OBER | KALER
Attorneys at Law

June 1, 2011

Ober|Kaler Healthcare Information Privacy, Security and Technology Bulletin

James B. Wieland | jbwieland@ober.com

Joshua J. Freemire | jjfreemire@ober.com

A Redo of the HIPAA Accounting Requirements? HHS Posts NPRM for HITECH Act Treatment, Payment and Healthcare Operations Accounting

On May 27, 2011, the Secretary of Health and Human Services posted a Notice of Proposed Rulemaking ("NPRM") nominally implementing the HITECH Act's requirement that covered entities and business associates provide individuals with an accounting of disclosures of their protected health information ("PHI") for treatment, payment and health care operations through an electronic health record for the prior three (3) year period ("TPO Accounting"). In point of fact, the NPRM proposes a number of fundamental revisions to the HIPAA accounting requirements.

The NPRM divides the HIPAA accounting rights of individuals into two separate rights: the right to receive an "access report," providing details regarding individuals and entities who have accessed an individual's electronic health records (even where they are permitted to do so under HIPAA) and the right to receive a scaled back version of the current HIPAA accounting of disclosures. As described in the NPRM:

> "These two rights, to an accounting of disclosures and to an access report, would be distinct but complementary. The right to an access report would provide information on

> who has accessed electronic protected health information in a designated record set (including access for purposes of treatment, payment, and health care operations), while the right to an accounting would provide additional information about the disclosure of designated record set information (whether hard-copy or electronic) to persons outside the covered entity and its business associates for certain purposes (e.g., law enforcement, judicial hearings, public health investigations). The intent of the access report is to allow individuals to learn if specific persons have accessed their electronic designated record set information (it will not provide information about the purposes of the person's access). In contrast, the intent of the accounting of disclosures is to provide more detailed information (a "full accounting") for certain disclosures that are most likely to impact the individual."

The proposed "access report" is intended to implement the HITECH Act's TPO Accounting requirement. The access report must include:

- The date and time of access;
- The name of the entity accessing the information (or, if available, the name of the natural person);
- A description of the information was accessed, if available; and
- A description of actions taken by the accessing user, if available. With regard to the actions taken by the user, the NPRM requires that entities provide an explanation in terms commonly automatically recordable in most electronic records systems, i.e. "create," "modify," "access," or "delete."

The NPRM provides that the access report must be provided "in a format that is understandable to the individual" and must be in a "machine readable" or other electronic form and format requested by the individual, if available, or otherwise as mutually agreed. "Machine readable data" is defined in the NPRM as "digital information stored in a standard format enabling the information to be processed and analyzed by computer."

Citing the HIPAA Security Rule, the NPRM states that the information required for the access report should already be available for electronically maintained PHI. Most electronic record systems have the capability of maintaining an "audit log," although the NPRM specifically declines to use that term, and these audit logs are typically monitored to ensure the security of the electronic information system, as required by the Security Rule.

Under the NPRM, the compliance date for the access report requirement is based on the date that the covered entity or business associate acquired the particular “electronic designated record set system”. For electronic designated record systems acquired after January 1, 2009, the compliance date is January 1, 2013. For electronic designated record set systems acquired on or before January 1, 2009, the access report compliance date is January 1, 2014. The NPRM recognizes that these split compliance dates may create difficulties for entities with multiple electronic designated record sets acquired at different times. For these entities, the NPRM encourages, but does not require, the voluntary provision of access reports from all systems by the earliest compliance date.

As proposed, the accounting of disclosures would be broader than the access report, and would consist of the following information:

- The date, or if not known, the approximate date of the disclosure or period of time during which the disclosure occurred (for multiple disclosures to the same recipient for a single purpose, the dates of the first disclosure and the last disclosure in the accounting period);
- The identity of the recipient of the individual’s PHI and, if known, his or her address (except when such information constitutes protected health information about another individual);
- A brief description of the type of PHI disclosed; and
- A brief description of the purpose of the disclosure that “reasonably informs the individual of the basis for the disclosure.”

The accounting of disclosures would continue to apply to both paper and electronic PHI, subject to the requirement that it be in a designated record set. The modified accounting requirements would apply 240 days after the publication of the rule in final form, i.e. 180 days after the effective date of the final rule, which will be 60 days after its publication as a final rule.

The NPRM proposes modifications to the existing requirements governing the reporting of disclosures of PHI to individuals in several ways:

- The current requirement to account for six (6) years of disclosures would be reduced to three (3) years for both the access report and the accounting (although a copy of any accounting or access report provided to an individual would be required to be retained for six (6) years, along with documentation of the designation of the individual responsible for the accounting or the access report);

- The time for response to a request for an accounting or an access report would be thirty (30) days, subject to one thirty (30) day extension and in the case of an accounting, subject to law enforcement delays, as under the current regulations; and;
- A "reasonable, cost-based fee" may be imposed for requests for more than one accounting or more than one access report by an individual in any twelve (12) month period.

Both the access report and the accounting would be limited to information contained in a designated record set. A designated record set is defined as "a group of records maintained by or for a covered entity" that constitutes either "the medical records and billing records about individuals," "the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan," or a group of records "used, in whole or in part, by or for the covered entity to make decisions about individuals." For purposes of this definition, the term record means "any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity." The NPRM notes that this extends to all information in an electronic designated record set, whether or not the electronic designated record set constitutes an electronic health record, as defined in the HITECH Act TPO Accounting provisions.

The NPRM provides, for the first time, a definitive list of the types of disclosures subject to an accounting, in place of the Privacy Rule's current approach of requiring an accounting for all disclosures not specifically identified as exempt. When preparing an accounting, entities must include disclosures that are:

- Not permitted by the Privacy Rule, unless the individual has received a notification of the impermissible disclosure under the HITECH Act requirements for reporting a breach of unsecured PHI;
- Made for public health activities, except disclosures to report child abuse or neglect;
- Made for judicial and administrative proceedings;
- Made for law enforcement purposes;
- Made to avert a serious threat to health or safety;
- Made for military and veterans activities, the Department of State's medical suitability determinations, and government programs providing public benefits; and for workers' compensation.

The NPRM goes on to explain, however, that no accounting would be required for the above disclosures if the disclosure was required by law (as opposed to being merely permitted by law), other than disclosures for judicial and administrative proceedings or for law enforcement purposes.

Finally, the NPRM requires that covered entities amend their notice of privacy practices to reflect the individual's right to receive an access report as described in the NPRM.

Comments on the NPRM will be due sixty (60) days after its publication in the Federal Register. The NPRM generally reflects an attempt to balance the interests of individuals in obtaining information about uses and disclosures of their PHI against the administrative burden on covered entities and business associates of recording and providing this information. The capability of current electronic records systems used in the health care industry should support the proposed access report requirements, although electronic storage space for such information may be a factor. The issue of identification of an "electronic designated record set" will be challenging, however, given the inclusiveness of the definition, particularly given the use of the catch-all phrase "used, in whole or in part, by or for the covered entity to make decisions about individuals."

Questions?

Contact Our Healthcare Information Privacy and Technology Group:

Jim Wieland | jbwieland@ober.com
Paul Kim | pwkim@ober.com
Sarah Swank | seswank@ober.com
Josh Freemire | jjfreemire@ober.com

About Ober|Kaler

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 130 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.
