Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Growing HIPAA Focus Leads To Fresh Compliance Options

By **Allison Grande**

Law360, New York (February 27, 2017, 4:17 PM EST) -- Health care providers and their business associates are increasingly looking for more streamlined and less costly options for charting compliance with federal health privacy law as regulators become more focused on the law, a demand that is being filled by tools such as Day Pitney LLP's recently updated self-assessment framework.

The law firm originally launched its digital HIPAA self-assessment tool in December 2015 in anticipation of an enforcement crackdown and a looming wave of aggressive audits by the Office for Civil Rights at the U.S. Department of Health and Human Services. The revision that went live Thursday adjusted the tool's content to reflect additional audit areas added by the OCR last year, including business associate requirements and use and disclosure of genetic information.

Attorneys outside Day Pitney told Law360 that using such assessment tools to devise security plans can prove to be a strong defense against government investigations.

"In a general sense, the key is to do something to prepare," Foley Hoag LLP privacy and data security practice co-chair Colin Zick said. "Don't just wait for the knock on the door."

While other law firms and consulting companies offer services that help covered entities assess their HIPAA risk, attorneys at Day Pitney say their tool is unique because it requires no commitment to retain the firm. It also distills the technical requirements of HIPAA's privacy, security and breach notification requirements into straightforward questions that are easier for companies to tackle than trying to take on the rule in its entirety.

"Hiring outside consultants to come in and do risk assessments can be extremely expensive and time-consuming, and they identify every little thing, which can sometimes become a little overwhelming when it comes to figuring out where to start," Day Pitney health care counsel Susan Huntington told Law360. "We thought that with our tool, we would model it on areas that OCR identified as being important in their audits and allow organizations to do their own self-assessments, which is very cost-effective and helps them identify the areas they need to focus on."

The tool is not intended to be as comprehensive or act as a substitute for an external audit, but it provides a starting point that is likely to appeal particularly to smaller health care providers that may not be able to afford a more comprehensive review and to business associates that were only recently swept up by the statute and may be unfamiliar with exactly what HIPAA compliance entails.

"The important thing is that you've done an assessment. Even if it's not perfect, and the company recognizes that there are things it has to work on, that's much better than not having done one at all," Day Pitney health care counsel Eric Fader said. "Hopefully, this tool can be the first step maybe not toward being perfect, because very few organizations are at 100 percent, but of getting from 50 percent or 60 percent to 95 percent, which will be looked favorably upon by OCR if there is ever an investigation."

Demonstrating that a covered health care provider or business associate has at least begun the process of looking at the way that their privacy and data security practices comport with HIPAA is particularly important in light of moves that the OCR has made in recent years to ramp up enforcement and monitoring efforts.

"It's extremely important for both covered entities and business associates to take HIPAA seriously," Holland & Knight LLP healthcare and privacy attorney Shannon Hartsfield Salimone said. "Periodic internal audits and self-assessments are a great way for companies to try to identify areas of risk before they become huge problems."

Both seasoned HIPAA vets and relative newcomers can benefit from regular self-assessments, which help companies not only figure out where their biggest vulnerabilities may lie but also expose risks that they may have overlooked.

"What these tools give you the capability of doing is help you deal with HIPAA compliance in aggressive and effective ways," Fox Rothschild LLP partner and assistant general counsel Michael J. Kline said.

The OCR began casting a more watchful eye on HIPAA compliance in 2015, when its inspector general released a pair of reports that criticized the regulator for not being proactive enough in identifying and taking action against HIPAA offenders. The office responded by initiating two waves of audits and setting records for both the quantity and dollar amounts secured in HIPAA enforcement actions in 2016.

The regulators' actions have run the gamut, targeting violations such as late breach reporting and lax security practices, with entities ranging from the largest health care providers to small medical practices. In several recent actions, including a $2.2 million settlement announced in January with MAPFRE Life Insurance Co. of Puerto Rico over the theft of a USB data storage device, the OCR specifically faulted companies for failing to conduct risk analyses and implement risk management plans.

"The message from recent enforcement actions is that you are expected to learn from and correct mistakes," Zick said. "If you don't have an effective feedback loop, you are going to have problems with OCR."

While Day Pitney originally set up the self-assessment tool to help companies prepare for the second wave of audits — which are now already well underway, as the OCR has chosen its enforcement targets and initiated the reviews — the firm's attorneys say that the assessment mechanism also has value when it comes to reducing enforcement exposure.

Attorneys outside the firm agreed that the use of assessment tools such as those offered by various private sector entities and even the OCR was essential not just for making it through audits but also for broader compliance purposes.

"The far more likely possibility for any covered entity or business associate is some kind of breach that

leads to an investigation, and these tools are helpful in ensuring that the right materials are in place," Wiley Rein LLP privacy practice chair Kirk Nahra said.

Besides being useful in countering concerns voiced by the OCR over the lack of proper risk assessments, mechanisms such as the Day Pitney tool can also help at the state level, where regulators like the Connecticut attorney general have been more closely scrutinizing a wide range of breaches and have tended to view companies that lack risk assessments as being negligent, as well as in private litigation.

"HIPAA has sort of increasingly been recognized as a standard of care in the way health care providers deal with patients' data," Fader said. "So even though there's no private right of action under HIPAA, people can and do sue health care providers for things like negligence and breach of fiduciary duty and allege that a failure to comply with HIPAA is a strong indication that their claims are viable."

Self-assessment tools like the one recently updated by Day Pitney are likely to find wide appeal as this regulatory and legal scrutiny continues to expand.

According to the Day Pitney attorneys, hiring an outside consultant to conduct a comprehensive risk assessment could cost about $10,000. By contrast, access to the firm's self-assessment tool costs approximately the same as the price of "a fully loaded Apple laptop computer," and it comes with two hours of legal consultation.

Health care entities and their business associates could also try to cut costs by conducting their own assessments in-house. But this may be feasible for larger firms with extensive internal legal teams, and smaller companies may struggle to discern the technical requirements of the sprawling HIPAA rule.

"Companies can do a lot of self-education on the internet, but the problem with that is that they get a lot of misinformation," Troutman Sanders LLP partner Steven Gravely said. "It's a bit risky to do it alone, especially if you're new to this space, since you can be taken off in the wrong direction."

However, attorneys noted that no matter what path companies choose to get a handle on their compliance standing, just getting an assessment isn't enough; covered entities need to be ready to act on the results.

The OCR drove home this point in a recent enforcement action against Children's Medical Center of Dallas, Gravely noted. In imposing a $3.2 million fine for the hospital's alleged failure to properly protect electronic health records until after the theft of an unencrypted laptop, the regulator noted the medical center had been advised following two different security consultations to implement risk-management plans in compliance with HIPAA and to encrypt or otherwise protect electronic devices but had failed to heed the advice.

"Conducting risk assessments and creating documentation doesn't hurt you," Fox Rothschild partner and HIPAA privacy officer Elizabeth Litten said, "unless you ignore and don't take action on the evidence in front of you."

--Editing by Christine Chun and Catherine Sum.