PUBLICATION

It's Coming: The HIPAA/HITECH Rule; What To Expect and What To Do Now [Ober|Kaler]

2012: Issue 6 - Focus on HIPAA/Privacy

On March 24, 2012, the Department of Health and Human Services (HHS) sent the much-anticipated rule implementing the HITECH Act changes to HIPAA (HITECH Rule) to the Office of Management and Budget (OMB). This starts the clock running on the 90-day period allowed for OMB review. It is expected that, given the scope of the regulations, OMB will take most, if not all, of its allotted 90 days. In any event, the HITECH Rule is expected by late June 2012. While the authors have noted references to this as the "Final Rule" in publications about the HHS document released to the OMB, the HHS announcement actually states that what was released to the OMB will be a "notice and comment rulemaking, as required by the administrative procedures act." Thus, the final rule will not be published until after the notice and comment period has ended. (See the discussion at the end of this article as to possible effective dates.) According to HHS, the HITECH Rule will include changes to the regulations regarding:

- **Business associate liability;**
- **Limitations on the sale of protected health information;**
- **Marketing and fundraising communications; and**
- **Individual rights to access electronic medical records and restrict the disclosure of certain information.**

In addition, HHS noted that:

- Interim final rules implementing HITECH Act provisions regarding enforcement and breach notification have already been issued and are currently in effect;
- New civil money penalty amounts apply to HIPAA Privacy and Security Rule violations occurring after February 17, 2009; and
- Covered entities and business associates must comply now with breach notification obligations for breaches that are discovered on or after September 23, 2009 (OCR announced previously, however, that it would use its enforcement discretion not to impose fiscal sanctions with regard to breaches discovered before February 22, 2010).

Apparently, the HITECH Rule will not include the HITECH Act's requirement that HIPAA accountings include disclosures for treatment, payment and health care operations (TPO). In May 2011, HHS proposed a HITECH accounting rule that would shorten the accounting period to three years for all accountings, not just TPO accountings as required under the HITECH Act. HHS proposed that accountings for TPO disclosures be in the form of an "access report" derived from protected health information in electronic form in an electronic designated record set. The proposed rule also contained a list of the specific disclosures that would require an accounting, giving clarity lacking in the present privacy rule, which provides that accountings are required for disclosures not otherwise listed in the privacy rule's accounting provisions.

No one can be certain of the contents of the upcoming rule until its release, but a review of a proposed rule provides a pretty good picture of subjects likely to be included. In July 2010, HHS published a proposed rule implementing the modifications to the HIPAA privacy, security and enforcement rules required by the HITECH Act as well as modifications that were not required by HITECH but intended to "*improve the workability and effectiveness of all three sets of HIPAA Rules*" (the Proposed Rule). It is not clear whether the changes not specifically required by the HITECH Act will be included in the upcoming HITECH Rule. Mapping the subjects in the Proposed Rule to the subjects identified by HHS for inclusion in the HITECH Rule indicates that a number of changes that will have significant operational and legal implications are forthcoming. The most important elements of the Proposed Rule's treatment of HITECH Act changes to the HIPAA Rule that are identified by HHS to be included in the forthcoming HITECH Rule are as follows:

Business Associates. The HITECH Rule should deal with a variety of aspects of HIPAA compliance by business associates, although the HHS announcement only specifically mentions business associate *liability*. The Proposed Rule would expand the definition of *business associates*, including clarifying the application of the HIPAA business associate requirements to entities that provide only data transmission services, a subject that has generated some industry uncertainty. Under the Proposed Rule, subcontractors of business associates that receive protected health information of the covered entity from the business associate would be treated as business associates themselves, arguably expanding HIPAA's direct reach. The term *subcontractor* is broadly defined in the Proposed Rule.

Enforcement for "Agent" Activities. In the Proposed Rule, HHS explained its belief that its Civil Monetary Penalties (CMP) authority allow it to impose CMPs on a covered entity or on a business associate based on a violation of that entity's *agent*, as defined by *federal common law*, acting within the scope of the agency relationship. This change was not specifically required in the HITECH Act. In a separate section of the Proposed Rule, HHS states that this enforcement authority would exist even in the event there is no contract between the covered entity (or business associate) and the subcontractor. These proposed CMP changes, if carried forward into the HITECH Rule, would impose a new layer of concern and potential negotiation in the contracting process between covered entities and their business associates and between business associates and their subcontractors.

Limitations on the "sale" of protected health information. The HITECH Act prohibits the sale of protected health information (including sales for which payment is indirect) absent an authorization from each individual whose protected health information is disclosed. The authorization must state that remuneration is involved. The HITECH Act specifies a number of exceptions, including sales for public health activities or research so long as the price charged reflects the costs of preparation and transmittal of the research data, and for treatment. The Proposed Rule adds an exemption for disclosures required by law and, importantly, an exemption for a disclosure for any other permitted purpose, so long as the remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for its permitted purpose or a fee provided for by state or federal law. The Proposed Rule substitutes *financial remuneration* for the HITECH Act's term *direct or indirect payment*. *Financial remuneration* is defined as "direct or indirect payment from or on behalf of the third party whose product or service is being described," except payment for treatment of an individual which is exempt. In addition, only financial remuneration, as opposed to any other form of remuneration, matters for this purpose. Finally, HHS comments emphasize that the financial remuneration must be for the communication and must be on behalf of the entity whose product is being described in the communication.

Marketing and fundraising communications. The HIPPA Privacy Rule permits use by the covered entity, or the disclosure to an institutionally related foundation, of limited types of protected health information (demographic information and dates of health care) for fundraising purposes. This use or disclosure, however, must be disclosed in the covered entity's notice of privacy practices along with a description of an effective opt-out right.

The HITECH Act adds a requirement that the opt-out right must be provided in a manner that is "clear and conspicuous" and that exercise of that right by an individual should be treated as the revocation of an authorization. The Proposed Rule would require that the clear and conspicuous opportunity to opt out be provided in *each* fundraising communication and may not cause the recipient an "undue burden" or involve "more than nominal cost." The Proposed Rule does not define what types of communication constitute fundraising, but instead requests comments on this issue. Comments are also requested on the limitation of the types of protected health information that may be used or disclosed. The Proposed Rule proposed to prohibit a covered entity from conditioning treatment or payment on an individual's acceptance of marketing communications and requires the covered entity to honor the opt-out in practice, rather than merely using "reasonable efforts" to do so.

Under the Proposed Rule, an important exception permitting certain marketing activities would be eliminated. The Proposed Rule would eliminate the current health care operations exception for marketing health-related products or services included in a plan of benefits or products or services available from the covered entity where the covered entity *receives or has received* direct or indirect remuneration for the communication, unless certain requirements are met (as described below). If finalized, this provision would bring these health care operations communications within the definition of marketing and require that covered entities obtain an individual's authorization before using or disclosing protected health information for this purpose. In the Proposed Rule, HHS explained that it understood the HITECH Act provision to evidence congressional intent to end the exception for

communications to individuals that were motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's healthcare, despite the communication's [sic] being about a health-related product or service.

For purposes of this change to the marketing rules, the Proposed Rule used the same definition of *direct or indirect remuneration* as was discussed previously with respect to sales of protected health information. However, for treatment communications, even if direct or indirect remuneration is received, the activity is not marketing and an authorization is not required *if* the covered entity treatment provider has disclosed the receipt of financial information in its communication and has provided recipients with a "clear and conspicuous" opportunity to opt out of receiving any additional communications of this type. The opt-out method may not cause the individual to incur an undue burden or incur more than a nominal cost.

With regard to the exemption for remunerated refill reminders, the Proposed Rule would add a requirement that financial remuneration for refill reminders be "reasonably related to the covered entity's cost of communication." The Proposed Rule does not define, but instead requested comments on, several key terms, such as whether this exception applies only to a drug currently being prescribed or extends to alternative drugs.

Individual rights to access electronic medical records. The Proposed Rule repeated the HITECH Act provisions enhancing the right of individuals to access their own protected health information by providing individuals the right to receive copies of their protected health information in the form and format requested by the individual (if readily reproducible in that form and format) or in a mutually agreed form and format. However, while the HITECH Act provision limited this right to protected health information in an electronic health record, the Proposed Rule extended the right to protected health information in any electronic designated record set, regardless of whether the designated record set is maintained in an electronic health record. According to HHS comments, any other implementation would "result in a complex set or disparate requirements for protected health information in electronic health records versus other types of electronic records systems."

Individuals' rights to restrict the disclosure of their information. The Proposed Rule repeated the HITECH Act provisions requiring that a covered entity agree to an individual's request to restrict disclosure of protected health information for payment or health care operations (unless the disclosure is required by law) if the protected health information relates solely to an item or service that is paid for out of pocket. The Proposed Rule adds that the payment may be made by the individual (as stated in the HITECH Act) or on behalf of the individual by another person. HHS requests comments on a number of key aspects of this HITECH Act provision, including the difficulty of administering this requirement in certain circumstances; whether the covered entity is required to inform downstream providers of the request; and which disclosures are "required by law."

Although the effective date (February 17, 2010) for many of these HITECH Act provisions has passed, the HHS announcement states that the NPRM and ensuing final rule will provide specific information regarding the expected date of compliance and enforcement of these new requirements. The Proposed Rule stated that HHS intends to provide covered entities with six months after the effective date of most modifications to standards and implementation specifications to comply and that this would also apply to future modifications to HIPAA Rules. The Proposed Rule also provided an additional period of "deemed compliance" for covered entities and business associates and business associate and sub-business associates with business associate agreements or written arrangements that complied with the requirements of the privacy rule in effect prior to the effective date of the final rule. This is available only if the contract or other arrangement is not renewed or modified during the 60- to 240-day period after the effective date of the final rule. This deemed compliance extends until the *earlier* of the date the prior contract is renewed or modified after the 240-day period *up to* a maximum of 1 year *and* 240 days after the publication of the final rule. This may or may not be carried over into the pending HITECH Rule.

While it may be impossible to state with certainty how the HITECH Rule will change the existing HIPAA landscape, there are steps that covered entities and business associates can take now to prepare for the changes sure to come:

- Expect far more changes, especially changes with operational consequences, in the final rule than are indicated in the "top five" provisions of the HITECH Act mentioned in the HHS release. This will be the case even if the final rule is limited to the HITECH Act requirements and does not include the additional "improved workability and effectiveness" provisions mentioned in the Proposed Rule.
- HIPAA policies and procedures should be assembled, if they are not already, in a single place and a team should be designated to handle amendments. Existing policies and procedures should be reviewed to determine if their provisions need to be changed prior to a final rule. For example, the breach notification requirements became effective September 23, 2009, subject to a waiver of penalties for breaches until February 20, 2010. Policies and procedures should be in place relating to the identification, investigation, mitigation and disclosure of breaches. Certain of the other HITECH Act changes are self-executing, i.e., they do not require implementing regulations to be effective or were effective one year after enactment of the HITECH Act, i.e., February 17, 2010, and should already be addressed in organization policies and procedures.
- Many likely changes to the HIPAA Rules will require maximum lead time to be implemented in a reasoned and cost-effective manner. For example:

  - The larger the covered entity, the greater the required institutional effort that must go into amending the notice of privacy practices. There is often a fight for real estate on the form, to keep it one sheet. In most large covered entities, the notice of privacy practices is amended only on an annual basis. Plan ahead for possible amendments required by the HITECH Rule.
  - Changes that affect electronic systems require lead time (usually more than the six month implementation delay mentioned in the Proposed Rule) to identify and implement, especially if

negotiation is required to deal with a third-party vendor or licensor. Covered entities and business associates with vendor or licensor contracts in place or in negotiation should review those contracts to determine if updates or upgrades are required to ensure that the subject system be capable of use in compliance with HIPAA, including amendments to HIPAA, in a timely manner. Similarly, entities should review the charges, if any, associated with such updates or upgrades, as "rush" charges may increase costs substantially.

- Business associate arrangements should be identified and reviewed. Business associates without a written business associate agreement should be identified and agreements put in place. For business associates with written agreements, the agreements should be placed in a central repository to be reviewed, ideally by a designated team familiar with the current and anticipated future requirements.

  - If the Proposed Rule is followed, there will be a significant advantage if a written agreement is in place prior to the publication of a final rule.
  - The days of a "standard" business associate agreement are likely over, as the requirements of a business associate arrangement may lead to business associates requesting specific provisions, such a lead time to report breaches. Similarly, increased compliance burdens on business associate relationships will likely lead to negotiations and/or disputes over whether or not a particular service provider should even be considered a business associate. This is especially true for companies that do not access protected health information, even if they store or transmit it.
  - As the so-called "cloud" environment is used more frequently to store protected health information, familiar breach risks occur in a different environment, requiring a different approach to a business associates responsibilities. Novel issues may arise as to accounting documentation, individual access, and return or destruction of protected health information in the cloud provider/business associate's hands. While not only a HIPAA issue, business associate agreements for these arrangements should be reviewed to ensure they specifically provide for the return of protected health information in a secure and usable form upon termination.
  - Vicarious liability for breaches of a business associate or sub-business associate considered an "agent" under federal common law will require careful negotiation and likely attention to insurance and indemnification requirements. Covered entities and first-tier business associates may have a different view of what is reasonable than the business associate or sub-business associate. Business associate agreements should be reviewed for sufficiency and clarity with regard to these provisions.
  - HIPAA's requirements for adequate physical, administrative and electronic security of electronic protected health information may work well for companies that are committed to and experienced in dealings with health care providers. However, less experienced and smaller entities, especially those not committed to the health care industry (such as copying services, third-party storage facilities or delivery services) may be unable to comply financially or simply unwilling to comply because of the effort involved. In addition to reviewing the associated business associate agreements, covered entities should consider reviewing the security (or lack thereof) provided to protected health information by their business associates.
- Covered entities and business associates should be prepared for wild cards. For example, if a final breach notification rule is issued with the HITECH Rule, there is a possibility that the interim threshold analysis will be eliminated or curtailed. When the Interim Final Rule was issued, Congress expressed strong objection to allowing a covered entity to commit a breach of unsecured protected health information but be required to provide notification if the covered entity determined that the breach did not pose a significant risk of financial, reputational or other harm to the individual or individuals involved. In 2010, HHS announced that it was withdrawing the breach notification final rule submitted in May 2010 from OMB review to allow for further consideration, given the Department's experience

to date in administering the regulations. At that time, many privacy advocacy organizations issued press releases attributing the withdrawal to lobbying against the interim harm threshold analysis.

Entities who act now to "get their (HIPAA) house in order" can be well-positioned to act quickly and efficiently to come into compliance with HITECH Regulations, no matter what changes they bring. The Ober Health Care Technology and Privacy team will provide details and analysis of the HITECH Rule in a series of articles and planned webinars.