Health Law Alert: HHS Releases Proposed Regulations Dramatically Expanding HIPAA Accounting of Disclosures Requirements

June 16, 2011

On May 31, 2011, the Department of Health and Human Services (HHS) released proposed regulations implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act's requirements for covered entities and business associates to account for disclosures of protected health information (PHI) for treatment, payment, and health care operations if the disclosures are through an electronic health record (EHR). The proposed regulations represent a significant change to the current requirements of the HIPAA Privacy Rule, and go much further than the HITECH Act appeared to require. HHS will accept comments on the proposed regulations through August 1, 2011.

Current Accounting Requirements and HITECH Changes

Since 2003, the HIPAA Privacy Rule has required covered entities to maintain records on disclosures of PHI, and to furnish that record of disclosures to individuals who request them. The Privacy Rule exempts certain categories from this accounting obligation, however, including disclosures for treatment, payment, and health care operations purposes. Privacy advocates have long argued that these exemptions constitute the majority of disclosures and that failing to include them undermines the benefit the accounting requirements were intended to achieve. HITECH addressed this by expanding the accounting requirements to remove the exemptions for treatment, payment, and health care operations when the disclosure is from an EHR.

Access Reports and Accounting of Disclosures

The proposed regulations would grant individuals access to this information in two ways: the right to an access report and the right to an accounting of disclosures. HHS believes that these two rights will provide individuals with greater transparency regarding the use and disclosure of their PHI, without imposing an undue burden. HHS' conclusion appears in large part premised on its view that covered entities already have a clear obligation to log access to ePHI under the HIPAA Security Rule. HHS believes that systems with designated record set information should already be configured to record when users access information, and that covered entities should be logging access to ePHI and regularly reviewing reports of such access.

An ***access report*** would provide an electronic log of anyone who has accessed ePHI in a designated record set, meaning electronic systems that maintain medical records, billing records, or other information that is used by covered entities to make payment or treatment decisions. This goes significantly beyond the requirements of HITECH because the access report would include all electronic designated record sets, rather than only EHRs, and cover both uses and disclosures. As proposed, the new access requirement would cover access to ePHI in a designated record set regardless of reason. This provision also includes access both by employees of covered entities and its business associates, including those external to the organization. Access reports would require the date, time, and name of the person (or entity) that accessed the information, and a description of the PHI that was accessed (such as "medications") along with the user's action (such as the information having been modified or deleted), to the extent that such information is available. Importantly, access reports would not need to include the "purpose" of the access. Thus, while covered entities would need to include ePHI access involving treatment, payment, and health care operations in the category of accesses for which tracking occurs, they would not need to distinguish among the purposes in providing the required reports to individuals.

The ***right to an accounting*** would provide additional information about the purpose of the disclosure of designated record set information (whether hard copy or electronic) to persons outside the covered entity and its business associates. However, this "full accounting" right would only be available for certain purposes. HHS proposes to limit accounting to the types of disclosures that are most likely to be of importance to individuals, such as disclosures to law enforcement, courts, or public health investigators, as well as "impermissible disclosures" that, based on a covered entity's risk analysis, did not rise to the level of being a "breach." In the proposed regulations, the accounting requirements are designated by affirmatively listing those uses and disclosures for which an accounting is required. This represents a reversal from the manner in which the Privacy Rule has historically regulated this issue—listing the situations in which an accounting is not required and requiring an accounting in all other cases.

Responding to Requests

In response to a request for an access report, covered entities would have 30 days to provide the accounting of disclosure or access report to the individual. A one-time extension of 30 days would be allowed when necessary as long as the individual was notified. The covered entity must provide the access report in the form (electronic or hard copy) requested by the individual.

One of the most significant challenges for covered entities are that access reports must include electronic designated record sets that are maintained by business associates. HHS believes that business associates' obligations under HITECH to maintain reasonable and appropriate safeguards for ePHI should include the ability to determine who has accessed ePHI. The proposed regulations state that if an individual requests this information, a covered entity must contact the business associates that create, receive, maintain, or

transmit electronic designated record set information and obtain from them access reports with respect to the individual's information. All of that information must then be compiled in a report and given to the individual within the requisite time period.

Open Questions and HHS' Recommendations

HHS recommends covered entities assess their electronic auditing of information system activity to ensure that they are comprehensively logging user access to ePHI in designated record sets. While much of HHS' logic in crafting the proposed regulations is based on its view that covered entities are already maintaining complete access logs, it is something of an open question as to whether that in fact is the case. HHS also suggests that covered entities develop disclosure forms for individuals to use when requesting access reports to narrow the scope of the access report as much as possible based on the individual's interests. This will reduce the administrative burden on the covered entity of producing more than what the individual requests.

Health plans, meanwhile, may be struggling with the notion that the new access requirements could apply to them as well, since it is likely they maintain electronic designated record sets. The HITECH Act sought to impose the broadened accounting requirements only on EHRs, the statutory definition of which would generally not apply to the information set possessed by plans.

If you have questions about the proposed accounting of disclosure regulations, please contact Jesse Berg at jesse.berg@lathropgpm.com or 612.632.3374.

HIPAA and HITECH issues, including the proposed accounting of disclosure requirements, will be featured at Gray Plant Mooty's 15th Annual Health Law Conference to be held July 14, 2011. Visit the Health Law Conference Web site to register.