COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 29, Number 1. January 13, 2020
Outlook 2020: Integrity Rule, Inpatient Audits Will Stir Things Up; Privacy Is 'Huge Focus'

By Nina Youngstrom

When an attorney at UofL Health in Kentucky was tricked by a phishing email, he called the compliance officer to report himself as "an idiot." Fortunately, it was only a test—a fake phishing email the health system sends out randomly to test employees' ability to resist the insidious attempts by hackers to access computer networks.

"I thought it was funny, but appreciated the fact that he knew he was duped and he took it seriously," says Shelly Denham, senior vice president of compliance, risk and audit services at UofL Health. "I think he truly learned a valuable lesson from that exercise." Even when they're attuned to phishing, people may click on the links, another reason why phishing, ransomware, cybersecurity and data privacy are very high on the risk list at UofL and other health care organizations. "It will be a huge focus this year," Denham says.

Welcome to 2020, the year that may be a turning point for data privacy and security. For starters, new state laws take effect in California and New York state and apply both to companies in those states and that have consumers there, while the HHS Office for Civil Rights (OCR) pushes ahead with its Right-of-Access Initiative.[1] "I think there will be a culture shift in the way people view their data," says attorney Jami Vibbert, with Venable in New York City. "You might see an uptick in individuals seeking to exercise individual rights, which may or may not happen under the California Consumer Privacy Act (CCPA),[2] but might happen under HIPAA."

That's just one inflection point for compliance and enforcement. There are other developments that will test health care organizations, including a regulation that went into effect Jan. 1 on patient discharge planning and a program integrity rule that will be phased in. Others that go live next year—on Medicare documentation and price transparency—require compliance preparation this year, compliance experts say. Meanwhile, Medicare beneficiaries continue to flock to Medicare Advantage, which worries physician advisers because they say more arbitrary denials will follow. Compliance experts predict a resurgence this year of audits of short stays and other areas with high error rates on the 2019 Medicare fee-for-service improper payment rate report. Enforcement of the False Claims Act will continue, powered by whistleblowers, but there will be some ripple effects because of the Supreme Court decision in *Azar v. Allina Health Services, et al.*[3] and the interplay between the Granston memo [4] and the Supreme Court decision in *Universal Health Services vs. United States ex rel. Escobar*[5] in 2016.

As compliance officers juggle competing priorities, they may get more support from board members. Two 2019 decisions from the Delaware Chancery Court expanded the seminal 1996 decision *In re Caremark*,[6] which was one of the first cases to recognize that boards must make a good-faith effort to implement an oversight system and monitor it, says attorney Paula Sanders, with Post & Schell in Harrisburg, Pennsylvania. The new decisions, about Clovis Oncology and Blue Bell Creameries, "expanded the expectations of boards of directors in the context of having an effective compliance program," she explains. They should be a wake-up call for board members who are still cavalier about compliance and reinforce their duty to examine the effectiveness of the compliance program. That includes asking senior leaders whether the information they get from managers is reliable and addresses the company's risks, Sanders says. As the decision in the Clovis Oncology derivative litigation[7] states,

"When a company operates in an environment where externally imposed regulations govern its 'mission critical' operations, the board's oversight function must be more rigorously exercised."

Privacy, Security Conversations Are Shifting

With the grave threats posed by hackers, cybersecurity is finally moving from an IT-focused conversation to an enterprise business risk conversation, says Brian Selfridge, a partner in Meditology Services. That's a recognition that security breaches have consequences beyond HIPAA fines, he says. For example, in October, DCH Health System in Alabama temporarily diverted all but the most critical hospital patients, reportedly for about 10 days, after it was a victim of a ransomware attack through phishing. The cybercriminals "disrupted access to computer systems at DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center," DCH said on its website. In response, four patients filed a class-action lawsuit[8] against DCH on Dec. 23, alleging because of the ransomware attack, which locked down their medical records, plaintiffs and the class members had "to forego medical care" and their private information "is in the hands of data thieves."

Ransomware is also evolving. While hackers usually hold data hostage and release it when they get paid, they're now "threatening to release the data publicly," Selfridge says. Health care organizations are particularly vulnerable to hackers "because data is going in a lot more places than ever before," including medical devices and platforms, document archiving and imaging, and cloud-hosted clinical and business support applications. There's more they can do to protect themselves, including patching and segmenting devices. "That way, when we get a ransom of a device, it may not affect our critical systems," he says.

Companies may rise to the occasion this year, partly to comply with new state laws, including in California, where the CCPA took effect Jan. 1, and in New York, where the Stop Hacks and Improve Electronic Data Security (Shield) Act[9] takes effect in March. CCPA is a data privacy and security law, with new rights for people to delete their personal information and opt out of data selling, and requirements for companies to disclose the data they're collecting and implement a security risk mitigation program. The Shield Act requires businesses to implement a data security program and expands the definition of personal information to include health information.