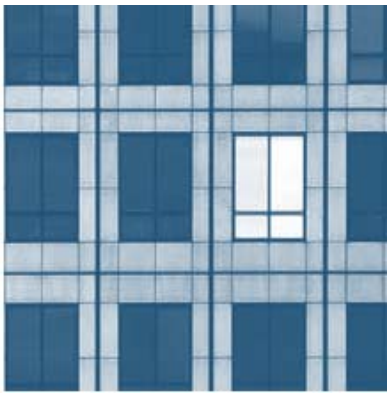
McDermott Will & Emery

On the Subject



Health Industry Advisory

September 7, 2010

The U.S. Department of Health and Human Services (HHS) recently issued proposed HITECH regulations that strengthen and clarify the privacy and security protection obligations with respect to protected health information and expand the requirements that apply to business associates.

HHS Issues HITECH/HIPAA Privacy, Security and Enforcement Guidance

The U.S. Department of Health and Human Services (HHS) recently issued proposed regulations regarding the standards for the protection and security of protected health information (PHI). In addition, on July 29, 2010, HHS announced that final breach notification regulations will be delayed for further consideration in light of the approximately 120 comments the agency received during the public comment period on the interim regulations issued in August 2009.

Background

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established standards for the protection and transmission of PHI. These privacy and security standards were expanded by the Health Information Technology for Economic and Clinical Health Act (HITECH), which was passed as part of the American Recovery and Reinvestment Act of 2009. New proposed HITECH regulations issued by HHS strengthen and expand the privacy and security standards for PHI, revise existing HIPAA regulations to reflect HITECH's changes to the HIPAA Administrative Simplification rules and clarify the enforcement mechanisms for ensuring compliance and the penalties for failures to comply.

Expansion of the Business Associate Relationship and Business Associate Responsibilities

The proposed regulations expand the definition of a "business associate" to include subcontractors of covered entities (persons who provide services to a business associate but are not part of the business associate's workforce) to the extent they require access to PHI. The definition of a business associate also includes specific types of entities, including patient safety organizations and health information organizations that oversee and govern the exchange of health-related information.

Under the proposed regulations, subcontractors are required to comply with the privacy and security rules currently applicable to business associates and are directly liable for violations of rules that apply to business associates. This applies regardless of whether the business associate and the subcontractor had a written contract; however, business associates who work with subcontractors are now required to enter into written agreements, similar to business associate agreements, that require the subcontractors to appropriately safeguard PHI. As such, under the proposed regulations, covered entities must revise their business associate agreements to provide that the business associate will only allow a subcontractor to create or receive PHI on its behalf if the business associate and subcontractor have entered into such a written agreement.

There is a transition rule applicable to the written agreement requirement. If, prior to the publication date of the final regulations (once issued), the covered entity or business associate had an existing contract or other written arrangement with a business associate that complied with provisions of the HIPAA rules then in effect, and such contract or arrangement was not renewed or modified between the effective date and the compliance date of the final regulations, then the requirement to have the business associate and the subcontractor enter into a written agreement can be delayed by up to one year beyond the final regulations compliance date.

The proposed regulations directly regulate business associates, essentially elevating them to covered entity status. For example, business associates are now required to have their own HIPAA policies and procedures. Nevertheless, a business associate agreement is still required between a covered entity and a business associate. The proposed regulations clarify the restrictions on the use and disclosure of PHI by business associates that are not subject to a business associate agreement. If there is no business associate agreement in place, a business associate must nonetheless limit its use and disclosure of PHI to those activities necessary to perform its obligations for the covered entity or as required by law. Other restrictions on the use and disclosure of PHI are also extended to business associates, including the requirement to disclose PHI to the secretary of HHS to investigate or determine compliance with HIPAA and the requirement to use and disclose only the minimum necessary PHI.

Protection of Deceased Individuals' PHI

Under current HIPAA privacy regulations, a deceased individual's PHI is afforded the same protections as apply to a living individual's PHI. However, in recognition that it can be difficult to locate a personal representative of a decedent, especially once an estate has been closed, the proposed regulations modify the definition of PHI to exclude the individually identifiable health information of persons who have been deceased for more than 50 years. The proposed regulations also clarify that a covered entity may disclose a decedent's information to family members and others who were involved in the care and payment for care prior to the decedent's death.

Increased Individual Access to Electronic Information

Under the proposed regulations, covered entities must provide individuals greater access to electronically stored information. HITECH added special access rules for covered entities that use or maintain an electronic health record on an individual. An electronic health record is defined under HITECH as an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff, so it appeared unlikely that a health plan would be subject to these rules. The proposed regulations expand this right of access to apply to all PHI in a designated record set that is maintained in electronic form. A designated record set includes the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan and other records used by a health plan to make decisions about an individual. Under the proposed regulations, a covered entity must provide an individual with an electronic copy of PHI electronically maintained in a designated record set in the form and format requested by the individual if readily producible, or in an otherwise agreed to form and format. In addition, the covered entity must transmit a copy of the electronic PHI directly to another person designated by the individual. Business associates that maintain PHI in electronic format are also directly obligated to comply with these expanded access rules under the proposed regulations. The proposed regulations clarify the rules for charging a requesting individual for the provision of PHI in electronic format.

Enhanced Civil Penalties

HITECH established four tiers of penalties based on level of culpability for violations that are greater than the previous HIPAA rules. The proposed regulations clarify the demarcations between these categories of culpability. In addition, covered entities and business associates face a greater risk of liability for violations of HIPAA and HITECH under the proposed regulations. Currently, a covered entity is exempt from liability for a business associate's violation if that covered entity has a compliant business associate contract in place, did not know of a pattern or practice of violation by the business associate and took appropriate steps upon discovery of the business associate's violation. The proposed regulations remove this exception, making a covered entity liable for civil penalties due to a business associate's (or a business associate subcontractor's) violation, regardless of whether there was a compliant contract in place or whether the covered entity knew of the violation or acted appropriately in response to it. The proposed regulations also provide that business associates are liable, under the federal common law of agency, for violations of their workforce members and subcontractors.

Additional Requirements for the Notice of Privacy Practices

Under the proposed regulations, a covered entity must include a description of certain types of uses and disclosures of PHI that require an authorization in its notice of privacy practices (i.e., psychotherapy notes, marketing, and sale of PHI). The notice should specifically describe an individual's right to request restrictions on the use and disclosure of PHI, including a statement that the covered entity must agree to a request to restrict disclosure to a health plan if the disclosure is for payment or health care operations purposes and pertains solely to a health care item or service that was paid by a person or entity other than the covered entity. Although this type of change would require a covered entity to distribute an updated notice to individuals within 60 days of a material change under current rules, HHS recognized that this requirement can be burdensome and costly,

and thus requested comment on several alternate timing proposals for informing individuals of these changes.

Implementation of HITECH Marketing and Sales Restrictions

The proposed regulations clarify that a refill reminder or other communication about a drug or biologic currently being prescribed for the individual is not marketing subject to HIPAA restrictions as long as any financial reimbursement received by the covered entity is reasonably related to the covered entity's cost of making the communication. Under HIPAA rules, communications for certain treatment purposes or for health care operations activities are also not considered marketing, except if the covered entity receives financial remuneration in exchange for making the communication. The preamble to the proposed regulations clarifies that communications made by health plans relating to health-related products or services provided under the plan or for case management or care coordination purposes are never considered "treatment" and would require individual authorization if any financial remuneration is paid to the plan.

Delay of Breach Notification Regulations

HHS previously issued the Interim Final Rule for Breach Notification for Unsecured Protected Health Information (published in the Federal Register on August 24, 2009), which became effective on September 23, 2009. After reviewing public comments submitted on the Interim Final Rule, HHS developed a final rule that was submitted to the Office of Management and Budget (OMB) for regulatory review on May 14, 2010. Then, in an unusual move, HHS announced it was withdrawing those final regulations from OMB review for further consideration on July 29, 2010. Final breach notification issues are expected in the coming months. In the meanwhile, the Interim Final Rule continues to apply.

Next Steps

HHS has requested comments on the proposed HITECH regulations on or before September 13, 2010. Once the final regulations are issued, HHS has indicated that covered entities will generally have 180 days to comply with the new rules. HHS also indicated that there would be no additional delay of the application of the regulations, once finalized, to small health plans.

As noted above, the proposed regulations expand the requirements that apply to business associates. If the final regulations contain similar provisions, then covered entities will have to revise their business associate agreements accordingly. HHS has proposed a transition rule based on the grandfathering of previous agreements, as discussed above.

While no action is required at this time, covered entities should ensure they have proper HIPAA privacy and security policies and procedures in place, and have identified and entered into business associate agreements with all business associates. The final HITECH regulations will likely place additional administrative demands on covered entities and require modifications to their policies and practices to ensure continued compliance with HIPAA and HITECH. Covered entities will also have to review HIPAA policies and procedures and business associate agreements once final breach notification regulations are issued.

For a more detailed summary of these proposed regulations, see "OCR Issues Proposed Modifications to HIPAA Privacy and Security Rules to Implement HITECH Act" at http://www.mwe.com/info/news/wp0710c.pdf

For more information, please contact your regular McDermott lawyer, or:

Amy M. Gordon: +1 312 984 6931 agordon@mwe.com

Jamie A. Weyeneth: +1 312 984 6913 jweyeneth@mwe.com

Maggie McTigue: +1 312 984 5812 mmctigue@mwe.com

For more information about McDermott Will & Emery visit: www.mwe.com

IRS Circular 230 Disclosure: To comply with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained herein (including any attachments), unless specifically stated otherwise, is not intended or written to be used, and cannot be used, for the purposes of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter herein.