Thomas D. Bixby
Law Office LLC
*Legal Advice for Health Plans*

***HEALTH LAW ALERT***
***May 31, 2011***

# HHS Proposes New "Access Accounting" Privacy Right

## Employees' Access to PHI Would be Subject to Reporting Obligation

Today, the Department of Health and Human Services Office for Civil Rights ("OCR") formally published a proposed amendment to the HIPAA Privacy Rule that would require a health plan (and any other covered entity) to provide individuals a report of each instance in which an employee (or any other person) accessed electronic protected health information maintained in a designated record set (an "electronic designated record set"). Although the proposal would reduce the burden of the Privacy Rule's disclosure accounting provisions, the new "access reports" would impose a significant new burden, requiring health plans to report, among other details, the date and time of each instance in which any person accesses an electronic designated record set as well as the name (when available) of the "natural person" who accesses the electronic information.

While OCR proposed the amendment as part of its implementation of HITECH Act provisions related to the HIPAA Privacy Rule, the proposal goes well beyond the disclosure accounting requirements of that legislation. The HITECH Act affects only protected health information contained in "Electronic Health Records" and only when disclosed to third parties. OCR explains that this broader scope is justified because the "access report" requirement "greatly improves transparency and better facilitates compliance and enforcement, while placing a reasonable burden on covered entities and business associates." Indeed, OCR asserts that the requirement to include in this access report "all access, rather than only access that represents a disclosure [to a third party], may actually be less burdensome on covered entities and business associates" because many covered entities have claimed their systems cannot distinguish between "uses" of protected health information and "disclosures."

Under the proposed amendment, the effective date for providing "access reports" would depend on when the covered entity acquired its systems for maintaining electronic protected health information in a designated record set. The compliance date would be January 1, 2014 with respect to electronic designated record sets maintained in systems acquired on or before January 1, 2009. Designated record sets maintained in systems acquired after January 1, 2009—newer systems—would be subject to the requirements a year earlier—January 1, 2013. The modifications to the old disclosure accounting requirements, which reduce the amount of information a covered entity must provide, would go into effect 240 days after the final rule is published.

The proposed amendment is published at 76 *Federal Register* 31426 (May 31, 2011). Comments must be submitted no later than August 1, 2011.

**Access Reports**

OCR proposes to implement this accounting-for-access requirement as a new individual right under the Privacy Rule that would supplement the current "disclosure accounting" right. Specifically, covered entities would be required to provide individuals upon request "access reports," giving details of each instance in which an electronic designated record set was accessed by any person for (almost*) any reason in the previous three years. An access report would identify "who has accessed protected health information about the individual in an electronic designated record set maintained by [the] covered entity or business associate" and would have to include:

- Date of access;
- Time of access;
- Name of natural person, if available, otherwise name of entity accessing the electronic designated record set;
- A description of what information was accessed, if available, and
- A description of the user's action, if available, *e.g.*, "create," "modify," "access," or "delete" records in the electronic designated record set.

Covered entities would have thirty days to provide the access report in a format that is understandable to the individual, but could extend the deadline for an additional thirty

### *Designated Record Sets*

The proposed "access report" requirement (as well as the original "disclosure accounting" requirement) would apply only to information in a "designated record set. A health plan's designated record set is a group of records maintained by or for a health plan that includes the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan and any other records used, in whole or in part, by or for the health plan to make decisions about individuals.

OCR believes that information in a designated record set "generally represents the protected health information that is of most interest to the individual" and that access reports do not (and disclosure accounting reports no longer) need to address protected health information, unless it is maintained in a designated record set.

The "access report" requirement would apply only to access to protected health information maintained electronically in a designated record set.

* The proposed amendment would permit a covered entity to exclude from an access report instances in which a "Patient Safety Organization" accesses protected health information for certain purposes under the Patient Safety and Quality Improvement Act of 2005. No other exceptions would apply.

days, if necessary. The first report in any 12-month period must be provided at no cost to the individual; subsequent reports may be subject to "a reasonable, cost-based fee."

**Disclosure Accounting**

The proposed amendment would ease requirements for the disclosure accounting provisions that have been in place since the original Privacy Rule went into effect in 2003. First, the proposed amendment would limit the period for which an individual is entitled to receive an accounting of disclosures to three years, down from the current six years. Second, the disclosure accounting requirement would apply only to protected health information maintained in a "designated record set" (see box on previous page). Finally, health plans would no longer need to include in an accounting several types of disclosures for which accounting is currently required. For example, covered entities would no longer be required to account for disclosures:

- That have already been reported to the affected individual under the HIPAA Breach Notification requirements;
- To health oversight agencies;
- Related to abuse, neglect, or domestic violence;
- For research purposes; and
- For protective services for the President.

The proposed amendment would, therefore, make compliance with the disclosure accounting requirements (as opposed to the "access reporting" requirements) less burdensome.

**Reporting Access by Named Employees**

The proposed amendment requires an "access report" to contain the "[n]ame of [the] natural person" accessing information only if the name is "available." But, based on the OCR's aggressive interpretation of a health plan's obligations under the Security Rule, it appears that the proposed amendment would require an enrollee's "access report" to include an employee's name every time health plan personnel access information about the enrollee in the health plan's systems.

The OCR asserts that health plans (and other covered entities) have an "existing obligation" under the HIPAA Security Rule to collect all data necessary for the "access reports" and "should already be logging access to electronic protected health information" each time an employee (or any other person) accesses information. This assertion is based (in part) on the Security Rule requirement that covered entities must implement "audit controls." The OCR apparently does not consider the possibility that a health plan could

meet this "audit control" requirement by logging a sample of instances in which an employee accesses information (rather than logging every instance).

The Security Rule requires health plans to assign each "user"—including each separate employee—a unique identification name or number to identify and track the user's identity. Taken together with OCR's assertion concerning audit controls, this means a health plan should already be collecting data every time any person accesses protected health information in a designated record set and should be able to identify the specific employee who accesses information. The "access report" would therefore have to list an employee's name each time health plan personnel access electronic protected health information in a designated record set.

In contrast, the "unique user" identification requirement permits health plans to identify a business associate with a single identifier, notwithstanding that the business associate might have several different employees accessing protected health information in the health plan's system. Accordingly, when a business associate's employee accesses the health plan's electronic designated record set, the health plan may not know the name of the "natural person" accessing the information. Thus, the name of the "natural person" accessing protected health information may not always be "available" to list in an "access report" even though the name of a health plan employee accessing an electronic designated record set would (apparently) always need to be included.

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or
TBixby@tbixbylaw.com