Health Industry Alert

January 25, 2013

Health Sector Braces for Wide Impact of Newly Released HITECH Omnibus Rule

On January 17, 2013, the Department of Health and Human Services (HHS) released the much-anticipated final omnibus rulemaking, implementing key privacy, data security, data breach notification and enforcement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. HITECH overhauled the existing health information privacy and security regime that had been in effect since 2003 under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The final HITECH rule makes major changes to the existing regime, creating significant new risks and obligations for health entities and the service providers that support them. Many affected entities will have much work to do to come into compliance. HHS has proven that it will not shy away from enforcement action; affected entities are generally afforded until only September 23, 2013 to come into compliance, so prompt action will be important for many of the entities that fall within the reach of this expansive rule.

KEY PROVISIONS OF THE FINAL HITECH RULE

Compliance officers, privacy officers, general counsel, chief operating officers and other executives across the nation began adding to their "to do" lists this week, contemplating the many steps they would need to take to come into compliance with the newly released final HITECH rule. Even entities that are currently in full compliance with HIPAA will have serious work to do to bridge the gap between the old HIPAA and the new. Entities that only recently discovered or embraced their business associate status will certainly have a busy year. This alert highlights the privacy, data security and breach notification provisions of the final HITECH rule that warrant prompt attention and provides some ideas for steps affected entities may want to take.

A New World for Business Associates and Their Subcontractors. When it comes to business associates, the HITECH Act and final HITECH rule are a total game-changer. Once the compliance deadline for the final HITECH rule comes, business associates will face direct liability for HIPAA violations on top of existing contractual liability. The final HITECH rule adopted an expansive definition of "business associate," compounding the effect of this change.

Under the original HIPAA regime, a business associate was, generally, a vendor or other service provider that used or disclosed HIPAA-protected health information (PHI) in the course of performing a function or service for or on behalf of a hospital, health plan, clearinghouse or other covered health care provider. Under the final HITECH rule, a business associate includes any person or entity that creates, receives, maintains or transmits PHI on behalf of a covered entity to provide a service (such as claims processing or data analysis) for the covered entity. With the inclusion of one key word — maintains — the agency removed any doubt as to whether entities that store PHI on behalf of covered entities (including cloud

providers) must contend with the rule. In addition to service providers who receive PHI in order to perform tasks for the covered entity, providers of personal health records that act on behalf of covered entities will be considered business associates. The final HITECH rule also specifies that health information organizations and e-prescribing gateways will be considered business associates, as will any other entity that provides data transmission services to a covered entity involving PHI and that requires routine access to such information. Importantly, a subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate is also treated as a business associate.

In addition to abiding by the terms of their business associate agreements, all business associates will need to comply directly with the HIPAA security rule and with many HIPAA privacy requirements. The agency clarified that business associates will be directly liable for certain privacy provisions of HIPAA, including:

- uses and disclosures of PHI that are not in accord with their business associate agreements or the HIPAA privacy rule
- failure to disclose PHI when required by the Secretary of HHS to do so to allow the Secretary to investigate and determine the business associate's own HIPAA compliance
- failure to disclose PHI in response to an individual's request for access (including a request for access to an electronic copy of PHI) in a manner consistent with the business associate agreement
- failure to provide an accounting of disclosures
- failure to satisfy the minimum necessary standard
- failure to provide breach notification to the covered entity
- failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf.

The final HITECH rule also adjusted the list of mandatory terms that must be included in business associate agreements. Compliant agreements in place on January 25, 2013 will be deemed compliant until September 23, 2014, unless the arrangement is modified or actively renewed between March 26, 2013 and September 23, 2013. To the extent that a business associate agreement is missing entirely, one that complies with the final HITECH rule will need to be executed by September 23, 2013.

Overhaul of Data Breach Notification Requirements. HITECH established an expansive protocol for providing notice in the event of a breach involving an individual's unsecured PHI. The interim final HHS HITECH Breach Notification Rule created a harm threshold, which allowed covered entities and business associates to forego notification if they determined that an incident posed little or no risk of harm to the individual. The interim final rule also included a narrow exception for incidents involving limited data sets.

The final HITECH rule eliminates the harm threshold and creates a presumption of data breach, and eliminates the exception for limited data sets.

- ***Risk of Harm Replaced with a More Objective Threshold***. HITECH defined a "breach" as the "unauthorized acquisition, access, use or disclosure of [PHI] which *compromises* the security or privacy of such information . . ." (emphasis added). The interim final rule took the position that PHI is "compromised" only if there is a significant risk of financial, reputational or other harm to an individual. Despite the fact that the vast majority of comments HHS received supported the risk of harm threshold, the final HITECH rule did away with the threshold, calling it "too subjective." In its place, the final HITECH rule creates a rebuttable presumption that a security incident will qualify as a breach and trigger notification obligations unless the covered entity or business associate can demonstrate that there is a "low probability" that the PHI has been "compromised."

- ***Factors for Risk Assessment***. The final HITECH rule provides that covered entities and business associates who experience a security incident must assess the probability that the PHI has been compromised. This assessment must consider at least the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. In the final HITECH rule, HHS indicated that it will issue additional guidance to aid covered entities and business associates in performing these types of risk assessments.

- ***Elimination of Exception for Limited Data Sets***. The interim final rule had provided that an impermissible use or disclosure of PHI that qualifies as a limited data set but excludes dates of birth and zip codes does not compromise the security or privacy of PHI and thus does not trigger breach notification obligations. The final HITECH rule eliminates this narrow exception, and incidents involving these types of data sets must undergo the same risk assessment as required for other incidents.

- ***Notification Protocol***. The final HITECH rule made no material modifications to the interim final rule's provisions governing when a breach is discovered, timeliness of notifications, content of notifications and methods of notification.

Flexibility for Fundraising. The final HITECH rule allows covered entities to use more granular data to target their fundraising communications, without authorization, than what HIPAA previously allowed. Under the old regime, covered entities could only use demographic information and dates of service for fundraising purposes. Under the final HITECH rule, if certain conditions are met, covered entities will be able to use demographic information relating to an individual (including name, address, other contact information, age, gender and date of birth), dates of service, health insurance status, department of service, treating physician and outcome information for fundraising purposes. HHS emphasized that covered entities must still apply the existing minimum necessary standard to any uses or disclosures of PHI, including those for fundraising purposes.

To take advantage of this flexibility, covered entities must include language in their notices of privacy practices alerting individuals that they may be contacted for fundraising purposes and informing individuals that they have a right to opt out of such communications. Each fundraising communication must also provide a "clear and conspicuous" opportunity to opt out from future targeted fundraising communications. Additionally, while the prior regulations required covered entities to make "reasonable efforts" to ensure that individuals do not receive such communications after opting out, the final HITECH rule states that covered entities are prohibited from making such communications. HHS emphasized that covered entities which choose to send fundraising communications to individuals must have data management systems in place to track and flag those who opted out. Individuals who have opted out, however, may be given an opportunity to opt back in to receive targeted fundraising communications.

Restrictions on the Sale of PHI. HITECH required covered entities and business associates to obtain authorization in order to disclose PHI for "direct or indirect" remuneration, subject to certain exceptions. The final HITECH rule expands upon the list of exceptions, providing "carve-outs"for public health purposes, research purposes (where the only remuneration is a reasonable cost-based fee to cover the cost to prepare and transmit the information), treatment purposes, in instances of the sale, merger, transfer, or consolidation of the covered entity and related due diligence, to allow individuals to access or obtain an accounting of disclosures of their PHI, payment purposes, activities required by law, to allow disclosure to business associates (where the business associate is paid for its services and not for the data), and for any purpose permitted by the HIPAA privacy provisions (provided the only remuneration received is a reasonable, cost-based fee to cover the cost of preparing and transmitting the information).

The agency also attempts to clarify the definition of "sale of PHI," stating that "sale" includes not only the transfer of ownership of data, but also access, license or lease agreements. HHS explained that "sale" does not include payments in the form of grants, nor does it encompass contracts or other arrangements to perform programs or activities (such as research studies) that involve the provision of PHI to the payer as a byproduct of other services. HHS also noted that a covered entity or business associate that wishes to re-disclose PHI received as a result of a sale for a non-excepted purpose must obtain authorization, unless the original authorization makes it sufficiently clear to the individual that the recipient may re-disclose the information.

Changes to Marketing. Under HIPAA, covered entities must obtain a valid authorization from individuals before using or disclosing PHI for marketing purposes, unless certain exceptions apply. Prior to HITECH, HIPAA provided several important "carve-outs" from the definition of marketing—for "treatment" communications and certain "health care operations" communications—that allowed covered entities to communicate with individuals without first obtaining authorization. HITECH sought to limit the types of communications about health-related products or services that may be considered "health care operations" under HIPAA—and thus would be excepted from the definition of marketing under HIPAA—in situations where a covered entity receives direct or indirect payment in exchange for making the communication (i.e., a "sponsored" communication). HITECH made an exception for communications that describe a drug or biologic that is currently being prescribed (e.g., a refill reminder) and provided that

such communications are not "marketing" so long as the payment made to a covered entity was "reasonable in amount."

Noting that HITECH omitted any reference to communications that can be considered "treatment" under HIPAA, the proposed HITECH rule distinguished between sponsored communications made for treatment purposes and sponsored communications made for health care operations purposes, and proposed to require authorization only for communications falling within the latter category.

The final HITECH rule shifted from this interpretation, citing ambiguity in the statute and the alleged difficulty in distinguishing treatment communications from health care operations communications, and will require covered entities to secure authorization even for those communications that are considered treatment where a third party is sponsoring the message—unless an exception applies. Importantly, HITECH left intact the exception to the authorization requirement for marketing communications that are "face-to-face." This exception will allow covered entities such as pharmacies and physicians' offices to continue communicating directly with patients orally or through written materials, even if those communications are paid for by third parties. Further, communications regarding refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, are also permitted under HITECH without authorization provided any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication.

Expanded Individual Rights. HITECH required covered entities to comply with an individual's request that his or her PHI not be disclosed for payment or health care operations if the PHI pertains solely to an item for which the individual has paid the health care provider out of pocket and in full. Additionally, HITECH required covered entities to grant individuals access to their electronic PHI. The proposed HITECH rule addressed how covered entities were to comply with the access and disclosure requirements, and would have required covered entities to revise their notices of privacy practices. The final HITECH rule clarifies that, while certain updates to the notice of privacy practices, described below, are needed, providers are not required to prepare and distribute off-cycle paper notices. Rather, providers must conspicuously post the revised notice and have copies available upon request at the site of care delivery. Health plans that have websites are required to post notice of privacy practices revisions on their websites by September 23, 2013, and to provide paper copies to members in the next annual mailing. Health plans without websites must provide the revised notice, or information about material changes to the notice and how to obtain a copy of the revised notice, by November 23, 2013.

- ***Notice of Privacy Practices***. The final HITECH rule requires that the notice of privacy practices include a description of the types of uses and disclosures that require authorization. In addition, the final HITECH rule provides that if a covered entity engages in certain listed activities, the notice of privacy practices must include separate statements, including: (1) that a covered entity may contact the individual to raise funds for the covered entity, and the individual may opt out of such communications; and (2) if a covered entity that is a health plan intends to use or disclose PHI for underwriting, it must include a statement that the covered entity is prohibited from using or disclosing

PHI that is genetic information. The final HITECH rule also requires that covered entities add a statement that the covered entity is required by law to notify affected individuals following a breach of unsecured PHI.

- ***Access to PHI***. The final HITECH rule maintains the requirement from the proposed HITECH rule that if a covered entity maintains a designated record set electronically, and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily available in such form. If it is not, the covered entity must provide the information in a readable electronic form and format as agreed to by the covered entity and the individual.

- ***Right to Stay "Off the Grid*."** The final HITECH rule requires that a covered entity abide by an individual's request to restrict disclosure of PHI to the individual's health plan where the individual chooses to pay for care out of pocket, if certain conditions are met. First, disclosure will only be limited to the extent that it is for the purpose of carrying out payment or health care operations and is not otherwise required by law. Second, the PHI that will be restricted must pertain solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full. This requirement may pose technological challenges for many covered health care providers.

Compound Authorizations for Research Permitted. Under the final HITECH rule, authorization for use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This new exception includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with informed consent under the Common Rule to participate in clinical research. In the final rulemaking, HHS requires such compound authorizations to "clearly differentiate" between an authorization that conditions research-related treatment, payment, enrollment in a health plan, or eligibility for other benefits on use or disclosure of PHI, and an unconditioned authorization. For example, covered entities would not be prohibited from using the same authorization for use or disclosure of PHI for treatment as part of a clinical trial and for tissue banking of specimens. HHS stated that compound authorizations must clearly allow individuals to opt in to unconditioned research activities.

The rulemaking also confirms HHS's intent to allow covered entities flexibility in designing the authorization. For example, unconditioned research could be described on a separate page or in a separate brochure incorporated by reference into the authorization, and the authorization could have one signature line with a check-box for participation in the unconditioned research or separate signature lines for each type of research activity.

The final HITECH rule also clarified that compound authorizations may be used for any type of research except to the extent the research involve the use or disclosure of psychotherapy notes; HHS stated that

authorizations for use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.

Authorizations Can Cover Future Research. The proposed HITECH rule requested comments on how authorizations should describe uses and disclosures for future research to ensure that individuals were able to knowingly consent. The final HITECH rule modified HHS's prior interpretation that authorizations for use or disclosure of PHI must be "study-specific" to comply with HIPAA's requirement that authorizations include a description of each purpose of the use or disclosure. HHS now indicates that authorizations may cover uses and disclosures for future research so long as the future research purposes are described such that it would be reasonable for the individual involved to expect that his or her PHI could be used or disclosed for future research. HHS also clarified that covered entities have the flexibility to describe information used for future research, which may include information collected beyond the time of the original study.

Limits on Protection for Decedents' Health Information. The final HITECH rule amends the HIPAA privacy rule to exclude individually identifiable information from the definition of PHI 50 years after an individual's death. While HHS promulgated the change in response to comments addressing the difficulties researchers faced in securing authorization for information that could be decades old, the amendment applies to information used or disclosed for any purpose. Additionally, the final HITECH rule allows covered entities to share PHI with individuals involved in a decedent's health care or payment for health care prior to death so long as the information relates to such involvement and sharing the information in this manner would not be inconsistent with any preferences known to the covered entity to have been previously expressed by the deceased individual.

ACTION ITEMS FOR AFFECTED ENTITIES

The final HITECH rule will have a major impact on many health sector participants. For starters, covered entities and business associates will need to take a step back and evaluate the impact of the final rulemaking on their operations. For some, this may involve engaging in a renewed analysis of the entity's HIPAA status. Some entities may be surprised to find, for example, that, upon examining their operations closely, some divisions or subsidiaries may be handling PHI (or paying for health care) in a manner that triggers HIPAA compliance obligations.

Virtually all affected entities would be well-served by reexamining their data flows. Indeed, as entities move forward in the coming months, it will be important for them to be sure they "know their flows" — that is, that they understand how their organization presently collects, creates, uses, discloses, transmits, maintains, stores and disposes of PHI. Entities should ask detailed questions that focus on the complete life cycle of their data, such as who in their organization handles PHI and for what purposes, where PHI is stored, how it is secured, with whom it is shared and why, and when and how it is disposed. Once data flows are understood, the risk analysis should be updated.

Written HIPAA compliance programs will need to be prepared or updated, depending on where an entity is in its HIPAA compliance journey. While covered entities may be engaging in a gap analysis exercise

over the coming months, many business associates may have a lot more work to do to come into compliance. Previously, their liability was limited to the four corners of their business associate agreements. Once the compliance date for the final HITECH rule arrives, they will need to answer directly to governmental authorities enforcing HIPAA, as well as to their contracting partners. Business associates that are in the earlier stages of their HIPAA journeys may find it helpful to start by developing policies and procedures, tailored to their business practices, that operationalize fully any promises that may have been made in existing business associate agreements, and by reaching out to downstream subcontractors to get necessary agreements in place.

For entities that already have robust and carefully tailored HIPAA compliance programs in place, policies and procedures sure to warrant attention include those concerning marketing, sale of PHI, research and breach notification, among many others. Forms will need to be updated, as will many internal instructions for when and how those forms are to be used. For instance, business associate agreements, access request forms and notices of privacy practice will require revisions. Business operations and policies developed to accommodate HITECH breach notification requirements will need attention; for example, internal decision analysis tools for determining when a breach has occurred will need to be overhauled.

With all of the excitement around the final HITECH rule, affected entities should be careful to remain focused on HIPAA-related priorities they may have identified in the days and weeks before the new rule was released. For example, efforts to reinvigorate workforce training programs, identify encryption technologies that make sense in an entity's environment, and make sure that appropriate policies and procedures are in place to avoid data incidents involving PHI stored on laptop computers and other mobile devices, are as important — if not more important — than they were before the final HITECH rule was released.

ADDITIONAL INFORMATION

For a review of HITECH, the proposed HITECH rule and the interim final HHS Breach Notification Rule, please click here, here and here to see our earlier alerts. For more on the final HITECH rule, or for assistance addresfsing privacy, data security or breach notification issues generally, please contact:

Contact Information

If you have any questions regarding this alert, please contact:

Jorge Lopez, Jr.
jlopez@akingump.com
202.887.4128
Washington, D.C.

Kelly Cleary
kcleary@akingump.com
202.887.4329
Washington, D.C.

Anna R. Dolinsky
adolinsky@akingump.com
202.887.4504
Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Mara McDermott
mmcdermott@akingump.com
202.887.4337
Washington, D.C.

