Unfinished Business: Solving the HIPAA Accounting Rule Dilemma

May 2013

Now that the Health Information Technology for Economic and Clinical Health (HITECH) rules finally have been released, health care companies and their business partners will turn to the significant challenges that remain for achieving full compliance and meeting these important new standards. At the same time, while this “omnibus” Health Insurance Portability and Accountability Act (HIPAA) regulation implements most of the provisions of the HITECH law, there remain some important elements of unfinished business for the U.S. Department of Health and Human Services (HHS) in finalizing the HITECH mandate. At the top of that list is the remaining obligation to implement changes to the HIPAA accounting rule.

The HITECH statute always has had an ambiguous goal. On the one hand, HITECH was designed at its core to provide economic incentives for doctors and hospitals to implement electronic health records. At the same time, Congress decided that while providing these incentives, it was also going to require stringent new privacy and security provisions as a result of these electronic health records. (And then Congress designed a wide range of new HIPAA provisions, most of which have nothing specific to do with electronic health records). The Omnibus regulation—four years in the making—now implements these provisions. (See Nahra, “The New HIPAA/HITECH Era Is Finally Here,” Privacy in Focus (February 2013)).

Accounting Rule Background

One of the HITECH changes that dealt directly with electronic health records involved the HIPAA accounting rule. (The other involved a patient’s right to access [or receive a copy of] their records). The HIPAA accounting rule was an unlikely candidate to create a significant HIPAA debate. While an original HIPAA provision, and one of the individual rights created for patients, it has seldom been used by patients across the country. Most covered entities have received few accounting requests. At the same time, each request is burdensome, as it requires a HIPAA-covered entity to gather information from a wide range of sources, both internal and from hundreds (and perhaps thousands) of business associates.

The accounting right allows individuals to receive a listing of certain disclosures of their health care information, outside the areas of treatment, payment and health care operations (known within HIPAA circles as “TPO” disclosures). In HITECH, Congress chose to modify the accounting right. Specifically, the HITECH legislation provided that this accounting rule exception for TPO disclosures of HIPAA-protected health information would no longer apply to TPO disclosures “through” an “electronic health record.”

The accounting regulatory changes have (for somewhat unexplained reasons) always been on a different (and slower) track than most of the other HITECH provisions. HHS issued a specific Notice of Proposed Rulemaking (NPRM) on the accounting rule, separate from the remaining provisions, on May 31, 2011 (available at 76 Fed. Reg. 31426).
It is fair to say that this proposal was not greeted with significant enthusiasm from anyone. Instead, it was soundly criticized by virtually every relevant audience and in every relevant comment. See generally Nahra, “The HIPAA Accounting NPRM and the Future of Health Care Privacy,” BNA Health IT Law & Industry Report (July 4, 2011).

Now that the Omnibus rule is out, HHS is turning its attention once again to the HIPAA accounting rule. In this re-evaluation, HHS should formally reject its NPRM creation of an access right, withdraw its discussion of the HIPAA Security Rule and develop a proposal that responds specifically to the mandate of Congress without requiring additional new compliance obligations beyond the congressional instruction.

Summary of Concerns

While there are a variety of reasons to criticize the original NPRM proposal on the accounting rule, several critical points stand out.

- The HHS proposal wildly misconstrued the state of feasible technology for tracking uses and disclosures of health care information, resulting in a proposal that was both not realistically feasible and exceedingly burdensome.
- HHS identified few specific patient interests that were furthered by the NPRM proposal, and the interests that were identified either are already addressed through privacy notices or are more appropriately and directly addressed by privacy investigations.
- HHS failed to assess the risks to health care company employees that would be created by providing information about them to patients, in addition to failing to analyze other unintended consequences of providing details about internal operations of health care facilities.
- HHS based many of its assumptions about technological feasibility on a misunderstanding of its own previous interpretations of the requirements of the HIPAA Security Rule.

An Accounting Proposal

Accordingly, while the NPRM proposal should be withdrawn, HHS must still address the congressional mandate on the accounting rule. In implementing a rule related to this mandate:

- Any new changes to the accounting rule should be limited to “disclosures of PHI” for treatment, payment and health care operations purposes that are made “through” an “electronic health record;”
- “Electronic health records” should be limited to those electronic health records that incorporate “meaningful use” standards; and
- Any compliance period for this new requirement should be delayed until the meaningful use standards incorporate a corresponding requirement connected to this accounting rule change (to ensure that these obligations can be met through appropriate technology) and the implementation date for this new meaningful use standard is in place (with accounting obligations applying only to disclosures from that point in time forward).

In implementing a final regulation (whether based on an additional proposed rule with comment or otherwise), HHS should focus its proposal on four specific elements, all taken from the HITECH statute.
Disclosures Only

First, any new accounting rule proposal should be focused exclusively on “disclosures,” as the statute dictates. Uses and disclosures by a hospital or other health care providers, for example, will be exactly the type of information use that already is spelled out in the privacy notice. There is little additional privacy interest in identifying specific employees who were involved in using a patient’s health care information in the settings where these activities are routine and consistent with the overall approach of HIPAA. To the extent that a particular entity is unable to distinguish between uses and disclosures in any particular situation, it obviously can include uses, as well, in its discretion. But the inability of some companies to draw this distinction should not result in a broadened mandate for everyone beyond the statutory requirements.

Only Those Disclosures “Through” an Electronic Health Record

Second, the requirement should only be applied to disclosures that are “through” an electronic health record. The statutory language focused explicitly on disclosures that are made “through” an electronic health record. This appears to incorporate the idea that it is these electronic health records where the appropriate technology can exist and where some kind of centralized control can be made involving these kinds of “accounting” issues. This technology and this centralization simply do not exist in all places in all covered entities (and, as we know now, do not exist today even in many electronic health records). Information is used and disclosed across health care companies in the normal, routine course of operations. Any accounting rule proposal should be limited to disclosures that are made “through” this core electronic health record, not to all disclosures across a covered entity or business associate outside of this core electronic health record.

Only Applied to “Meaningful Use” Electronic Health Records

Third, HHS should ensure that “electronic health record” is defined in a way that is consistent with the overall approach of the HITECH law, to incorporate the “meaningful use” electronic health records that are at the core of that law. Congress imposed this requirement on covered entities that use these “meaningful use” electronic health records. This obligation should be imposed on those that use these “meaningful use” electronic health records, as well as the limited number of business associates who use these specific electronic health records in a way that they make disclosures “through” these records. All other disclosures of information—made outside of this specific electronic health record context—should be excluded from this expanded requirement.

The Requirement Should Be Applied Only When the Technology Is in Place

Last, any new accounting requirement should not be imposed until the needed technology exists and is implemented across the health care industry. This means that even an appropriately limited proposal is not appropriate until it is feasible—and it will be feasible only when the core electronic health records in fact have the capabilities to provide this accounting detail—and relevant entities have been required to implement this new technology. Any requirement prior to this time is destined to create an impossible obligation—one where the burden and feasibility issues far outweigh any potential benefit to individuals.

Conclusions

In applying this congressional mandate, HHS should strive for an approach that addresses the mandate as necessary, but that does not create unnecessary burdens and costs (as well as potential harm to health care company employees or other HIPAA entities) in order to promote generalized patient interests that are better addressed in other ways. While there clearly are relevant patient interests at stake, these interests can be
addressed in a more targeted and more cost effective way through other means than the broad obligations envisioned by the NPRM proposal. HHS should withdraw its NPRM proposal in its entirety, particularly in relation to the proposed access report, and should focus its attention on a much more limited proposal (as required by Congress) that focuses exclusively on disclosures of PHI through a certified electronic health record at the time when this technological capability is built into these core electronic health records.