

HHS Issues Proposed Rule Modifying Accounting of Disclosures under HIPAA and HITECH

Background

Under the HIPAA Privacy Rule, individuals are currently entitled to receive an accounting of disclosures made by a covered entity of their Protected Health Information (“PHI”). The covered entity must provide such accounting for the six years preceding such request (*see* 45 C.F.R. § 164.528). Historically, this right has been defined broadly, but has always been subject to a number of exceptions, including for disclosures of PHI for treatment, payment, and health care operations (“TPO”) purposes. In short, under the TPO exception, the covered entity was not responsible for providing individuals with information regarding disclosures of their PHI if such disclosures were made in connection with TPO disclosures (*see* 45 C.F.R. § 164.528(a)(1)(i)). The *Health Information Technology for Economic and Clinical Health Act of 2009* (“HITECH”) granted broader rights to individuals with respect to their PHI, including expanding the rights of individuals to receive an accounting of TPO disclosures made through an electronic health record (“EHR”), but has limited the time period for maintaining documentation of such disclosures to the three years prior to the date on which the accounting is requested (*see* 42 U.S.C. § 17935(c)).

At the time the accounting requirement was implemented, most records were maintained in paper and not electronic files. Now that electronic recordkeeping is the norm, disclosures are typically more frequent, and tracking them requires reliance on individuals to document properly the disclosure. In addition, electronic tracking of disclosures places increased burden on the underlying information system to store properly and separately record disclosures. HHS has proposed a new rule described below that purportedly seeks to address these difficulties while still allowing individuals access to broader information regarding how their PHI is used and disclosed.

Revised Right to Accounting of Disclosures

On May 31, 2011, HHS published a proposed rule that would modify and expand individuals’ rights to receive accountings of disclosures generally as follows:

- Individuals would have the right to receive a written accounting of disclosures in the three years prior to their request if such PHI is maintained by a covered entity or business associate in a designated record set. The reduction in the time period from six years to three years is designed to reduce the burden on health systems and to acknowledge the fact that most patients will not need more than three years of information to determine whether a disclosure was properly or improperly made and to whom.
- Individuals would be entitled to receive accountings of disclosures only for a specific list of reasons including, among others, disclosures for public health purposes, for judicial and administrative proceedings and in order to avert a serious threat to health or safety. Individuals would still be allowed access to information regarding disclosures for TPO but only in the form of an “access report” as described below.

- Accountings of disclosures would have to contain, among other information, the name of the entity or person who received the PHI as well as a brief description of the type and purpose of the disclosure.
- A covered entity or business associate would have to provide the individual with the option to limit any requested accountings to a specific time period or type of disclosure. For example, if an individual wanted information only related to disclosures to a certain company, or related only to a certain matter, the covered entity or business associate would be required to tailor the information provided in accordance with the request.
- A covered entity or business associate would be required to act on the individual's request for an accounting no later than thirty days following the request (note the Privacy Rule currently allows sixty days for a response).

Access Reports

In response to suggestions that accounting for TPO disclosures through an EHR would be unmanageable and costly, HHS has proposed use of an "access report" as a simplified way of ensuring that individuals have more comprehensive access to information regarding the use and disclosure of their PHI. This new right is intended to provide individuals with information about TPO disclosures as required by HITECH, but in a more manageable way. Significantly, the proposed rule also expands the reach of HITECH, which currently applies only to disclosures of PHI through an EHR. An individual's right to an access report would apply to uses and disclosures of electronic PHI in any electronic designated record set.

An individual's right to an access report would generally apply as follows:

- Individuals would have the right to receive an access report within thirty days of a request for PHI stored in an electronic designated record set.
- Such report would need to show, in a readable form and for the three years prior to the request, (1) date(s)/time(s) of access and (2) if available, (i) what PHI was accessed, (ii) who accessed the PHI, and (iii) actions taken by the accessing individual(s) with respect to the PHI (*e.g.*, modify or create).
- The proposed rule would require covered entities and business associates to comply with the access report requirement by January 1, 2013 or January 1, 2014, depending on the age of their respective electronic designated record set systems.

Changes to Notices of Privacy Practices

HHS also notes that covered entities would be required under the proposed rule to update their notices of privacy practices to reflect individuals' rights to receive access reports.

Challenges for Providers and Business Associates

According to HHS, compliance with the access report requirement should not create any additional burden on covered entities and business associates given that the HIPAA Security Rule already requires covered entities and business associates to keep internal access logs for stored PHI. Despite this HHS comment, compliance would still require significant effort and cost to ensure that such access logs are readable to the general public. Further, because many healthcare providers utilize multiple electronic data systems, complete access reports will likely require aggregation of PHI across these multiple systems into single, integrated reports. The aggregation and storage of such data in a modified form may also create significant burden on current EHR systems, not to mention the additional steps and processes (including training of staff) that

must be put in place to ensure that the instances of use and disclosure are properly documented and readily accessible in the event such a report is requested. Penalties for non-compliance with the HIPAA Privacy Rule can be significant, especially given enhanced penalties under HITECH. Finally, revision and redistribution of notices of privacy practices by providers will involve significant effort and cost to achieve compliance.

HHS is accepting comments on its proposed rule through August 1, 2011.

For further information, please contact the Ropes & Gray attorney who usually advises you.