wiley

NEWSLETTER

HIPAA's Unanswered Questions

September 2012

Another month goes by without the publication of the final Health Insurance Portability and Accountability/ Health Information Technology for Economic and Clinical Health (HIPAA/HITECH) rules. It's now been three and a half years since the HITECH statute was passed and more than two years since the proposed HITECH rules were published in July of 2010. And there's no clear end in sight to this delay.

What are the top unanswered questions about these rules and how they will affect the HIPAA structure and health care privacy? Here's my take on the top ten issues and unanswered questions.

What's Taking So Long?

There's really no answer for this. It's true that the framework for these modifications is a bit unusual. Congress passed the HIPAA statute in 1996, expecting to follow it with specific legislative provisions on privacy and security. As we all know, that didn't happen. That left it to Health and Human Services (HHS) to draft the original HIPAA Privacy Rule (followed by the HIPAA Security Rule and various other provisions).

In HITECH, therefore, Congress passed legislative provisions revising an HHS regulation. Unusual, but certainly not unprecedented. And Congress drafted the specific language that would be used to modify the rules. So it shouldn't have been that hard, at least, to incorporate these changes in the rule.

Yet it has proven very difficult to work through the bureaucratic process. Where there were specific deadlines in the law (such as with the breach notification provisions), HHS was able to get something issued (even if it was in the form of an interim final regulation). Not much else has happened.

And, given the precision of the Congressional language, including the specific effective dates of these provisions (many of which were to be effective in February 2010), it was irresponsible of HHS to wait until after these effective dates had passed to issue a proposed rule that made clear that the HITECH provisions were not in fact self-implementing and (apparently) meant nothing on their own. That resulted in enormous wasted time, money and energy (particularly to revise business associate agreements) where there was no reason for this action. (See Nahra, "What's Important about the HITECH NPRM?" *Privacy In Focus* (August 2010)).

Obviously, a lot has been happening at HHS in the past few years, with most of the regulatory activity focused on health care reform. But there really is no explanation or any good excuse for why it has taken so long to issue these final privacy and security rules, particularly since Congress already did most of the work (for better

or worse) in 2009.

What Will Happen If the Rules Are Issued After the Election?

At this point, while various senior privacy officials have made comments indicating that the final rules would be published this summer, that does not seem to be the case. It certainly could still happen. But it is increasingly unlikely that the rules will be out by the end of the summer. That also makes it less likely that they come out before the election (and, obviously, that political issue has now become a significant variable independent of whether the final rules have been completed).

So what is likely to happen if the rules do not come out before the election? Will the results of the election matter?

There's minor history to guide us. The original HIPAA Privacy Rule was issued at the very tail end of the Clinton Administration, following the 2000 election. It was one of the last regulations to be issued by the Administration and was clearly viewed by that Administration as part of its legacy.

There obviously are two scenarios on the election—President Obama wins, or he loses. If he wins, any time pressure for the HIPAA rules probably disappears (other than the ongoing pressure to get something out at some time). That would give the Administration some time to issue a broader or stronger set of privacy provisions, with less political pressure, if it wanted to do so. As discussed below, there is some indication that the Administration would like to make broader changes to the HIPAA structure, although that was not at all obvious from the proposed HITECH rule.

If President Obama loses, we can expect that a final HITECH rule will be issued before the end of the Administration, based on whatever language has been prepared to this point in time. It is unlikely that the Administration will miss this chance. While (as with the Bush Administration) there will be some opportunity for a new Administration to make changes, the shorter compliance time period of seven months makes this somewhat unlikely.

So, the election results may have some impact on the new HITECH rules, but my best guess is that the results will affect timing more than the substance of the rules.

Is There Going to be Something Dramatic?

Aside from the length of the delay in general, the most surprising element is that the proposed HITECH rule said so little. The overwhelming majority of the proposed rule was virtually a clerical exercise—translating the congressional language into regulatory provisions. There was little interpretation of the congressional language and little new regulatory modification independent of Congress' action. While HHS indicated that its proposal was going beyond the HITECH language based on HHS' experience in enforcing the HIPAA rules, the proposal actually made very few independent changes. Therefore, there was no good rationale for why it took so long for this initial proposal to come out.

So, in many ways, the single biggest "unanswered question" may be whether HHS has something dramatic up its sleeve. Let me be clear—there is no evidence whatsoever to lead to a conclusion that HHS will be making significant changes to the HIPAA rules in this HITECH rulemaking. There was nothing dramatic in the proposed rule, and nothing has even been floated by the Administration in the time since the proposal (aside from the fundamentally misguided accounting proposal, which is on a separate track and does not seem to be linked to any other changes).

But, if there is something dramatic under way, that would at least provide some justification for these otherwise unexplained delays, even if the result would seem to be an unfair one of making change without an opportunity to comment. Given the debacle of the accounting rule (see Nahra, "The HIPAA Accounting NPRM and the Future of Health Care Privacy," *BNA Health IT Law & Industry Report* (July 4, 2011)), HHS should avoid the option of making dramatic changes to the HIPAA rules, unless it gives the health care community a full and fair opportunity to comment on any proposals.

What Will Happen with the Breach Rule?

In terms of actual impact on the health care industry, by far the biggest effect from HITECH to date has been the publication of the interim final regulation related to security breach notification. This regulation—which took effect despite not being "final," has resulted in notification of thousands of security breaches, large and small, across every segment of the health care industry. This has led to publicity, lawsuits, enforcement and general attention to overall security practices.

In publishing the interim final regulation, HHS clarified that the HITECH statute incorporated a "risk of harm" threshold, with the result that security breaches will need to be disclosed to individuals where there is a "significant risk of financial, reputational or other harm" resulting from the breach. This reporting threshold created significant controversy (and generated substantial support). Moreover, whatever one's view on the standard, it is clear that (1) many security breaches are being disclosed and (2) health care companies do not appear to be drawing too fine a line on this risk of harm, given many of the "close call" breaches that have been disclosed, where any harm seems either very speculative or minimal.

After receiving comments on the proposal, HHS apparently made its decision on a final regulation and sent the final regulation off to the Office of Management and Budget (OMB) for final approval. While awaiting final approval at OMB, HHS withdrew this proposal. Despite widespread media reports claiming that this withdrawal was a "victory" for patient privacy interests, it is in fact impossible to tell what this withdrawal means. Was it withdrawing a "status quo" proposal that simply adopted the terms of the interim regulation? Or had it made substantial changes and then changed its mind? Or was the withdrawal based solely on process (OMB had too many health care regulations to review, so it asked for "no deadline" regulations to be withdrawn)?

In any event, this final breach regulation will be included in the omnibus HITECH regulation, whenever it is finally published. Given the "success" of the interim final regulation to date, in terms of the disclosure to individuals, HHS and others about a large number of security breaches, there is no obvious need to revise the

risk-of-harm threshold. There clearly are many open questions (such as how to define or identify "other" harm from a breach and what individuals should do about nonfinancial threats), as well as the purpose of the media disclosures. But, given the impact of this regulation on the industry to date, the final language will clearly be of enormous significance to the health care industry, its business partners and individuals across the country.

Marketing

One of the key "new" provisions of the HITECH statute involved marketing and the desire of Congress to preclude marketing that involves "remuneration." While written in a convoluted manner, the statute appeared to alter the existing marketing provisions of HIPAA by imposing a new restriction in situations where the previous rule permitted individual information to be used or disclosed in connection with marketing. Under HITECH, if the entity received "direct or indirect remuneration" for the marketing, now an authorization would be required.

This statutory provision cried out for a regulatory interpretation, primarily as to the meaning of "direct or indirect" remuneration. However, the proposed regulation did little to clarify the statutory terms. The language of the final rule will be important to significant segments of the health care industry (including pharmaceuticals and wellness programs), by defining the scope of these new limitations.

Sale

The HITECH law also included similar language about the "sale" of protected health information. As with the marketing provisions, while HHS "clarified" some exceptions to this prohibition, it did not address some of the statutory ambiguities. While there is little blatant sale of information that is permitted today, consistent with the current rules, this provision does have an impact on certain practices that involve cooperative treatment efforts, research and other adjacent activities to core treatment and payment actions. Again, to the extent that HHS clarifies or expands on this language, this provision will have an important impact on a wide range of health care activities.

Subcontractors

One of the major provisions of the HITECH law expands the reach of HIPAA from covered entities to business associates. While business associates (service providers to health care entities) always have had contract obligations, the HITECH law would now subject business associates to direct compliance obligations with enforcement risks.

In the proposed HITECH regulations, HHS (in perhaps the most significant "interpretation" in the proposed rule) determined that this new legal obligation would be applied not only to direct business associates, but also to all downstream contractors of the business associates. This conclusion dramatically expanded the impact of the HITECH change. Moreover, because of the substantial obligations imposed by the HIPAA Security Rule, this interpretation exposed many vendors to HIPAA risks in situations where they might have no realistic reason to know that they are receiving or accessing information protected by the HIPAA rules. While

there is a significant ongoing debate about the fairness of this approach for these downstream contractors, the final rule will answer the question of whether downstream contractors will need to meet new HIPAA compliance responsibilities and will define the full scope of these responsibilities. This interpretation will have an impact on any company that contracts downstream from any health care company, regardless of how many "links" there are in this contracting chain.

Allocation of Responsibility with Business Associates

The expansion of compliance responsibilities to business associates also has raised a variety of questions related to the relationships between covered entities and their business associates. For example, many have questioned whether there is any continuing need for business associate contracts at all. In addition, as the breach situations involving business associates have made clear, there is an ongoing complexity to allocating responsibility and potential enforcement exposure among the covered entity and its business associates. This is being handled today on a situation-by-situation basis. Will the final rule address this allocation issue, in terms of breach response, other mitigation activities, enforcement exposure or any other way in which the covered entity and a business associate may both have responsibility (and where that responsibility typically will be overlapping)?

Enforcement

While we have been waiting for new rules, the HHS Office of Civil Rights has been engaged in a parallel trail of activity relating to enforcement of the existing HIPAA rules. Enforcement clearly has increased, although the number of enforcement actions remains small. The ongoing HIPAA audit program has exposed dozens of health care companies to proactive audits, independent of any specific wrongdoing or reported problem. And HHS clearly is beefing up its investigations, at least in terms of the volume of early stage investigations. Many of these inquiries are based on reported breaches or other complaints and the investigations often look into activities that seem largely unrelated to the initial reports.

At the same time, there is an ongoing risk that state attorneys general—who were given clear HIPAA enforcement authority in the HITECH statute—may decide that they can initiate enforcement actions under the new rules at any time, without waiting for a final HHS regulation. In one highly publicized situation, for example, the Minnesota Attorney General (AG) brought a HIPAA enforcement action against a business associate, even though the business associate is not subject to the HIPAA rules yet in the eyes of the primary enforcement agency.

As the publication of the final rule continues to be delayed (and there will be a seven-month compliance period from any final publication), we will be watching to see whether HHS or state AGs compensate for this delay with an expanded enforcement approach or more aggressive enforcement activity.

Is There a New Era of Health Care Privacy Coming?

The last big unanswered question may be the most interesting. As the HITECH rules have been delayed, we have seen a variety of new regulations in other parts of the health care industry that have touched on health care privacy issues and HIPAA. Recently, we have seen new rules involving Stage 2 Meaningful Use, the proposed Nationwide Health Information Network and the Accountable Care Organization rules, along with others. Many of these regulations have addressed privacy rules in two ways. While they typically have endorsed the HIPAA regime and adopted HIPAA as a baseline structure, these proposals also have added to HIPAA in important ways. Some have given new consent rights. Others have proposed new kinds of security controls or other kinds of actions that add to HIPAA's requirements. In these situations, the justification for a new approach has not been at all clear. While each little HIPAA tweak may not itself be important, it is surprising to see so many situations where the Administration has determined that HIPAA is not "good enough" in a specific situation, even where it is the governing rule for the remainder of the health care system.

So, while we await the final rules, it is important to consider whether these other steps—outside of core HIPAA regulation—either predict changes in the final HIPAA/HITECH rules or indicate that there may be a next step "HITECH 2" that may try to more dramatically change the overall HIPAA structure.

Conclusions

The continuing delays in issuance of the HITECH rules have led to confusion and uncertainty. At the same time, increased enforcement and ongoing security breach reporting means that every company in the health care industry—and all of their business partners—needs to be paying close attention to protecting the privacy and security of patient data. The health care industry needs to maintain its vigilance on privacy and security in the face of these delays, while at the same time preparing for the HITECH future—whenever it comes—that may significantly change the privacy and security environment.