HHS Finalizes Comprehensive Modifications to HIPAA Regulations in Omnibus Final Rule

On Thursday, January 17, 2013, the Department of Health and Human Services Office for Civil Rights ("HHS") released in pre-publication form the rule commonly known as the "HIPAA Omnibus Rule," which we refer to below as the "Final Rule."[1]

As summarized in a prior alert, on July 14, 2010, HHS published its notice of proposed rulemaking ("NPRM") entitled "Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act" ("HITECH"). Further, as summarized in another alert, on August 24, 2009, HHS published its Interim Final Breach Notification Rule (the "Interim Breach Rule"). This Final Rule, to be published in the Federal Register tomorrow, finalizes (i) changes in the NPRM, with some modifications, (ii) changes in the Interim Breach Rule, with some modifications, and (iii) the changes previously proposed to HIPAA under the Genetic Information Nondiscrimination Act ("GINA").

The Final Rule will be effective on March 26, 2013. Covered entities and business associates must comply with the Final Rule within 180 days, or by September 23, 2013. HHS has provided a longer compliance timeframe for certain other requirements, such as required changes to business associate agreements. All modifications to the Enforcement Rule, which governs the compliance responsibilities of covered entities during the enforcement process, will be effective on March 26, 2013.

I. Breach Notification and Enforcement Rules

1. Modifications to the Definition of Breach; Notification Obligations Mostly Unchanged

The Final Rule makes limited but significant changes to the Interim Breach Rule that became effective on September 23, 2009. Most significantly, the Final Rule replaces the harm standard present in the Interim Breach Rule with an access standard. HHS makes clear in commentary that it views the former harm standard as overly subjective, and indicates its belief that the new standard will be more objective and will likely increase the number of incidents resulting in breach notifications.

The Final Rule also sets forth four "required" risk assessment factors that should drive any breach analysis:

- Nature and extent of the protected health information ("PHI") involved (*e.g.,* types of identifiers and likelihood of re-identification),
- Type of unauthorized person in receipt of the PHI as a result of the breach (*e.g.,* thief, other health care provider),
- Whether the PHI was actually "acquired or viewed;" and
- Extent to which the risk to PHI has been mitigated.

The Final Rule maintains mostly unchanged the content and timing requirements of breach notices, whether to individuals, prominent media outlets or the Secretary of HHS ("Secretary"). Nonetheless, the

[1] This final rule is formally entitled, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules."

commentary provides a number of instructive clarifications.

For additional information about changes to the breach notification rule, please click here.

2. Modifications to the Enforcement Rule

HHS may conduct a formal compliance review (when prompted by media reports or reports by state or other federal agencies) or an investigation when the preliminary review in response to a complaint or other inquiry reveals culpability less than willful neglect. HHS must initiate a formal investigation when a party appears to have exhibited willful neglect. The Final Rule no longer requires the Secretary to exhaust all informal resolution efforts before moving directly to a Civil Monetary Penalty ("CMP"). The Final Rule establishes four tiers of CMPs based on culpability levels: "reasonable diligence," "reasonable cause," and two separate tiers that correspond to "willful negligence."

Within each tier, HHS will consider aggravating and mitigating factors, including reputational, physical or financial harm to the affected individual(s), the number of individuals affected, and prior indications of noncompliance by the entity under scrutiny. HHS may not impose CMPs for violations due to reasonable diligence or reasonable cause that are corrected within 30 days. However, entities may no longer assert reasonable diligence as an affirmative defense to CMP liability; rather, a showing of reasonable diligence would result in assessment under the lowest penalty tier. Even in cases of willful neglect, curing a violation within 30 days of actual or constructive knowledge of the violation may reduce the entity's potential penalties substantially.

II. Specific Modifications Regarding Business Associates

1. Applicability of the Privacy and Security Rules to Business Associates

The Final Rule makes clear that HHS will hold business associates directly liable (*i.e.*, business associates will face liability beyond contractual liability to covered entities) for certain violations of the Privacy Rule or the Security Rule including:

- Impermissible uses and disclosures of PHI;
- Failure to disclose PHI when required by the Secretary;
- Failure to disclose PHI upon request to a covered entity, individual, or individual designee, as applicable;
- Failure to limit PHI used or disclosed to the minimum amount necessary to accomplish the intended purpose;
- Failure to enter into business associate agreements with subcontractors that create or receive PHI for the business associate; and
- Failure to maintain adequate physical and technical safeguards for electronic PHI maintained on behalf of covered entities.

2. Modifications Required for Business Associate Agreements

The Final Rule contains a number of provisions regarding business associate agreements originally proposed in the NPRM. Consistent with prior contractual implementation requirements, covered entities and business associates must implement required changes to all business associate agreements if the agreements are renewed or modified after September 23, 2013, but no later than one year after September 23, 2013.

Please click here for a summary of these changes and other items relevant to business associates.

III. Updated Marketing Rules

Although the NPRM suggested significant changes to permissible marketing practices, the Final Rule includes additional material modifications to the NPRM. Notably, the NPRM proposed allowing providers to make treatment-related marketing communications for which the provider receives financial remuneration, on behalf of third parties (*i.e.*, subsidized treatment-related communications), without authorization if patients were advised of such possibility in the provider's notice of privacy practices ("NPP"). The Final Rule is significantly more restrictive, requiring covered entities to secure individual authorizations in advance of engaging in any non-exempt marketing practice. The Final Rule also adopted the term "financial remuneration" set forth in the NPRM without change, and provided some clarifying guidance, including the specific exclusion of non-financial benefits from this definition.

For a summary of these changes, please click here.

IV. Modifications Required For Notices of Privacy Practices

Significantly, the Final Rule requires covered entities to modify and re-distribute their notices of privacy practices ("NPPs") to include the following:

- A description of uses and disclosures that require individual authorization, such as uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI;
- A statement that other uses and disclosures not described in the NPP (or required under HIPAA) will be made only with an individual's authorization, which may be revoked;
- If PHI is used for fundraising purposes, an explanation regarding fundraising communications, as well as information regarding an individual's right to opt out of receiving such communications;
- A statement that covered entities must or will notify affected individuals following a breach of their unsecured PHI;
- For health care providers only, a statement informing individuals of their right to request a restriction of certain disclosures of PHI to a health plan if the individual pays out of pocket in full for the health care item or service; and
- For health plans only, a statement informing individuals that health plans will not use or disclose genetic information for underwriting purposes.

V. Changes to Rules Governing Research

The Final Rule adopts several changes to the provisions governing research. Many of these changes were adopted in direct response to recommendations made by the HHS Secretary's Advisory Committee on

Human Research Protections and the Institute of Medicine. In general, the Final Rule allows research entities subject to HIPAA to utilize so-called "compound authorizations" in connection with research and also eliminates the requirement that research authorizations must be study-specific in favor of a more flexible standard for researchers. The Final Rule also retains exceptions to the authorization requirement for any use or disclosure permitted by the Privacy Rule when remuneration means only payment of the reasonable cost of providing the PHI. The Final Rule also clarifies that a covered entity's outsourcing of research review, approval, and oversight functions, such as the use of an external or independent Institutional Review Board, does not give rise to a business associate relationship. Lastly, as discussed in more depth below, the Final Rule adopts the NPRM proposal that 50 years is appropriate protection for decedent health information, which has important implications for the research community.

For a more detailed summary of changes relevant to research, please click here.

VI. Changes to Rules Regarding Fundraising

The Final Rule requires covered entities to provide individuals with an opportunity to opt out of receiving fundraising communications. The Final Rule also expands the types of health related information covered entities may use for fundraising purposes, and requires covered entities to make changes to their NPPs to reflect the use of PHI for fundraising purposes.

For a more detailed summary of changes relevant to fundraising, please click here.

VII. Other Miscellaneous Changes to the Privacy Rule

The Final Rule makes a number of additional modifications to the Privacy Rule that will vary in relevance for covered entities and business associates depending upon their business. The additional changes we summarize include those regarding: (i) limited circumstances under which covered entities may sell PHI; (ii) individual rights to request restrictions on uses and disclosures of PHI to health plans, (iii) enhanced rights of individuals to access PHI in electronic form, (iv) protections required on PHI of decedents and (v) permitted disclosure of immunization records to schools.

For a more detailed summary of these changes, please click here.

VIII. Modifications Required Under GINA

GINA requires HHS to make a number of modifications to the Privacy Rule to enhance protection of genetic information for individuals, except with respect to long term care insurance plans. This exception for long term care insurance plans is pending additional review by HHS, based upon concerns that having this information is essential to accurately underwriting long term care.

Please click here for a brief summary of these changes.

Please click here for a compilation of all sections of this alert.