WOMBLE CARLYLE
INNOVATORS AT LAW®

Client Alert

January 2013

A Detailed Analysis of Changes to HIPAA and the Implications for Healthcare Providers and Others in the Healthcare Industry

On Friday, January 25, 2013, the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") published a final rule modifying the HIPAA Privacy, Security, and Enforcement Rules (the "Final Rule") as mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Many of these modifications were set forth in a Notice of Proposed Rulemaking ("NPRM") dated July 14, 2010, although the Final Rule does not adopt all the proposals as described in the NPRM.

The Final Rule also modifies the Breach Notification Rule, which has been effective as an interim final rule since September 23, 2009. Finally, the Final Rule strengthens privacy protections for certain genetic information under the Genetic Information Nondiscrimination Act ("GINA").

The Final Rule makes significant changes to HIPAA and the potential penalties for violating HIPAA. The Final Rule also expands the scope of HIPAA, meaning that some businesses that were not subject to HIPAA before the Final Rule now have HIPAA compliance obligations and can be subject to enforcement action for noncompliance. Healthcare providers and others in the healthcare industry should be aware of these changes and how they will apply to their particular business.

The Final Rule is effective on March 26, 2013, and Covered Entities and Business Associates must comply with the Final Rule by September 23, 2013.

Changes to the HIPAA Privacy Rule:

Background: The HIPAA Privacy Rule governs the use and disclosure of Protected Health Information ("PHI"). Prior to the HITECH Act, the Privacy Rule only applied to Covered Entities (i.e., covered health care providers, health plans, and health care clearinghouses). Covered Entities could engage Business Associates to provide services to the Covered Entities involving the use or disclosure of PHI as long as the Covered Entity and the Business Associate entered into an appropriate Business Associate Agreement. Business Associates were contractually liable for compliance with the Business Associate Agreement but were not directly liable for HIPAA compliance. However, the HITECH Act provided that, as of February 17, 2010, Business Associates were also directly subject to many provisions of the Privacy Rule.

Modifications:

Applicability to Business Associates and Subcontractors: As required by the HITECH Act, the Final Rule clarifies that certain (but not all) provisions of the Privacy Rule are directly applicable to Business Associates. As a result, Business Associates are now directly liable for compliance with these provisions and may be subject to enforcement for noncompliance. For example, Business Associates are now directly liable under HIPAA for (i) impermissible uses and disclosures of PHI, (ii) failure to provide notification of a Breach of Unsecured PHI to a Covered Entity, (iii) failure to provide access to a copy of electronic PHI in the manner set forth in the applicable Business Associate Agreement, (iv) failure to disclose PHI to HHS to investigate or determine the Business Associate's compliance with HIPAA, (v) failure to provide an accounting of disclosures of PHI, and (vi) failure to comply with the requirements of the Security Rule.

The Final Rule also clarifies that if a subcontractor of a Business Associate creates, receives, maintains, or transmits PHI on behalf of the Business Associate, the subcontractor is also a Business Associate with direct HIPAA compliance obligations. However, a Covered Entity is not required to enter into Business Associate Agreements with these subcontractors. Instead, the Covered Entity must continue to enter into Business Associate Agreements with its Business Associates, who are then required to enter into Business Associate Agreements with their subcontractors.

Business Associate Agreements: Most Business Associate Agreements will need to be revised to comply with the Final Rule, and OCR recognizes that Covered Entities and Business Associates are concerned with renegotiation and amendment of existing Business Associate Agreements. A Covered Entity and a Business Associate (and a Business Associate and its subcontractor) may continue to operate under an existing Business Associate Agreement for a certain amount of time if (1) prior to January 25, 2013, the Business Associate Agreement complied with then-current HIPAA rules and (2) the Business Associate Agreement is not renewed or modified from March 26, 2013 until September 23, 2013. If these conditions are met, the parties can operate under the existing Business Associate Agreement until the earlier of (1) the date the Business Associate Agreement is renewed or modified on or after September 23, 2013 or (2) September 22, 2014. The Final Rule makes clear, though, that a Business Associate may not use or disclose PHI in a manner contrary to the Privacy Rule even if the Business Associate Agreement with the Covered Entity has not yet been amended.

Marketing: The Final Rule significantly changes the approach to marketing that was set forth in the NPRM. In short, the Final Rule requires individual authorization for all treatment and health care operations communications where the Covered Entity receives financial remuneration from a third party for making the communications when the third party's product or service is being marketed in the communications. If a Business Associate, including a subcontractor, receives the financial remuneration from a third party in exchange for making the communication, the authorization from the individual is required prior to sending the communication.

The term "financial remuneration" does not include non-financial benefits; it includes only payments made in exchange for making the communications. If the financial remuneration received by the Covered Entity from the third party is for anything other than making the communication, the Covered Entity is not required to obtain individual authorization under this marketing provision. For example, if a third party provides financial remuneration to a Covered Entity for implementing a disease management program, the Covered Entity could communicate with individuals about the program without obtaining individual authorizations as long as the communications are about the Covered Entity's program and are not encouraging individuals to use or purchase the third party's product or service.

Sale of PHI: The Final Rule adopts a general prohibition on the sale of PHI without an individual's authorization. The "sale of PHI" is defined as a disclosure of PHI by a Covered Entity or Business Associate where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. Unlike the meaning of "financial remuneration" for purposes of the marketing provisions discussed above, the Final Rule explains that the use of the term "remuneration" here means that the prohibition of the sale of PHI applies to the receipt of nonfinancial, as well as financial benefits, in exchange for the PHI.

The prohibition of the sale of PHI is subject to certain exceptions. For example, when the remuneration received by the Covered Entity or Business Associate in a research context is a reasonable cost-based fee covering the cost to prepare and transmit the PHI for research purposes, the prohibition does not apply. A broad exception for disclosures for public health purposes is also included.

Research: Although the Final Rule explains that the sale of PHI includes disclosures for which the Covered Entity receives remuneration, it is important to note that, in many cases, disclosures of PHI to researchers will not be prohibited by the sale of PHI provision. For example, OCR states that the sale of PHI does not include payments a Covered Entity may receive in the form of grants to perform a research study because any provision of PHI to the payer is a byproduct of the service being provided. Also, under the Final Rule, a Covered Entity may continue to use or disclose de-identified information for research purposes because de-identified information, by definition, is no longer PHI. Moreover, Covered Entities are still permitted to use and disclose PHI for research purposes without de-identifying the PHI as long as individual authorization is obtained in accordance with 45 C.F.R. § 164.508 or without individual authorization in certain limited circumstances.

Notably, in most cases, neither an external researcher performing research nor an independent Institutional Review Board ("IRB") performing research review, approval and continuing oversight functions would fall within the definition of Business Associate because they are not performing a function, activity, or service for a Covered Entity as described in the definition of Business Associate. However, if the external researcher or IRB performs a function, activity, or service for a Covered Entity that falls within the definition of a Business Associate, like performing a health care operations function on behalf of the Covered Entity, then the researcher and IRB (and their subcontractors) are Business Associates and HIPAA compliance obligations and liabilities would apply.

The Final Rule also modifies the Privacy Rule to permit a Covered Entity to combine conditioned and unconditioned authorizations for research into one document. Importantly, the authorization must differentiate between the conditioned and unconditioned research components so the individual may opt in to the unconditioned research activities. This is significant in that compound authorizations could be used for biospecimen banking that also permits future secondary use of patient data to the extent there is a valid authorization. In a welcome change, the Final Rule modifies HHS's prior interpretation of the Privacy Rule that research authorizations must be study-specific. Instead, under the Final Rule, future research purposes must be adequately described in the authorization so it would be reasonable for an individual to expect that his or her information could be used or disclosed for such future research.

Decedent Protections and Disclosures about Decedents to Those Involved in Care: The Privacy Rule currently requires Covered Entities to protect a decedent's PHI the same way it protects the PHI of living individuals. The NPRM proposed to require Covered Entities to comply with the Privacy Rule with respect to decedents for a shortened period of 50 years following the date of death. The Final Rule adopts this proposal but notes that this required 50-year period of protection under the Privacy Rule does not preempt state or other laws that may provide greater protection, such as those laws applicable to information about a decedent's mental health or HIV/AIDS status.

Also, OCR has included an amendment permitting Covered Entities to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to his or her death, unless the Covered Entity knows that the disclosure is inconsistent with any prior expressed preference of the decedent. These changes do not impact the authority of a decedent's personal representative, but rather seek to ensure that family members and others can find out about the circumstances surrounding the death of loved one unless the individual previously objected to disclosing such information to those involved in his or her care. The Final Rule notes that Covered Entities making disclosures pursuant to this provision should not share information about past, unrelated medical problems.

Fundraising: The Privacy Rule currently permits the use and disclosure of certain types of PHI for fundraising purposes but has always required that fundraising communications contain a description of how the individual may opt out of receiving such communications. In response to the HITECH Act, the Final Rule clarifies which types of PHI may be used and disclosed for fundraising purposes and strengthens the opt out provisions.

Under the Final Rule, demographic information (including names, addresses, other contact information, age, gender, and dates of birth), dates of health care provided to an individual, department of service information (e.g., cardiology, pediatrics, oncology), treating physician, outcome information, and health insurance status may be used and disclosed for fundraising purposes.

Fundraising communications must provide the individual with a clear and conspicuous opportunity to opt out of any further fundraising communications. While Covered Entities are free to decide what methods individuals may use to opt out, the Final Rule makes it clear that the chosen methods may not impose an undue burden or more than a nominal cost on individuals. For example, requiring individuals to write and send a letter to the Covered Entity asking not to receive further fundraising communications is considered an undue burden and would not be an appropriate opt out method. In addition, if an individual elects not to receive further fundraising communications, OCR notes that this election should not lapse after a certain period of time. Covered Entities need to review and update their fundraising policies to ensure they comply with the requirements of the Final Rule.

Notices of Privacy Practices: The Final Rule makes several changes to the Notice of Privacy Practices ("NPP") requirements of the Privacy Rule. For the most part, the Final Rule adopts the changes proposed in the NPRM: (i) the NPP must include a statement regarding the uses and disclosures of PHI that require an authorization, such as marketing, psychotherapy notes, and sale of PHI, and require that uses and disclosures not described in the NPP will be made only with the individual's authorization; (ii) the NPP must state that the Covered Entity may contact an individual to raise funds for the Covered Entity and that the individual has the right to opt out of receiving such fundraising communications; (iii) health plans that underwrite are prohibited from using or disclosing PHI that is genetic information about an individual for underwriting purposes. Such health plans are required to include a statement in their NPP explaining this prohibition. The Final Rule notes that this requirement does not apply to issuers of long term care policies, which are not subject to the underwriting prohibition; (iv) the NPP must explain that the Covered Entity must agree to a request to restrict disclosure of PHI to a health plan if the individual has paid out of pocket in full for the health care item or service. The Final Rule notes that only covered health care providers (and not other Covered Entities) are required to include this explanation in the NPP; and (v) the NPP must notify individuals of their right to receive notification following a Breach of the individual's Unsecured PHI.

Because the Final Rule treats all subsidized treatment communications as marketing communications for which individual authorization is required, the Final Rule did not adopt the changes from the NPRM which would have provided individuals the right to opt out of receiving treatment communications when the covered entity has received financial remuneration in exchange for making the communication to the individual.

The Final Rule considers the changes described above to be material changes requiring revision of NPPs, but the Final Rule removes the requirement that health plans make the revised NPP available within 60 days of a material revision to the NPP. In place of the removed provision, the Final Rule adds a new subsection to require a health plan that currently posts its NPP on its website to prominently post the material change or the revised NPP on its website by the effective date of the material change and to provide the revised NPP or information about the material change in the health plan's next annual mailing to individuals then covered by the plan. The Final Rule clarifies that a Covered Entity is not required to revise and distribute a new NPP upon publication of the Final Rule to the extent the Covered Entity has already revised its NPP in response to the HITECH Act or state law requirements and such revisions are consistent with the Final Rule.

Disclosures to Schools: OCR has long heard concerns that requiring authorizations for disclosures of student immunization information to schools made it difficult for parents to provide the necessary immunization documentation. In response to these concerns, the Final Rule states that a Covered Entity must obtain active agreement, which may be in oral or written form, from the parent, guardian, or other person acting in loco parentis to disclose proof of immunization to a school when state law or other law requires the school to have such information prior to admitting the student. While

written authorization is no longer required, Covered Entities must still document and maintain the agreement obtained under this provision.

Requested Restrictions: Under the Privacy Rule, individuals can request restrictions on the uses and disclosures of their PHI, but Covered Entities have not been required to agree to any requested restrictions. However, the HITECH Act describes certain circumstances in which a Covered Entity must comply with an individual's request for restriction of disclosure of PHI. To implement this provision of the HITECH Act, the Final Rule provides that a Covered Entity must agree to an individual's request to restrict disclosure of PHI to a health plan if (i) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and (ii) the PHI pertains solely to a health care item or service for which the individual has paid the Covered Entity in full.

Health care providers are encouraged, but not required, to notify downstream providers of the fact that an individual has requested a restriction on the disclosure of PHI to a health plan. Also, to avoid the possibility of payment issues, a provider may require payment in full at the time such a restriction is requested.

If you have any questions about the Final Rule or HIPAA please contact Jill M. Girardeau, the principal drafter of this alert, Sarah B. Crotts, Deonys de Cardenas, Tracy Field, or any member of Womble Carlyle's Health Care Practice Group.