sanction by OCR for violations of these requirements.

Expanded Definition of Business Associates. The Final Rule adopts OCR's proposal to expand the scope of the "business associate" definition to apply explicitly to subcontractors of business associates, as well as to Health Information Organizations, E-prescribing gateways, Patient Safety Organizations, and persons that offer Personal Health Records to individuals on behalf of a covered entity. OCR also modified the definition to apply not only to persons that create, receive or transmit PHI, but also to persons that "maintain" PHI, in order to make it clear that persons who merely possess or store PHI on more than a random or infrequent basis are business associates, even if they rarely or never actually access or view the information.

Business Associate Subcontractor Agreements. The Final Rule requires that business associates enter into business associate agreements with subcontractors in the same manner that covered entities currently are required to enter into business associate agreements with their business associates. This requirement applies to business associate subcontractors that create, receive, transmit or maintain PHI in order to perform a function, activity or service that the business associate has agreed to perform. Each such subcontractor is itself a business associate, and the obligation to enter into downstream business associate agreements will go "down the chain" as far as the delegation and information goes. The subcontractor obligation does not apply to business associates that disclose PHI to third parties for the entity's own management and administration or legal responsibilities.

Business Associate Contract Transition Provisions. The Final Rule includes transition provisions that permit an additional year for existing business associate agreements to come into compliance, unless such agreements are renewed or modified prior to the extended compliance deadline. In particular, for business associate agreements and downstream contractor agreements existing prior to January 25, 2013, the compliance date for revising agreements to conform to the Final Rule will be September 22, 2014, unless the agreement is renewed or modified during the period from March 26, 2013 to September 23, 2013, in which case the agreement will need to come into compliance as of the date of renewal or modification. An automatic or "evergreen" renewal that occurs without any change in terms or other action by the parties does not trigger the earlier deadline.

Marketing

The Final Rule takes a streamlined—albeit more restrictive—approach to marketing activities involving PHI. In general, the Rule still requires an authorization for any use or disclosure of PHI for "marketing." In addition, exceptions to the authorization requirement remain for (1) face-to-face communications and (2) promotional gifts of nominal value. Notably, though, the Final Rule provides that if the marketing involves direct or indirect "financial remuneration" from a third party, an authorization must be obtained and it must state that such remuneration is involved. This requirement applies irrespective of whether the underlying disclosure meets an exception to the *definition* of marketing (*e.g.*, for certain "treatment" activities). Stated otherwise, marketing communications—whether for treatment, health care operations or otherwise—that involve financial remuneration require an authorization.

"Financial remuneration" is defined as direct or indirect payment "for or on behalf of a third party whose product or service is being described." It does not include any payment for treatment of an individual.

The core definition of "marketing" remains the same: To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. However, in addition to other

exceptions, the Final Rule inserts an express exclusion for the provision of refill reminders. Such reminders must relate to a drug or biologic that is currently being prescribed for the individual, and any financial remuneration received by the covered entity in exchange for making the communication must be reasonably related to the covered entity's cost of making the communication.

Sale of PHI

The Final Rule incorporates an express prohibition against the sale of PHI by covered entities or business associates in the absence of an authorization. In the event an authorization is obtained to sell PHI, the authorization must specifically state that the disclosure will result in remuneration to the covered entity or business associate making the disclosure/sale (the seller).

While "sale" of PHI is defined broadly to mean a disclosure of PHI by the seller, where the seller receives remuneration from the recipient of the PHI, in exchange for the PHI, the Final Rule sets forth numerous exclusions. For example, "sale of PHI" does not include disclosures for public health, certain research purposes, treatment and payment, and for any other purpose permitted by the Privacy Rule, where the only remuneration received by the seller is "a reasonable cost-based fee" to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law. Corporate transactions (*i.e.*, sale, transfer, merger, consolidation) of all or part of a covered entity and related due diligence are also excluded from the definition of "sale."

Research

The Final Rule includes a number of important provisions related to research, including changes and interpretations intended to harmonize requirements between HIPAA and the Common Rule. Notably, (1) the Final Rule expressly permits compound authorizations, and (2) OCR sets forth its view that authorizations that relate to future research are permissible. The definition of "research" remains the same: a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Prior to the changes in the Final Rule, the Privacy Rule precluded certain so-called "compound" authorizations because it did not permit a research authorization that included a treatment condition to be combined with any other legal permission. As a practical matter, for example, this meant that a single authorization could not be used for a research study that included treatment and tissue banking of specimens (since this generally would involve an authorization that would condition research-related treatment).

Under the Final Rule, compound authorizations for research are permitted. An authorization for a research study may now be combined with any other type of written permission for the same or another research study. However, where a covered health care provider combines conditioned and unconditioned authorizations for research, the authorization must clearly differentiate between the conditioned and unconditioned research components and clearly allow the individual the option to opt-in to the unconditioned research activities.

Another way the Final Rule aims to harmonize with the Common Rule involves authorizations for future research. Prior to the Final Rule, OCR interpreted the Privacy Rule to require that a research authorization be study-specific, thereby preventing future uses and disclosures for research. While the Final Rule does not make changes to the regulatory text of the Privacy Rule, OCR now takes the position that the research "purposes" that must be included in an authorization need not be study-specific. Instead, to satisfy the "purpose" requirement the authorization must adequately describe the future research such that "it would be reasonable for the individual to expect that his or her [PHI] could be used or disclosed for such future research."

Fundraising

The Final Rule expands the types of PHI that may be used (without the need for an authorization) for fundraising purposes. The additional types of PHI include date of birth (as opposed to static age), general department of service (*e.g.*, cardiology, oncology), treating physician information, and outcome information. In addition, covered entities must provide a clear and conspicuous method for opting out of fundraising communications and the method must not result in undue burden or more than nominal cost to the individual.

Notice of Privacy Practices

The Final Rule requires that a number of changes be implemented to the notice of privacy practices (NPP) of covered entity providers and health plans. NPPs must include statements:

- setting forth the right of affected individuals to be notified following a *breach* of unsecured PHI;
- regarding *uses and disclosures that require authorization*, including uses and disclosures of psychotherapy notes (if applicable), for marketing, or involving the sale of PHI;
- informing individuals of their right under HITECH to *restrict certain disclosures to health plans* when the individual has paid out of pocket in full for the health care item or service;
- regarding *fundraising* and an individual's right to opt-out of such communications (but this is only required if the covered entity intends to engage in fundraising, as the Final Rule did not adopt the proposed rule requirement that NPPs include the mechanism describing how individuals can opt-out of receiving fundraising communications); and
- reflecting the prohibition on health plans' (except issuers of long term care policies) use or disclosure of PHI that is *genetic information* for underwriting purposes (but this is only required if the health plan intends to use PHI for underwriting purposes).

OCR has deemed the changes required by the Final Rule to be material. This means that covered entities will need to provide revised notices to individuals. The Final Rule does not alter current rules governing the distribution of revised NPPs by covered entity providers. It does, however, provide some relief to health plans that currently post their NPPs on their consumer websites. These health plans can "provide" the revised NPP by (1) prominently posting the material change or its revised notice on the site by the effective date of the change to the notice, which is the compliance date of the Final Rule, or September 23, 2013; and (2) providing the revised notice, or information about the material change and how to obtain the revised notice, in the next annual mailing. Health plans that do not post

their NPPs on their website must provide the revised notice (or information about the material change and how to obtain the revised notice) to members within 60 days of the revision.

Individual Rights

Right to Request Restrictions. The Final Rule implements the HITECH provision requiring covered entity providers to agree to a request to restrict disclosures of PHI about the individual to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and the PHI pertains solely to the health care item or service for which the individual (or person other than another health plan) has paid the covered entity provider in full. In the preamble to the Final Rule, OCR addresses some of the operational difficulties of this rule including how to handle, for example, mandatory billing requirements, prohibitions on unbundling services, and HMO services. OCR also clarifies that it is the burden of the individual (and not of the covered entity) to notify other downstream providers, such as pharmacies, of the health plan restriction request.

Access Requests. HITECH afforded individuals with a right to obtain an electronic copy of their PHI if the covered entity uses or maintains an electronic health record. OCR has interpreted this right more broadly in the Final Rule, allowing individuals to obtain an electronic copy of PHI that is maintained electronically in a designated record set (which may or may not satisfy the definition of electronic health record). Under the Final Rule, individuals have the right to receive an electronic copy in the form and format that they request if readily producible; if not, then in a machine-readable electronic form and format, as agreed upon by the individual and the covered entity. OCR acknowledges that some legacy systems may not be capable of producing any form of electronic copy. Thus, some covered entities may need to invest in new systems to meet the electronic access requirements.

Individuals may also request that covered entities send a copy of their PHI directly to another person, as long as the request is in writing, signed by the individual, and clearly designates the person to whom and the place to where the PHI should be sent. Subject to more stringent state laws governing fees, covered entities may charge a reasonable-cost based fee for the copy of the PHI. This expressly includes fees for the labor involved in preparing the copy, but it does not include retrieval fees or costs for recouping capital investments, storage and infrastructure. The fee may also include the cost of supplies (*i.e.*, paper or portable electronic media) used for creating the copy. Finally, the time frames for responding to the request for access, whether paper or electronic, are identical (*i.e.*, within 30 days after receipt). However, the Final Rule reduces the amount of additional time available to covered entities to respond when records are offsite from 60 days to a one-time extension of 30 days.

Enforcement

The Final Rule retains the tiered-penalty structure implemented through the interim final enforcement rule (adopted October 30, 2009), but adopts certain modifications including, among others:

- the HITECH requirement that OCR must investigate *any* complaint if a preliminary review indicates *possible* (not probable) noncompliance due to willful neglect;

- the HITECH expansion of direct civil and criminal liability to business associates for violations of the HIPAA Rules;
- a clarification that covered entities remain liable, in accordance with the Federal common law of agency, for the acts or omissions of their agents (including business associates) acting in the scope of agency and that business associates are similarly liable for acts or omissions of their subcontractors; and
- the HITECH requirement of mandatory assessment of civil monetary penalties for violations due to willful neglect.

What Does The Final Rule Mean to You?

Regulated entities should review their HIPAA privacy, security, and breach notification policies and procedures to ensure appropriate modifications are made to reflect the requirements of the Final Rule. Business associate agreements will also require revisions, with due care given to the issue of agency and allocation of liabilities, among other things. Business associates (and their subcontractors) that create, receive, maintain or transmit electronic PHI must come into compliance with the Privacy and Security Rule requirements, which means, among other things, the performance of a security risk assessment and implementation of HIPAA security policies.

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in 17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice.