Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

HIPAA Update Ushers In Broad Security, Reporting Regime

By Allison Grande

Law360, New York (January 22, 2013, 10:37 PM ET) -- With last week's massive overhaul of the Health Insurance Portability and Accountability Act, federal health officials imposed heightened data security and breach reporting obligations on health care providers, insurers and their business associates that sent them all scrambling to rework contracts and establish procedures to meet the expansive new requirements, attorneys say.

The 563-page final rule released Jan. 17 formally implements sweeping changes to HIPPA, including expanding liability to include billing contractors and other business associates of already covered health care providers, health plans and clearinghouses that process insurance claims, as well as the implementation of a new standard for determining whether data breaches need to be reported.

“This is a paradigm shift in the privacy world, and definitely something for all businesses to pay attention to,” Hunton & Williams LLP's global privacy and data security practice head Lisa Sotto told Law360 on Tuesday. “These obligations being pushed onto every subcontractor is extraordinary, and I can’t think of any other privacy law, at least in the U.S., that does this.”

The bulk of the new regulations, which were required in order to implement certain provisions of the Health Information Technology for Economic and Clinical Health Act of 2009, were outlined in a proposed rule issued in July 2010, but delays stalled the issuance of the final, binding rule. Still, many businesses are unprepared for the sweeping changes, attorneys say.

“While the expansion of the rule is not a surprise, a lot of organizations haven’t fully gotten under way in their compliance efforts,” Morgan Lewis & Bockius LLP partner W. Reece Hirsch said. “But now that the starting gun has sounded, it’s a race to get ready by the Sept. 23 compliance deadline.”

Although fully complying with the rule will require an extensive reassessment of data security and privacy practices, attorneys recommend that companies start by updating their vendor contracts and data breach risk-assessment plans.

“Business associates will need to improve their security practices and documentation significantly, ... revise their contracts with their clients and with their downstream contractors and ... ensure they are meeting all of the new and old HIPAA requirements,” Wiley Rein LLP partner Kirk Nahra said. “They also will need to make sure that, in the event of any kind of security breach, they are meeting all of the requirements of the newly revised and tougher notification rules.”

In a somewhat surprising departure from the draft regulations, the regulator replaced the current requirement that notification of a data breach is only triggered when there is a significant risk of harm to individuals, instead obligating companies to report all breaches unless they can demonstrate a low probability that protected health care information has been compromised.

“The previous focus was on harm to the individual, but now the focus is on the violation of the rule and the probability of personal health information being compromised,” Sotto said. “The general shift in privacy law in the last few years has been to go to a harm threshold that revolves around risk of harm to an individual, and this is more bureaucratic and pulling back from this trend.”

The Office of Civil Rights said in its final rule that the change was prompted by commenters who “expressed concern that the risk-assessment focus on ‘harm to an individual’ in the interim final rule was too subjective and would lead to inconsistent interpretations and results across covered entities and business associates.”

To help covered entities more uniformly interpret the new requirement, the regulators provided four factors that should be considered when determining if a covered data breach has occurred: the nature and extent of the protected health information involved, to whom the disclosure was made, whether the protected health information was actually viewed and the extent to which the risk has been mitigated.

But despite this attempt at clarity, attorneys worry that the list leaves unanswered questions that will result in inconsistent interpretations and overreporting.

“I would much prefer some more black-and-white rules that say, 'If you can show me this and this, you don’t have a breach,' because otherwise, you’re just betting that you were right,” Foley Hoag LLP security and privacy practice co-chair Colin Zick said. “A lot of state rules for breach issues have that kind of clarity, but here it seemed like the waters are muddied in order to make sure that people are reporting when in doubt.”

Besides overhauling their data breach response plans to meet these new reporting obligations, companies will also need to revisit their agreements with previously uncovered third-party contractors, attorneys noted.

The revamped agreements will include provisions that reflect the new data-security obligations that business associates will need to undertake, many of which go beyond general security standards. These include hiring a security compliance officer, instituting comprehensive training, and putting in place new data retention and destruction requirements.

“Business associates — generally, vendors serving health plans, hospitals and many other health care providers — may have a lot of work to do to come into compliance,”Akin Gump Strauss Hauer & Feld LLP senior counsel Jo-Ellyn Sakowitz Klein said. “Previously, their liability was limited to the four corners of their business associate agreements. Once the compliance date for the new ... rule arrives, they will need to answer directly to governmental authorities enforcing HIPAA, as well as to their contracting partners.”

While business associates that operate exclusively or primarily in the health care space should have an easier time transitioning, the regulation also draws in subcontractors that could include cloud providers that may not even be aware that they are storing protected health information, making compliance with the rule more difficult, attorneys noted.

“Some entities may be surprised to realize that they are business associates,” Holland & Knight LLP data privacy and security team co-chair Shannon Hartsfield Salimone said. “The preamble indicates that an entity such as a document storage company that ‘maintains’ this information on behalf of a covered entity is a business associate, even if the entity does not actually view the protected health information."

Meanwhile, Rep. Ed Markey, D-Mass., on Friday raised the possibility that further revisions to the rule might be on the horizon, noting, “Areas for improvement remain — particularly when it comes to the sale of protected health information without a patient’s informed consent.” But attorneys are skeptical that companies will have to worry about another major change anytime in the near future.

“The newest rule is a major update to HIPAA,” Hirsch said. “While there will most likely be future tweaks, I think that the landscape is much more settled now, so any subsequent changes will be much more around the edges.”

--Editing by Elizabeth Bowen and Chris Yates.