wiley

NEWSLETTER

What to Do While You Are Waiting for the HIPAA Rules

July 2012

It sounded like they were finally coming. The wait would soon be over. The final Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) rules were sent to the Office of Management and Budget (OMB) for approval on March 24, 2012. OMB has 90 days in which to approve the regulations. In June 2012, in its May "Retrospective Regulatory Review Update," the Department of Health and Human Services (HHS) indicated that it was targeting July 2012 for publication of the final rules. During a presentation in early June, the director of the HHS Office of Civil Rights indicated that the final rules were "very close." In the same week, the national coordinator for Health Information Technology announced that the final rules would be out before the end of the summer.

But, now we see that OMB has requested an extension of the deadline, for at least another 30 days. Some other rules under review have been under this theoretical 90-to 120-day review since as early as May of 2011. We're now well past the three-year anniversary of the passage of the HITECH law in February 2009. And we're quickly approaching the two-year anniversary of the publication of the proposed HITECH rule (from July 2010). Does anyone even remember what the proposed rule says? (In case you have forgotten, see Nahra, "What's Important about the HITECH NPRM*?," Privacy In Focus* (August 2010)).

So, while we wait yet again, it is clear both that these rules are coming, sometime, and that they are moving toward final publication, even if does not seem imminent. While its not unreasonable for companies to simply wait, there are several key steps that should be focused on now, while there is time to make a difference.

We Know Most of What the Rules Will Say

Obviously, the substance of the final rules will be important. And despite the fact that the proposed rules themselves broke little new ground (and chose instead to simply adopt without variation the statutory provisions identified by Congress), it certainly is possible that the final rules will contain significant new provisions that have not been subject to public comment. (Query-is that why all of this has taken so long? And, if so, is it fair to publish final rules with provisions that have not been subject to public debate?)

However, we know *most* of what the final rules are going to say, at least in its most significant provisions. We know that business associates will be subject to specific compliance obligations under the final rules. We know that business associates will need to follow the HIPAA Security Rule in its entirety. We know that business associates will not need to follow all of the Privacy Rule, but instead will need to comply only with those provisions that are incorporated into standard business associate agreements.

So, since we know most of what the rules will say, it is fair and appropriate to move forward now, to identify where changes need to be made and to develop a plan for these changes during the compliance period for these rules (expected to be seven months following publication).

Use This Period to Evaluate Where You Stand on What Is Not Being Changed

At the same time, while the HITECH changes will be important, they will not affect many provisions of the HIPAA rules. The substance of the Security Rule is not changing in any way. Much of the Privacy Rule is not affected by HITECH. Nonetheless, I encourage both covered entities and business associates to examine all of their current HIPAA policies, to ensure that the status quo on complying with these provisions is appropriate in today's environment. The lengthy delay in implementing the HITECH rules has led-in some instances-to continued evolution of privacy and security practices, some positive and some less so, so companies are well advised to ensure that their practices are appropriate today, regardless of whether a particular policy is affected by the final HITECH rules.

Enforcement Is Growing and Becoming More Broad-based

It also is important to remember that HIPAA enforcement is an ongoing possibility, even before the rules are finalized. While we have not seen an enforcement explosion, we are seeing a slight uptick in enforcement actions, with many of them sending significant messages to the health care community. The Blue Cross Blue Shield of Tennessee case sends the message that HHS will go after companies even where they have provided appropriate notification of a security breach. The Phoenix Cardiac Surgery case, where a $100,000 fine was levied against a physician practice, shows that HHS will pursue cases, even against small entities, where there was a "systemic failure to implement any security" and "lax privacy protections," and the target "had to start from scratch" on HIPAA compliance. Both of these cases make clear that HHS will institute enforcement even where the original complaint or notice relates to a different issue. The most recent action, against the Alaska Medicaid Agency, sends a loud and clear message that HHS will go after anyone, even a state agency providing health care services to the poor. And the Minnesota attorney general's disturbing action against Accretive Health sends the message that not everyone agrees that business associates are not yet subject to enforcement under HIPAA. So, while you wait for the rules to come out, HHS is not waiting to continue and expand its enforcement efforts.

The HHS Audit Program Is an Additional Exposure Risk

HHS also is in the midst of a significant audit program, focused on improving overall HIPAA compliance. Close to 200 entities of all kinds will be subject to audits before the end of 2012. These audits are significantly disruptive and require a meaningful effort from any affected entity. And while HHS has indicated that the

primary purpose of these audits is to gather information about the state of the industry's compliance efforts and to provide useful information about compliance strategies, HHS has explicitly refused to say that it will not institute enforcement actions against specific companies based on their audit results. Accordingly, while one Office for Civil Rights (OCR) investigator is quoted as saying that they are moving enforcement efforts from "HIPAA lite to HIPAA jolt," and HHS also has said that the audits are not meant to be punitive, they also have said (not surprisingly) that if an audit finds "no evidence of trying to comply" or if an entity "actively misleads the audit team," then enforcement can result from the audit itself.

Security Is the Big Thing

With all of the attention devoted to privacy issues in Congress, in the media and in the overall public debate, it is clear that the most meaningful current risks relate to security practices. Security breaches are routine in the health care industry and among business associates in all kinds of entities, large and small. While the health care industry is not unique in this-and may not even be as bad as some other industries-there are enormous risks to health care data from security breaches. In addition, as all initial audit findings confirm, full compliance with the complexity and comprehensiveness of the HIPAA Security Rule remains low. For business associates, the need to move from the current contractual standard of "reasonable and appropriate" safeguards to full compliance with the HIPAA Security Rule clearly is the biggest challenge about HITECH compliance.

On the substance, we know exactly what the HIPAA Security Rule will say. It is not being changed in any substantive way by the HITECH statute or the proposed HITECH rules, other than to make business associates subject to the full rule. Therefore, there is no reason to wait at all to begin or expand HIPAA compliance efforts on security. The risks of a breach exist today. The risks of an audit exist today. The risks of failing to meet the government's guidance on HIPAA security (even including the wildly aggressive recitation of HIPAA audit trail requirements from the misguided proposed HIPAA accounting rule) are quite substantial. While business associates will have seven months to bring themselves into compliance, this may not be enough time for many companies. This work should begin now. For covered entities, the obligations exist today, and the risks are clear and growing. Every company in the health care industry, whether a business associate or a covered entity, should be actively engaged in aggressive reviews of HIPAA security policies and ongoing security compliance efforts.

Breach Notification Remains a Major Challenge

The breach notification rule is in effect now, even as an interim final rule, for both covered entities and business associates. The final rule may change the current harm standard (which could create even larger challenges) but it is clear that this current interim final rule is having an impact across the health care industry, more than any other provision of the HITECH statute. And because HHS has made clear that reporting a breach, even if all reporting requirements are met, does not avoid potential HIPAA enforcement, it is crucial for companies both to develop an appropriate breach response plan and to improve overall security to reduce the chances of a security breach. Companies must be ready to act quickly in connection with a security breach. In my experience, a failure to get the right information to the right people quickly enough is the

biggest single flaw in companies' reporting efforts. This risk is current and substantial right now.

Get a Handle on the BA Side (and Downstream)

While the rules are not yet final for business associates, the coming changes do place a higher priority on managing an overall approach to business associates (and for client relations by business associates). Companies should, *now*, be reviewing their business associates to make sure all of them have been identified and that their contractual status has been identified. I would not make efforts yet to revise business associate contracts that have not already been modified by HITECH, but knowing who your contracts are with and what they say now is an important effort. Contracts need to be in place with all business associates now. They may need to be changed under HITECH, but the requirement exists today. Covered entities should have an approach in mind for handling HITECH's requirements, and this starts with a complete identification of all business associates, an assessment of the risks posed by these entities and an overall view of future contracting efforts. For business associates, the same concepts apply to downstream contractors-business associates should identify all contractors who are captured by the definition of business associates, and perform the same assessment done by covered entities. Also, business associates should develop their own strategy for how they will implement appropriate contractual changes when the final rules are released.

Identify Marketing Issues and Any Other "Sale of PHI" Issues

While my primary focus in this evaluation is on security issues, there certainly will be changes to the HIPAA Privacy Rule. I do not expect these changes to be dramatic. However, even aside from the realistic possibility of unknown "wild card" issues emerging in the final rules, we know that two of the primary changes from HITECH will involve remuneration/payment for certain activities. We expect two different provisions to be implemented, one dealing with marketing that involves payment and the other involving the sale of Protected Health Information (PHI). While the details of these provisions are not clear-and the proposed rules did very little to explain the ambiguous HITECH statutory language-I encourage covered entities and business associates to identify any practices that may be implicated by these provisions. This will involve any situation where a covered entity or business associate is being paid to do something that involves marketing or the exchange of PHI. Obviously, this will not affect payment for specific services, but anything beyond that may be in play. I do not necessarily encourage these practices to be stopped at this point (although many companies will identify marketing activities that will be prohibited without authorizations under the new rules). Instead, at a bare minimum, companies should identify their activities that are affected by these provisions, so that once the final rules are published, they can move quickly to eliminate programs that violate the rules, develop compliant approaches or alter practices to act consistently with these new prohibitions.

Conclusions

On the whole, the delays in issuance of these final HITECH rules continue to create confusion. Given the long passage of time, this delay also appears to be generating a passivity, or a general loss of interest, in the new HITECH requirements. That is a mistake. The risks of privacy and security breaches-especially expensive, embarrassing and time-consuming security breaches-are substantial and real. Companies should use this

interim period wisely-to improve security practices, identify areas of risk and plan for the actions that will be required during the HITECH compliance period. *Use this time wisely-the results will be well worth the expenditure of time and money.*