

## Accounting of Disclosures Under HIPAA: The Controversy Continues

### Proposed HHS rule would create a right to an “access report” and reduce accounting of disclosures requirements

By Adam H. Greene and Rebecca L. Williams

May 31, 2011

On May 31, 2011, the Department of Health and Human Service (HHS) published its proposed revisions to the accounting of disclosures requirements, one of the more controversial mandates under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

In short, the proposal would provide patients and enrollees with the ability to learn who has seen their records, through an “access report” (without providing information about the reason), and would provide more detailed information for disclosures of information that are most likely to be of interest to the individual (such as disclosures to law enforcement).

HIPAA-covered entities should remember that this is a proposed rule and, therefore, should not rush to make costly changes to systems and processes based on this proposal. Nonetheless, they should understand the proposal and its possible implications, and proactively address some basic issues.

This is a good time for covered entities to:

- Comment on the proposed rule (comments are due Aug. 1, 2011), both with respect to provisions that may be overly burdensome and those that may prove beneficial.
- Assess their electronic auditing of information system activity to ensure that they are comprehensively logging user access to electronic protected health information in designated record sets.
- Revisit and, if necessary, update their documentation relating to designated record sets (generally medical and billing records).
- Verify (and reassess, if necessary) which business associates have access to designated record sets.

#### What HITECH said

The current HIPAA Privacy Rule requires an accounting of disclosures of all protected health information, but excludes certain types of disclosures. Most notably, disclosures for treatment, payment, and health care operations did not need to be included in an accounting, an exception that many privacy advocates assert swallows the rule.

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires HHS to remove the exception for treatment, payment, and health care operations to the extent that disclosures are through an electronic health record. Notably, HITECH provides that HHS may balance the interests of individuals and the burden on covered entities when determining what information needs to be collected about these types of disclosures.

### **The new right to an access report**

The most significant proposed change, which is designed to address the requirements of HITECH, is to provide individuals with the right to receive an access report. The access report would include the date and time of access and the name of the user (or name of the entity if the name of a specific user is unavailable). It would be limited to electronic designated record sets, meaning electronic systems that maintain medical records, billing records, or other information that is used by covered entities to make payment or treatment decisions.

The access report also would require the inclusion of a description of what type of protected health information was accessed (such as “medications”) and the activity that was performed (such as the information having been modified or deleted), but only if this information is available. Covered entities would not need to change their information systems to collect these latter two types of information.

The preamble to the proposed rule states that the access report implements HITECH requirements because it provides information about each disclosure for treatment, payment, and health care operations that is through an electronic health record. Specifically, under the proposed rule, covered entities would provide the date, time, and name of the user each time someone accesses an electronic health record for any reason, which would include the purposes of treatment, payment, and health care operations (albeit, the access report would not state the purpose of any particular access).

The proposal goes significantly beyond the requirements of HITECH because the access report includes all electronic designated record sets (rather than only electronic health records) and covers both uses and disclosures. This means the proposed rule does not differentiate between employee access and access by users who are outside the organization.

The proposed inclusion of all protected health information maintained in electronic “designated record sets” rather than “electronic health records” seems to impose access reports on a more expansive universe of covered entities than originally contemplated under HITECH. For example, a large number of health plans, which likely would not be operating an electronic health record as defined in HITECH, would be maintaining protected health information electronically in designated record sets. Also, covered health care providers that have not implemented electronic health records, but may, for example, be billing electronically, would get pulled into the expanded access report

requirements.

The proposed rule stresses that covered entities should work with individuals to provide an access report that is limited to the individual's interest. For example, if the individual wants to know if a neighbor who is employed at the hospital has viewed her health information, then there is no need to run a lengthy access report listing everyone who has accessed the individual's information.

The proposed rule presumes that covered entities already are maintaining audit logs that identify all user access to electronic designated record set information in accordance with the HIPAA Security Rule. A significant question, and a potential area of comment, is whether this is in fact the case (although covered entities may want to be cautious in developing comments that indicate that they do not maintain comprehensive audit logs, since this may be viewed as noncompliance with the Security Rule).

One of the most significant challenges may be that access reports must include electronic designated record sets that are maintained by business associates. Accordingly, upon receiving a request for an access log, a covered entity would need to run an access report for each of its systems, have its business associates that electronically maintain designated record sets do the same, and then provide these reports (as an aggregated report), to the patient or enrollee.

The proposed rule takes away an option under HITECH in which a covered entity could provide an individual with its own report and a list of its business associates. The covered entity must provide the report within 30 days, although a single 30-day extension would be available when necessary. Adding in the time to allow business associates to process the access report will make a 30-day (or even a 60-day) response more challenging.

The proposed rule states that a covered entity should provide the option to limit the access report by organization. The covered entity need not collect information from business associates unless the individual is seeking this information.

### **Changes to the old accounting of disclosures provision**

HHS also proposes a number of changes to the existing accounting of disclosures provision, which should mostly come as welcome news to covered entities. The proposal would remove a number of categories of disclosures, such as those for research or as required by law, from the accounting requirements. HHS proposes to limit the "full accounting" to the types of disclosures that are most likely to be of importance to individuals, such as impermissible disclosures (that did not rise to the level of a breach) or disclosures to law enforcement or courts.

The proposal also would limit the period of accounting from six years to three years, limit the scope of information to that which is in a designated record set, and provide more flexibility regarding how dates are recorded (for example, numerous disclosures

could be listed as “December 2010 through August 2011”).

A change to the old accounting of disclosures provision that covered entities will not welcome is that the timeframe for responding to an accounting request would be reduced from 60 days to 30 days (with a 30-day extension still available).

### **Proposed compliance dates**

HHS proposes that compliance with the changes to the “full accounting” would be within 240 days of publication. This should not prove challenging, since these changes are mostly reductions in covered entities’ responsibilities.

The compliance dates for the requirement to provide access reports would be Jan. 1, 2013 (for electronic designated record set systems that were acquired after Jan. 1, 2009), and Jan. 1, 2014 (for electronic designated record set systems that were acquired on or before Jan. 1, 2009). The staggered dates are based on the HITECH provision and provide extra time for older legacy systems to come into compliance.

### **Winners and losers**

Arguably, all covered entities come out as both winners and losers under the proposal. Health care providers who already are maintaining comprehensive audit logs may come out as winners because their “full accounting” requirements are reduced and the new “access report” requirement may prove to be a limited burden (it is likely that covered entities will continue to receive few requests and, therefore, will have few occasions where they actually incur the burden of generating access reports).

Covered entities will not be required to record the purpose of each access of the electronic health record, which many feared would be the result of this rulemaking; however, the purpose still must be tracked for the types of disclosures that are subject to the “full accounting.” Covered entities that do not have audit capabilities or do not currently maintain comprehensive audit logs would have to begin doing so, at significant expense.

Health plan providers may be the hardest hit under the proposal because they generally do not maintain electronic health records and so they may have thought that they would be unaffected by the rulemaking (although they benefit from the reductions to the “full accounting”).

This advisory is a publication of Davis Wright Tremaine LLP. Our purpose in publishing this advisory is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.