Compliance Advisory:

HITECH Final Rule

MEADE ROACH & ANNULIS
HEALTH CARE ATTORNEYS

January 2013

HHS Publishes Omnibus HITECH Final Rule

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) released a much-anticipated omnibus final rule (the Final Rule) implementing the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). The Final Rule was published in the Federal Register on January 25, 2013. 78 Fed. Reg. 5566 (Jan. 25, 2013). The Final Rule contains many expected changes; however, the Final Rule also contains some unanticipated (and, in some cases, unwelcome) surprises.

1. Scope

The Final Rule effectuates modifications to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) that were required by HITECH. Specifically, the Final Rule modifies and integrates the following previously published sets of rules: (a) a proposed rule (the Proposed Rule) concerning HITECH changes to HIPAA, published July 14, 2010; (b) the interim final rule addressing breaches involving unsecured protected health information (PHI), published August 24, 2009 (the Breach Notification Rule); (c) the interim final rule adopting HITECH changes to the HIPAA enforcement rules, published October 30, 2009 (the HIPAA Enforcement Rule); and (d) the final rule modifying HIPAA as required by the Genetic Information Nondiscrimination Act of 2008 (GINA), published October 7, 2009, which primarily impact health plans and employers. The Final Rule does not address the notice of proposed rulemaking concerning accounting of disclosures or access rights, published May 31, 2011.

The Final Rule will require covered entities and business associates to change their breach notification policies and procedures and, in many instances, their business associate agreements. Covered entities may also be required to amend their Notice of Privacy Practices (NPPs) and their health information privacy and security policies and procedures.

2. Key Dates

Many of the changes to HIPAA (e.g., tiered civil money penalties) that were required by HITECH were effective upon enactment of the statute (i.e., February 17, 2009). Other provisions of HITECH are not effective until such time as HHS publishes final implementing regulations. The Final Rule is effective as of March 26, 2013. However, as indicated in the Proposed Rule and as was the case with the original HIPAA Rules, in recognition of the fact that it will take time for covered entities and business associates to implement some of the changes required by the Final Rule, HHS provides that it will not enforce the Final Rule until 6-months after the effective date (i.e., September 23, 2013) (the Compliance Date). Further, as discussed more fully below, covered entities and business associates that have valid business associate agreements in place as of the Final Rule's publication date (January 25, 2013) will have up to 12-months from the Compliance Date (i.e., September 23, 2014) to replace or update their current business associate agreements with agreements that comply with the Final Rule. Any existing business associate agreements that are renewed or modified prior to September 23, 2014 must conform to the Final Rule at that time. Ideally, all new business associate agreements entered into after January 25, 2013 will conform to the Final Rule upon execution, but in any event no later than September 23, 2013.

- *Effective Date = March 26, 2013*
- *Compliance Date = September 23, 2013*
- *HITECH Compliant BAAs required for BAAs in effect as of January 25, 2013 = no later than September 22, 2014*

3. Business Associates.

a. One of the biggest changes required by HITECH was the direct application of HIPAA to business associates. Prior to HITECH, a business associate's HIPAA obligations were dictated solely by the applicable business associate agreement. As of the Compliance Date, most of the Security Rule, Privacy Rule and Breach Notification Rule (as revised) apply directly to business associates. However, HHS makes it clear that such direct application does not alleviate the need for a business associate agreement; rather, if a business associate improperly uses or discloses a covered entity's PHI, the business associate may be in violation of both the operative business associate agreement and HIPAA.

If you are a business associate and you have not already begun to develop and implement a health information privacy and security program, you should start—now.

b. In addition to the direct application of HIPAA to business associates, the Final Rule also expands the definition of business associates to specifically include HIOs, e-prescribing gateways and other persons that provide data transmission services including PHI. HHS construes such entities as more than mere conduits of information.

c. Under the Final Rule, HHS adds a definition of subcontractor and specifies that business associate obligations extend to a business associate's subcontractors, such that business associate obligations continue downstream for so long as there is PHI involved.

Covered entities need to make certain that their business associate agreements obligate their business associates to bind the business associate's subcontractors and business associates need to make certain to obligate their subcontractors to protect and secure any PHI received, maintained or transmitted by the subcontractor.

d. The Final Rule also modifies the definition of business associates to include vendors that "maintain" PHI on behalf of a covered entity, even if those vendors do not routinely access any PHI. In the past, storage vendors (including many electronic hosting entities) have argued that they are not business associates if they do not "access" a covered entity's PHI. As of the Compliance Date, that argument may no longer be valid. The HHS commentary indicates that anything more than "transient" or "temporary" storage (such as may be the case with an ISP) triggers business associate status. A storage vendor/hosting services provider may only be able to argue that it does not have "access" to PHI if that PHI is encrypted and the vendor does not have the encryption key. This may have particular significance for cloud service providers offering storage services to covered entities.

HHS' decision to expand the definition of business associates to include entities that "maintain" PHI on behalf of covered entities could have significant implications for hosting services and cloud service providers. Covered entities should review contracts and business arrangements with those vendors.

4. Security Rule

The Final Rule does not significantly change or modify the Security Rule, aside from its direct expansion to business associates. However, publication of the Final Rule should serve as a reminder to covered entities and business associates of the need to conduct or update the required Security Rule risk analyses. The recently released preliminary results of OCR's HIPAA compliance audits indicate that many covered entities have not conducted the required risk analyses.

5. HIPAA Enforcement Rule

The most significant change to the HIPAA Enforcement Rule made by the Final Rule is that HHS will investigate complaints about covered entities or business associates where a preliminary review indicates a possible violation due to willful neglect. Other compliance reviews are permissive. The Final Rule also makes it clear that a covered entity may be liable for the actions or inactions of its business associate in accordance with the federal common law of agency.

6. Marketing Communications

Under HIPAA, covered entities are restricted in how they can use and disclose PHI for marketing. The Final Rule implements HITECH and imposes further restrictions on marketing activities by covered entities and their business associates. Except for marketing in the form of face-to-face communications or involving promotional gifts of nominal value, the Final Rule makes it clear that if marketing involves financial remuneration from a third party whose product or service is being promoted, written authorization is required. The covered entity's NPP must also be revised to reflect such activity. However, the Final Rule retains the standalone exemption to marketing for communications about refill reminders and drugs or biologics currently prescribed for an individual, but only if any remuneration received by the covered entity for making the communication is cost-based. HHS has indicated that it intends to provide future guidance with respect to the scope of the exemption regarding refill reminders and drugs or biologics.

7. No Sale of PHI

HITECH and the Proposed Rule imposed significant restrictions on a covered entity's sale of PHI. With limited exceptions, a covered entity is prohibited from selling PHI without individual authorization. Sale is broadly defined to include license rights. Thus, there need not be a transfer of ownership of PHI for there to be a sale under HIPAA. There are exceptions to this prohibition for, among other things, research activities. However, the research exception is limited. Specifically, a covered entity may sell/license PHI in the form of a limited data set to a third party for research without individual authorization but only if the remuneration received is "a reasonable cost-based fee to cover the cost to prepare and transmit the [PHI] for such purposes." Thus, a covered entity cannot profit from the disclosure of PHI in the form of a limited data set to researchers for research activities. Because this prohibition applies only to PHI, it would not apply to the sale or license of de-identified health information (which is not PHI). The practical consequence of this provision for covered entities is:

a. If you rely upon data use agreements to disclose limited data sets of PHI for research, you need to ensure that those agreements comply with the Final Rule (i.e., remuneration received is limited to a reasonable cost-

based fee). In recognition of the practical consequences imposed by this change, if covered entities have data use agreements in place as of the publication date of the Final Rule (January 25, 2013), the Final Rule permits covered entities to continue with those agreements until such time as those agreements are renewed, but no later than September 23, 2014;

b. If you disclose PHI in the form of a limited data set to a third party for health care operation activities (e.g., quality assurance or assessment, receipt of a product discount/rebate) and receive some form of remuneration, there is no exception to the individual authorization requirement. As of the Compliance Date, you must discontinue this disclosure of PHI for remuneration without individual authorization.

c. Consider whether you can accomplish the intended purpose of disclosures for research or health care operation activities involving remuneration through the disclosure of de-identified health information, as the prohibition on the sale of PHI does not apply to de-identified health information.

Covered entities need to carefully consider the prohibition on the sale of PHI and how it might apply to them and their business activities.

8. Compound Authorizations for Research

In response to public comments and recommendations from various federal advisory committees, the Final Rule makes it clear that authorizations for research may include an authorization for use and disclosure of PHI for a particular research study, as well as an authorization for the future use and disclosure of blood and/or tissue specimens (and attendant PHI) as part of a biorepository. This is welcome news for researchers and covered entities seeking to establish and operate biorepositories.

9. Fundraising

The Privacy Rule restricts a covered entity's (and its business associates') use and disclosure of PHI for fundraising. The Final Rule expands the list of PHI that may be used and disclosed by a covered entity and its business associate without individual authorization for fundraising to include department of service, treating physician, outcome information and health insurance status. The Final Rule also makes it clear that the demographic information that a covered entity is permitted to use and disclose for fundraising without individual authorization includes name, address, contact information, age, gender and DOB. Covered entities had previously complained about the limited types/categories of PHI that they could use and disclose without individual authorization for fundraising. The Final Rule also sets forth an absolute prohibition for fundraising communications where the individual has opted-out of receiving such communications.

10. Notices of Privacy Practices

Covered entities will likely need to amend their NPPs to address some of the changes required by HITECH and the Final Rule. For example, a NPP will need to address the covered entity's obligation to obtain individual authorization for the use and disclosure of PHI for marketing, and the sale of PHI. Covered entities will also need to address breaches involving unsecured PHI in their NPPs and the right of persons to opt-out of receiving fundraising communications. Covered health care providers will need to address an individual's right to request a restriction on certain disclosures to health plans (see below). Health plans that use PHI for underwriting purposes will need to address restrictions on the use and disclosure of genetic information as required by GINA (see below). Readers should note that health plans have different distribution/publication requirements for revised NPPs than health care providers.

11. Right to Request a Restriction on the Use and Disclosure of PHI

Under HIPAA, an individual may request that a covered entity restrict how it uses and discloses the individual's PHI; however, the covered entity need not agree to that request. HITECH changes that. Under HITECH, a covered health care provider must agree to a restriction request for disclosure of PHI if the disclosure would be to a health plan for payment or health care operation purposes and the individual agrees to pay-out-of pocket for the underlying product or services. The proposed implementation of this change raised many questions. The Final Rule attempts to answer those questions. Concerns were raised about the ability of a provider to unbundle services and split bills. In response, HHS advises that health care providers need to counsel patients as to issues implicated by unbundling claims and split billing and, if possible, accommodate the patient's wishes. In regard to downstream and other providers (e.g., pharmacies, therapists), HHS advises that it is the individual's ultimate responsibility to manage restriction requests, but HHS encourages providers to counsel patients as to the issue. For individuals insured by HMOs, HHS makes it clear that if participating providers are precluded by law or contract from accepting out-of-pocket payment from individuals for covered services, then the provider may inform the individual that she would need to obtain the product/service out-of-network. HHS also advises providers that they may require payment in full at the time of the restriction request in order to avoid collection and pre-certification requirements.

Despite HHS' efforts to clarify how the out-of-pocket payment provision is to be implemented, providers will need to work through implementation issues prior to the Compliance Date.

12. Right to Access

In the Final Rule, HHS eliminates the provision that allows covered entities up to 60 days to provide access for PHI that is not maintained on-site. Access for all designated record sets must be provided within 30-days. The Final Rule does not address the proposed access right set forth in the notice of proposed rulemaking published on May 31, 2011. That issue (along with the expanded

right to receive an accounting of disclosures) will be addressed at a later date.

13. Breach Notification Rule

One of the more significant changes made by the Final Rule concerns a covered entity's duties and obligations involving a breach of unsecured PHI. HHS had previously addressed this issue in the Breach Notification Rule. The Breach Notification Rule was effective as of September 23, 2009. In the Breach Notification Rule, HHS indicated that there was a breach of unsecured PHI if there was an impermissible use or disclosure that "compromises the security or privacy of [PHI]." "Compromises the security or privacy of [PHI]" was further defined as "poses a significant risk of financial, reputational or other harm to the individual." Determining whether there was a significant risk of financial, reputational or other harm became known as the harm threshold analysis. In the Final Rule, HHS abandons the harm threshold analysis. HHS argues that the harm threshold analysis was too subjective and that covered entities were abusing the process. In its place, HHS establishes a presumption that all impermissible uses and disclosures of unsecured PHI are breaches unless the covered entity (or business associate) can establish that there is a "low probability that the PHI has been compromised" (emphasis added). In order to establish that there is a low probability that the PHI has been compromised, covered entities (and business associates) must take into account (at least) these four factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk to PHI has been mitigated.

As a practical matter, the four "objective" factors that a covered entity (or business associate) must consider to determine if there is a low probability that the PHI has been compromised are the same "subjective" factors that were considered in deciding whether there was a significant risk of financial, reputational or other harm. However, as of the Compliance Date, covered entities (and business associates) cannot ignore the presumption of a breach and the "low probability" versus "significant risk" language. In other words, the burden shifts to the covered entity to prove (or have a strong argument) that there was either no unauthorized use or disclosure of PHI, or at least a low probability of such a compromise.

The Final Rule significantly changes the Breach Notification Rule. As of the Compliance Date, covered entities and business associates must presume there is a breach involving unsecured PHI unless the covered entity or business associate can establish a "low probability" that the unsecured PHI was compromised. Such a determination will require careful analysis and documentation by the covered entity or business associate. Covered entities and business associates may be more motivated to encrypt PHI so as to make it "not unsecured."

14. GINA

The Final Rule implements changes to the Privacy Rule required by GINA. Among other changes, the Final Rule defines health information to include genetic information. The changes are significant for health plans and employers. Employers may not use genetic information to discriminate against employees. In regard to health plans, the Final Rule prohibits health plans (other than issuers of long-term care policies) from using or disclosing genetic information for "underwriting" purposes.

If you have any questions about this Client Advisory, the Final Rule or your health information privacy and security program, please contact:

Brian D. Annulis at 773.907.8343 or bannulis@meaderoach.com

Ryan D. Meade at 773.697.3882 or rmeade@meaderoach.com

Michael C. Roach at 773.697.3883 or mroach@meaderoach.com

Julie A.M. Fisher at 773.510.0132 or jfisher@meadeoach.com

Stephen J. Weiser at 312.403.4284 or sweiser@meaderoach.com