Davis Wright Tremaine LLP

Proposed HIPAA Rule Raises Possibility of Financial Institutions Turning Over Employee Names to Health Care Patients

06.30.11
By Adam H. Greene

A recent proposed expansion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule would have a substantial impact on financial institutions that serve as business associates, potentially requiring them to turn over lists of employees to HIPAA covered entities' patients and enrollees. On May 31, 2011, the Department of Health and Human Services (HHS) published a proposed rule expanding an individual's right to receive an "accounting of disclosures" under HIPAA.

The proposed rule would continue to provide individuals with the right to receive an accounting of disclosures, but would also introduce the right for an individual to receive an access report: a report listing the names of persons at the covered entity and its business associates who electronically accessed the individual's protected health information in a "designated record set." HHS is accepting comments on the proposal until Aug. 1, 2011.

Financial institutions that act as HIPAA business associates should:

- Evaluate whether any of their electronic systems may qualify as designated record sets;
- Evaluate whether they will be able to comply with the rule if it is finalized as proposed; and
- Consider commenting on the proposed rule to seek clarification on whether it is applicable to financial institutions and to highlight any potential burden.

What HITECH said

The current HIPAA Privacy Rule requires a covered entity to provide an individual with an accounting of disclosures of all protected health information (hard-copy and digital), including disclosures to or by business associates of the covered entity. However, current law excludes certain types of disclosures, most notably disclosures for treatment, payment, and health care operations. The exclusion of disclosures for payment purposes generally excepts disclosures to or by financial institutions from the accounting requirements (e.g., where a financial institution is acting as a business associate because it provides certain services, such as a lockbox, to a HIPAA covered entity).

Although the accounting of disclosures provision has a history of being extremely cumbersome to covered entities and generating few requests from individuals, Congress nevertheless expanded individuals' right to the accounting. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Reinvestment and Recovery Act of 2009, requires HHS to remove the exception for treatment, payment, and health care operations to the extent that disclosures are made through an electronic health record.

The proposed rule

The proposed rule generally seeks to make two sets of changes to the current law. First, it seeks to lessen the burden associated with the current accounting of disclosures requirements (i.e., it excepts additional categories of disclosures and limits the types of protected health information for which an accounting is required). Second, and most relevant to financial institutions, is the proposal to provide individuals with the right to receive an access report detailing who has seen the individual's protected health information.

The access report is a response to the perception that the current law does not provide individuals with the information that they are most often seeking (i.e., they are less interested in how their information is being disclosed and more interested in whether a particular person has learned of their health information). Under the proposal, an individual would be entitled to receive a report providing the names, dates, and times that persons have electronically accessed their protected health information. The request could be limited to a particular person, time period, or institution (e.g., I would like to know whether my neighbor, who works at the hospital, has seen my health information). Or it could encompass all access by persons at the covered entity and its business associates over as much as a three-year period. A covered entity would have 30 days (with a single 30-day extension available) to respond with the access report, which (depending on the scope of the request) may include electronic access at business associates.

One of the key elements of the proposed right to an access report is that it is limited to protected health information about the individual in an "electronic designated record set maintained by a covered entity or business associate." "Designated record set," a term that has been in place since the final HIPAA Privacy Rule was published in 2000, is

defined as:

1. A group of records maintained by or for a covered entity that is:
   (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
   (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

2. For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

The key question for financial institutions is whether, to the extent that they act as business associates, any of their records meet this definition. In particular, there may be ambiguity as to whether a financial institution's lockbox records qualify as "billing records." To the extent that a financial institution is acting as a health care clearinghouse and is acting as a business associate of another covered entity, the financial institution should also assess whether its clearinghouse systems qualify as parts of the designated record set.

Under the proposal, if any of a financial institution's electronic systems are considered to be designated record sets (e.g., because they qualify as billing records), then the financial institution would be required to respond to an individual's request for an access report by providing the covered entity the names of any employees who electronically accessed the individual's information in such systems. The covered entity would then add the data to its own access report and turn this information over to the individual.

Next steps

A financial institution that is a business associate should consider whether any of its electronic systems qualify as "billing records" or otherwise may fall within the definition of "designated record set." If so, it should consider the impact of this proposal, including its ability to comply (the proposed compliance date would be Jan. 1, 2013).

Financial institutions may also consider commenting on the proposed rule, such as by highlighting any potential burdens or concerns, or by seeking clarification regarding whether the rule would encompass certain types of electronic systems.

If you have any comments or would like more information, please contact Adam Greene.

Disclaimer