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

Health Cybersecurity Guide Could Redefine 'Reasonable'

By **Allison Grande**

Law360 (January 3, 2019, 10:11 PM EST) -- Voluntary health care cybersecurity standards recently unveiled by the U.S. Department of Health and Human Services are likely to unofficially set a new "reasonable security" standard that could help fuel both private litigation and more formal policymaking efforts, attorneys say.

HHS used the waning days of 2018 to drop a new four-volume publication aimed at providing voluntary cybersecurity practices to health care organizations of all types and sizes. The guide, which was released on Dec. 28 and produced in collaboration with the private sector, lays out the top five cyberthreats facing the industry, offers 10 practices to help reduce these risks, and urges all industry stakeholders to immediately take protective and preventive measures to boost their cybersecurity game.

Attorneys who advise health care clients on these topics predicted that industry players would find the new guidance to be a useful roadmap for addressing growing cyber risks within the industry. But they were quick to caution that, while the proposed standards may be voluntary, they didn't come without some liability risks.

"A document like this provides one more step toward defining and creating a consensus around what constitutes 'reasonable security' in the health care space," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP. "That kind of thing can be taken into account by not only policymakers but also the courts."

While companies can't be held directly liable for not taking the new voluntary guidelines to heart, privacy and data security lawsuits regularly hinge on negligence-related theories, and the new guidance is likely to give plaintiffs' attorneys additional ammunition to allege that an organization failed to act reasonably when it came to protecting the sensitive health information with which it was entrusted, attorneys noted.

"Certainly if something goes wrong, a lawyer bringing a lawsuit is going to look at the voluntary standards and see if they've been met, and then make allegations related to that," Mayer Brown LLP partner Marcus Christian said. "That commonly happens, particularly when those voluntary standards are aligned and consistent with best practices."

Health care companies are also likely to face backlash from regulators — including HHS' Office for Civil Rights and the U.S. Food and Drug Administration, which regulates medical device makers — if they fail

to make an effort to review and implement the voluntary best practices, according to attorneys.

"As these security expectations are put out there in the public domain, even though they're not law, all tides rise and the standard of care elevates," Bradley Arant Boult Cummings LLP partner Amy Leopard said. "And as you push the standard of care up, it becomes the waterline for everyone."

With OCR becoming increasingly active in pursuing alleged violations of the Health Insurance Portability and Accountability Act's privacy and security rules, attorneys said it wouldn't be difficult to envision a scenario where a company that falls under the regulator's scrutiny faces additional heat for making no effort to implement any of the suggested best practices.

"This type of guidance makes it tougher for health care organizations to plead ignorance about their knowledge of the cybersecurity practices that are available to them," Saul Ewing Arnstein & Lehr LLP partner Karilynn Bayus said.

Policymaking also could be influenced by the new guidelines, attorneys say.

OCR put out a request for information in December seeking public input on how the HIPAA could be modified, with a particular emphasis on making improvements to the HIPAA privacy rule, and there is growing momentum in Congress to harmonize the current broad patchwork of privacy and security requirements across the U.S.

"Hopefully the next phase of policymaking will be to harmonize some of this complexity, and this guidance could prove to be helpful by focusing on what security measures are most important and prioritizing resources," Leopard said.

Even if the guidance ends up carrying very little risk, attorneys still anticipate that health care companies of all sizes will come to view the document as a valuable resource for establishing adequate data security.

"I see this as a belated holiday present to the health care sector," Holland & Knight LLP partner Shannon Hartsfield said. "Instead of issuing brand new rules, from what I've seen, these documents provide useful, easy to read guidance and suggestions for examining an organization's cybersecurity practices."

However, the recommendations will ultimately only be useful to the point that companies put in the effort to take necessary steps such as paying attention to their activities, monitoring their systems, analyzing their own weak spots, and staying on top of business and technological developments, Wiley Reinprivacy and cybersecurity practice chair Kirk Nahra said.

"The issues in this area often aren't driven by a lack of knowledge — they are driven by a lack of resources and attention," Nahra said. "Raising awareness of these issues and how best to combat them is important. Making it easier to understand the risks and options is important. But there is no substitute for companies digging in and paying attention to these concerns and then creating thoughtful approaches to mitigating risks in their own business operations."

The guidance is likely to be appealing to companies for several reasons aside from the potential to reduce liability risks with compliance, attorneys noted.

"One interesting feature of this HHS publication is that it doesn't attempt to rewrite existing standards

or create new ones, but builds on existing effective principles and practices for which there is a consensus within the health care industry," Tucker Ellis LLP counsel William Berglund said. "This should help increase the likelihood that organizations will adopt the principles in the report."

The way that the report was put together with input from over 150 cybersecurity and health care experts across the public and private sectors; its acknowledgment that security plans should be tailored an organization's size, complexity and resources; and the growing sophistication and prevalence of cyberthreats should also bolster the guidance's appeal to health care companies, attorneys say.

"This document is a helpful starting point for organizations to look at their own cybersecurity policies and protections and look at the gaps that need to be addressed," Saul Ewing partner Bruce Armon said. "And it serves as a reminder that at least from the federal government's perspective, they're aware of the cybersecurity risks that health care companies face and are providing them with an opportunity to take these issues seriously."

--Editing by Emily Kokoll and Breda Lund.