

June 08, 2011

## **Proposed Rule Modifies HIPAA's Accounting of Disclosures Requirements**

On May 31, 2011, the U.S. Department of Health and Human Services (HHS) issued a [Notice of Proposed Rulemaking](#) (the "Proposed Rule") to modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule's standard for accounting of disclosures of protected health information (PHI).

The purpose of the Proposed Rule is, in part, to implement the statutory requirement under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act") to require Covered Entities and Business Associates to account for disclosures of PHI to carry out treatment, payment, and health care operations if such disclosures are through an electronic health record (EHR). HHS also proposes to expand the accounting provision to provide individuals with the right to receive an access report indicating who has accessed their electronic PHI in a Designated Record Set (an "Access Report").

### **Current Requirements**

The current Privacy Rule requires Covered Entities to make available to an individual upon request, an accounting of certain disclosures of the individual's PHI made during the six years prior to the request (an "Accounting of Disclosures"). A disclosure is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." An accounting must include all disclosures of PHI except for disclosures specifically exempted under the Privacy Rule; disclosures of PHI to carry out treatment, payment, and health care operations are specifically exempted from the accounting requirement.

The current Privacy Rule applies to disclosures of paper and electronic PHI regardless of whether such information is in a Designated Record Set. Although the Covered Entity is responsible for providing an individual with the accounting of disclosures, the accounting must include disclosures to and by the entity's Business Associates. Business Associates are required to make available to the Covered Entity the information required for the accounting.

### **Changes Required by HITECH Act**

The HITECH Act provides that the exemption of disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures through an EHR (an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff). With respect to disclosures by Business Associates who make disclosures through an EHR to carry out treatment, payment, and health care operations on behalf of a Covered Entity, the Covered Entity must provide either an accounting of the Business Associates' disclosures, or a list and contact information of all Business Associates so that the individual may contact each Business Associate for an accounting of the Business Associate's disclosures.

### **The Proposed Rule**

The Proposed Rule contains two separate and distinct rights for individuals: (1) the right to an Accounting of Disclosures, and (2) the right to an Access Report.

**Accounting of Disclosures.** The Proposed Rule includes a number of changes to an individual's right to receive an Accounting of Disclosures. Currently, an individual has a right to an Accounting of Disclosures of PHI about the individual, regardless of where such information is located. The Proposed Rule limits the accounting provision to PHI about the individual contained in a Designated Record Set; a Designated Record Set includes the medical and health care payment records maintained by or for a Covered Entity, and other records used by or for the Covered Entity to make decisions about individuals. The Proposed Rule also decreases the period of time that a Covered Entity and Business Associate must account for disclosures from six (6) years to three (3) years.

The Proposed Rule incorporates a direct reference to Business Associates to make clear that the Covered Entity must include accounting information for all disclosures by the Covered Entity's Business Associates that create, receive, maintain or transmit Designated Record Set information.

Further, the Proposed Rule explicitly lists the types of disclosures that are subject to an accounting rather than listing the types of disclosures that are exempted as in the current Privacy Rule. Covered Entities will continue to be required to account for disclosures that are impermissible under the Privacy Rule unless the Covered Entity (directly or through a Business Associate) has provided breach notice. Covered Entities must also account for disclosures for public health activities, for judicial and administrative proceedings, for law enforcement activities, to avert a serious threat to health or safety, for military and veteran activities, for the Department of State's medical suitability determination, to government programs providing public benefits, and for workers' compensation.

The Proposed Rule also makes several modifications to the content of the accounting. Covered Entities or Business Associates would need only to provide an approximate date or period of time for each disclosure, if the actual date is not known (currently, the actual date of disclosure is required). For multiple disclosures of an individual's information to the same person or entity, the approximate period of time is sufficient rather than the exact start and end date, as presently required. The date of disclosure may be descriptive (e.g. "within 15 days of discharge"). Instead of requiring a brief description of the PHI disclosed, the Proposed Rule requires a brief description of the type of PHI disclosed.

Individuals have the option of limiting the accounting to a particular time period, type of disclosure, or recipient.

In addition, the Proposed Rule modifies the provision of the accounting by decreasing the Covered Entity's permissible response time from 60 days to 30 days, by requiring that Covered Entities provide individuals with the accounting in the form and format requested by the individual if readily producible (e.g. an electronic copy of the accounting), and by clarifying that the Covered Entity may require the individual to submit the accounting request in writing.

The HITECH Act requirements considerably altered the HIPAA accounting rule by substantially increasing burdens for Business Associates and Covered Entities, including the requirement to track a much broader set of disclosures. While the Proposed Rule alleviates some of the burdens of accounting requirements (e.g., by limiting the accounting to the Designated Record Set and by reducing the number of years required to be included), the main expansion from the HITECH Act -- requiring accounting of disclosures made for treatment, payment, and operations -- remains and is implemented by the Proposed Rule.

**Access Report.** The Proposed Rule provides a right for individuals to receive an Access Report that indicates who has accessed their electronic Designated Record Set information; this requirement does not extend to access of paper records. The right to an Access Report would provide information on who has accessed electronic PHI in a Designated Record Set (including access for purposes of treatment, payment, and health care operations) over a three (3) year period. It is important to note that an electronic Designated Record Set is different and more expansive than an Electronic Health Record.

Covered Entities typically have electronic Designated Record Set information in multiple systems, each maintaining separate Access Logs (raw data that an electronic system containing PHI collects each time a user accesses information). In the Proposed Rule, HHS indicates that its expectation is that data from each Access

Log will be gathered and aggregated to generate a single Access Report which also shall include data from Business Associates' systems.

HHS defines an Access Report as a document that a system administrator or other appropriate person generates from the Access Log in a format that is understandable to the individual. The Access Report does not distinguish between “uses” and “disclosures” and thus, would apply when any person accesses an electronic Designated Record Set whether that person is a member of the Covered Entity's workforce or a person outside the Entity. Thus, every time a nurse accesses information in an electronic Designated Record Set for treatment purposes, this must be tracked and included in the Access Report.

The information contained in an Access Report is less detailed than the information provided under an Accounting of Disclosures. For example, the Access Report does not include the purpose(s) of the person's access, but does provide the date and time of access, and the name of the person accessing the information, if available. HHS also proposes to require a description of the PHI that was accessed and the action of the person who accessed the PHI, but only to the extent that such information is available. HHS indicates that because the Access Report is limited to electronic access, the report includes only information that a Covered Entity is already required to collect under the HIPAA Security Rule.

The timing requirement for provision of an Access Report is the same as for provision of an Accounting of Disclosures – Covered Entities have 30 days to provide an Access Report. A Covered Entity can require that an individual request an Access Report in writing but the Covered Entity must provide the Access Report in the form and format requested by the individual if it readily producible in such form and format.

**Other Changes.** The Proposed Rule also revises the requirements for Notices of Privacy Practices in order to inform individuals of their right to receive an Access Report in addition to their right to receive an Accounting of Disclosures. In addition, HHS provides that a Covered Entity shall exclude from an Accounting or an Access Report any information that meets the definition of Patient Safety Work Product under the Patient Safety and Quality Improvement Rule.