

Are HIPAA Changes Coming?

June 2018

Privacy in Focus®

While the health care industry continues to wonder what the enforcement philosophy and approach of the HHS Office for Civil Rights (OCR) will be under new leadership, there is now a likelihood that some elements of the HIPAA Rules will be undergoing change in the next few years, based on a series of upcoming rulemaking proceedings. At a minimum, we can expect several different rulemaking proposals over the course of 2018.

What Is Happening?

As part of a broader administrative document setting forth a broad regulatory agenda across the federal government, HHS has indicated an official intention to propose changes to several components of the HIPAA rules. This formal regulatory announcement follows various media reports of speeches by HHS leadership about these expected proposals.

The Accounting Rule

The most significant proposal involves the HIPAA accounting rule. The accounting rule has been one of the primary “individual rights” in the Privacy Rule since it first went into effect. As part of the HITECH statute, Congress directed that certain changes be made to the accounting rule, primarily to broaden the scope of the rule in connection with electronic health records. While the statutory language created meaningful concerns in the health care industry, these concerns exploded when HHS – in May of 2011 – issued a proposed rule on the accounting provisions. (It has never been fully explained why the accounting rule provisions have been on a separate time frame from most of the remainder of the HITECH

Practice Areas

Privacy, Cyber & Data Governance

changes.)

This proposal was met with widespread and virtually universal criticism. While there are a variety of reasons to criticize the NPRM proposal on the accounting rule, several key 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.

As I said at the time:

My conclusion is that this NPRM is fundamentally misguided and should be withdrawn – it relies on an unreasonable interpretation of the HIPAA Security Rule, fails to reflect the technological reality of today’s health care environment, and mistakenly presumes (even if its assumptions were correct) that creation of this access report will impose little burden, all to support (in a surprisingly untargeted way) an ill-defined and relatively unjustifiable patient interest in learning specific details about the internal activities of health care companies. See generally, Nahra, “The HIPAA Accounting NPRM and the Future of Health Care Privacy,” *BNA Health IT Law & Industry Report* (July 4, 2011), available here.

Now, *seven years* after this proposal was issued, HHS is withdrawing the proposal. In its place, HHS will initiate a new “advanced notice of proposed rulemaking,” to gather stakeholder input on how to move forward with the accounting rule. It will be critical for HIPAA-covered entities and business associates to carefully think through this issue so that they can help HHS get to a much more balanced approach on the HITECH requirements for the accounting rule.

In general, I encourage HHS to consider the following points:

- 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).

Patient Privacy Notices

HHS also has indicated its intention to “change the requirement that health care providers make a good faith effort to obtain from individuals a written acknowledgment of receipt of the provider’s notice of privacy practices, and if not obtained, to document its good faith efforts and the reason the acknowledgment was not obtained.” While we have not yet seen a lot of discussion about the interests served by this proposal, HHS seems to be of the view that this obligation is burdensome for health care providers without much benefit for patients. While there are meaningful criticisms of the language of most privacy notices, it will be interesting to see how HHS removes this requirement while still making clear how individuals should receive these notices.

Individual Shares of Civil Penalties

HHS also has indicated that it will be issuing later this year an “advance notice of proposed rulemaking” requesting public input for how OCR may share funds collected from HIPAA enforcement actions with affected individuals. OMB says the notice “would solicit the public’s views on establishing a methodology under which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected with respect to the offense.” This step also is required by the HITECH statute. However, despite this announcement, this step may still be a long time in coming. Not only is this an “advanced notice” of proposed rulemaking – meaning that it is simply seeking information from which HHS might develop a future proposed rule – but OCR has announced similar plans 12 previous times, all without any actual activity. There is no obvious reason why this year should be any different.

This issue is a challenging one, and there is likely to be a lot of controversy about any proposal. Defining “harm” in the context of a regulatory enforcement proceeding is extremely difficult, and will put additional pressure on OCR’s already tight resources. There also will be a concern from industry that this provision will lead to higher demands for monetary payments – to “compensate” these individuals while also permitting OCR to obtain significant amounts for its own purposes. In addition, as courts across the country continue to struggle with definitions of “harm” in class action litigation, there likely will be reasonable concerns that any OCR definition of harm will spill over to a litigation context.

Good Faith Sharing

The most abstract provision – and one not driven in any way by the HITECH statute – involves OCR’s stated effort to “modify the HIPAA Privacy Rule to clarify that health care providers are presumed to be acting in the individual’s best interests when they share information with an incapacitated patient’s family members unless there is evidence that a provider has acted in bad faith.” Presumably, this provision is driven by ongoing concerns about opioid abuse situations – which, on a broader level, is driving virtually all of the health care privacy debate at this time, particularly in Congress.

While the goal of this provision may make sense, it is not at all clear why it is needed. OCR clearly can (and generally has) taken this view in its enforcement efforts generally. It clearly has the ability to insulate providers from enforcement if they disclose in this context, and can change its approach if there is an indication of bad faith. So, until we see a proposed rule, it is hard to understand what this provision will do beyond setting into the rule current enforcement discretion, and it will be interesting to watch whether this provision “flips the burden” for OCR in enforcement settings, where they will be required to show bad faith before taking enforcement action.

Conclusions

The health care industry likely will see a flurry of these proposals over the course of the next year. Most of these proposals seem to be at the “advanced notice” stage, meaning that any meaningful implementation of new rules is still a long way off. However, particularly for the accounting rule, it will be important for the industry to think carefully about how best to engage in this dialogue, since these provisions may require significant resources for the industry to implement.

© 2019 Wiley Rein LLP