COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 10. October 14, 2021 Severino: Protecting ePHI Starts With Properly Conducted Risk Analysis

By Jane Anderson

Guarding electronic protected health information (ePHI) under HIPAA begins with a proper risk analysis, and most settlements issued by the HHS Office for Civil Rights (OCR) involve missing or inadequate risk analysis or risk management.

That's the word from Bob Chaput, executive chairman and founder of the security firm Clearwater, and Roger Severino, former director of OCR and current senior fellow at the Ethics and Public Policy Center, who spoke Sept. 30 at a Clearwater-sponsored webinar focusing on what OCR wants in risk analysis.[1]

According to data compiled by Clearwater, 89% of the 62 ePHI-related cases that resulted in fines from OCR were due to a failure to conduct a quality risk analysis, Chaput said. "When ePHI is involved, the security rule applies, and therefore, with the security rule applying, risk analysis and risk management implementation specifications are examined by OCR," Chaput explained. "The 89% basically represents that 55 of those 62 organizations in the ePHI cases had adverse findings."

Out of the 48 OCR settlements and civil monetary penalties that occurred during Severino's tenure, 26 involved ePHI events, Chaput said. A total of 85% of the corrective action plans included in the settlements of these incidents required risk analysis, and 73% of the CAPs required organizations to implement risk management plans and processes, the Clearwater analysis found.

In addition, nearly 90% of the settlement funds collected during Severino's tenure as OCR director—$56.2 million out of $63.5 million total—was related to risk analysis and risk management events, Chaput said.

After a Breach, 'Work Backwards'

Severino said protecting ePHI begins with risk analysis and risk management. "Think about the logic of it," he explained. "If you have a major breach or a major impermissible disclosure, it's often the case that an error happened at the front end. It could have been predicted and spotted, and mitigating strategies could have been put in place that would have prevented it. And that's how we actually approached all of our enforcement cases. So we work backwards. If there was actual harm, an actual impermissible disclosure, what could have prevented it?"

There's also a question of whether an organization faces a higher level of culpability, he said: "How much knowledge was there of their obligation and of the level of risk? If you turn a blind eye towards the risk, you have a higher likelihood of being in the willful neglect [penalty tier], and doing a proper risk analysis and risk management plan will help you stay away from those higher tiers. We want people to take the steps to dig through and find out what the levels of risk are. The last thing an enforcer wants to do is punish people for becoming aware and learning what the problems are, but learning what the problems are is the first step, and then taking the proper actions is the second step. And that's what will help you avoid some of the larger penalties."

When presented with CAPs, entities typically said that the focus on risk analysis and risk management made

sense, Severino said. "This is something where I hope entities are able to learn from the mistakes of others," he added. "It's something where we should be able to get to the point where the industry is moving beyond the large penalties and actually are responding to the threats as they evolve."