Health Law manatt

May 31, 2011

HHS Proposes Changes to HIPAA Accounting of Disclosures Provision

Authors: Robert D. Belfort | Susan R. Ingargiola

On May 27, 2011, the U.S. Department of Health and Human Services ("HHS") issued a notice of proposed rulemaking (the "NPRM") to modify the accounting of disclosures provision of the Health Information Portability and Accountability Act's ("HIPAA") Privacy Rule (the "Privacy Rule").

In addition to amending the Privacy Rule's existing accounting requirement, the NPRM implements and expands a provision of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") that requires HIPAA-covered entities ("CEs") and their business associates ("BAs") to account for disclosures of protected health information ("PHI") to carry out treatment, payment, and health care operations ("TPO") if such disclosures are made through an electronic health record ("EHR").

Background

Currently, the Privacy Rule requires CEs to make available to an individual upon request an accounting of certain disclosures of the individual's PHI made by the CE or its BAs during the six years prior to the request. A disclosure is "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."

For each disclosure, the accounting must include the date of the disclosure, the name (and address if known) of the entity or person who received the PHI, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for the disclosure). The accounting must include disclosures of PHI for any purpose, except for those purposes specifically listed in the Privacy Rule. Most importantly, the Privacy Rule currently excludes disclosures for TPO from the accounting requirement.

The current accounting provision applies to disclosures of paper and electronic PHI, regardless of whether the information is in a designated record set. A designated record set is a group of records maintained by or for a CE that is (i) used to make decisions about individuals; (ii) a provider's medical and billing records about individuals; or (iii) a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

Proposed Revisions to Accounting of Disclosures

The NPRM proposes the following changes to the Privacy Rule's current accounting of disclosures provision:

- Limiting the accounting provision to PHI in a designated record set as opposed to all PHI regardless of where it is located.
- No longer requiring CEs and BAs to account for certain categories of disclosures that are currently subject to the accounting provision, including but not limited to disclosures for health oversight purposes, impermissible disclosures for which the CE (directly or through a BA) has provided breach notice, and disclosures for research purposes.
- Reducing the time period for which CEs and BAs must account for disclosures from six to three years prior to the individual's request.
- Reducing the time period for a CE to respond to a request for an accounting from 60 to 30 days.
- Reducing the time period that CEs and BAs must maintain the documentation necessary to generate an accounting of disclosures from six to three years.

- Requiring CEs to provide individuals with the option of limiting their accounting request to a specific time frame, type of disclosure, or recipient.
- Requiring CEs to provide the accounting in the form and format requested by the individual (if readily producible) and, if not, in a readable hard copy form or another form and format agreed to by the CE and the individual.
- Clarifying that CEs may require individuals to make a request for an accounting in writing.
- Excluding patient safety work product reported voluntarily under the Patient Safety and Quality Improvement Act of 2005 (the "PSQIA"). The PSQIA establishes a voluntary reporting system to enhance the data available to assess and resolve patient safety and health care quality issues. To encourage the reporting and analysis of medical errors, PSQIA provides federal privilege and confidentiality protections for patient safety information called *patient safety work product.* Patient safety work product includes information collected and created during the reporting and analysis of patient safety events.

The NPRM proposes to maintain the elements that must be included in an accounting under the Privacy Rule's existing accounting provision but with a few minor modifications, such as allowing a CE or BA to provide an approximate date or period of time for each disclosure, if the actual date is not known. CEs and BAs would have to comply with the revised accounting of disclosures provision by no later than 240 days after publication of the final regulation.

New Access Report Requirement

In addition to the right to an accounting of disclosures, the NPRM proposes to provide individuals with a right to receive from CEs an "access report" that indicates who has accessed their PHI in an electronic designated record set. CEs would have to incorporate access by their BAs into the report.

While primarily designed to implement the HITECH Act requirement that CEs and BAs provide individuals with an accounting of disclosures through an EHR for TPO, the proposed access report would expand the HITECH Act requirement by

including *uses* of PHI (i.e., electronic access by members of a CE's or BA's workforce) in addition to *disclosures* (i.e., access by someone outside of the CE or BA). It would also expand the HITECH Act's requirement to include all uses and disclosures of all PHI in an electronic designated record set – not just disclosures through an EHR for TPO. The access report would cover only direct access through the electronic system in which the record is maintained. It would not apply to uses or disclosures facilitated through other means.

HHS states that the administrative burden on CEs of providing an access report will be reasonable in light of their existing obligation to log access to electronic PHI under the HIPAA Security Rule (the "Security Rule"). The Security Rule currently requires CEs to "implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic [PHI]." Thus, HHS states, systems with designated record set information should already be configured to record events such as users' access to information. The Security Rule also currently requires CEs to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." Accordingly, HHS asserts that CEs should already be logging and regularly reviewing reports of access to electronic PHI.

CEs and BAs would be required to produce an access report upon request beginning January 1, 2013, for any electronic designated record set systems that were acquired after January 1, 2009. For electronic designated record set systems that were acquired on or before January 1, 2009, CEs and BAs would be required to produce an access report upon request beginning January 1, 2014.

The new access report would include the following information:

- The date and time of access;
- The name of the person (if available) or the name of the entity accessing the electronic designated record set information;
- A description of what information was accessed (if available); and
- A description of the action by the user, if available (e.g., "create," "modify," "access," or "delete").

CEs would have to provide individuals with the option to limit their access report to a specific date, time period, or person. HHS also recommends, but is not proposing to require, that CEs offer individuals the option of limiting their access report to specific organizations. CEs would have to provide the report in a format that can be reasonably understood by individuals without an external aid.

As with the accounting of disclosures requirement, CEs would have 30 days to provide an access report upon request. The access report would have to be in the machine readable or other electronic form and format requested by the individual (if readily producible) or, if not, in a readable electronic form and format as agreed to by the CE and the individual. If the individual does not agree to accept the readable electronic format that is readily producible by the CE, the CE may provide a readable hard copy. A CE may not charge for providing the first access report to an individual in any 12-month period, but may charge a reasonable, cost-based amount for each additional access report that is requested within the 12-month period (which may include the reasonable costs of including uses and disclosures of BAs). The NPRM proposes to allow CEs to require individuals to make requests for an access report in writing.

A CE and BA would have to retain the documentation needed to produce an access report (e.g., the necessary access log) for three years. However, a CE would have to retain for six years copies of access reports it provides to individuals, and would have to maintain a designation of the persons or offices responsible for receiving and processing requests for access reports for six years from the last date the designation was in effect.

Changes to Notice of Privacy Practices

The NPRM proposes to require that CEs revise their notice of privacy practices ("NPP") to include a statement setting forth an individual's right to receive an access report. This addition would constitute a material change to the NPP and thus would necessitate that health care providers with a direct treatment relationship with individuals make the notice available upon request and have the NPP posted and available on or after the effective date of the revisions.

Health plans would have to distribute the revised notice to current members within 60 days of the revisions. HHS suggests that a health plan can minimize its

mailing costs by including notice of the new right to an access report in an annual mailing prior to the date that notification is required.

Public comments on the NPRM are due by August 1, 2011. The NPRM is currently available here.

back to top