

Report on Medicare Compliance Volume 31, Number 21. June 13, 2022 COVID-19, Active Shooters Raise the Stakes for ERM; It's 'a Marathon, Not a Sprint'

By Nina Youngstrom

When a man shot his sister at Wayne UNC Health Care in Goldsboro, North Carolina, on June 6, it was an up-close-and-personal reminder why UNC is including workplace violence on the list of risks for its nascent enterprise risk management (ERM) process. The incident happened only days after a patient killed his surgeon at St. Francis Hospital in Tulsa, Oklahoma.

Active shooters and COVID-19 are two threats that underscore the importance of ERM. “Look at what we have been dealing with the past two and a half years,” said Patrick Kennedy, executive director of hospital compliance at UNC. “You are basically shuttering a large portion of your business because of the pandemic.” Add cyberattacks, general economic unrest, uneasiness in many communities, and active shooters, and “that’s the backdrop” for ERM, which is a systematic method for identifying and addressing issues “before they compromise the business and keep us from doing what we are there to do, which is to provide patient care,” Kennedy said.

The COVID-19 pandemic may have been a turning point for ERM. The public health emergency really brought attention to ERM, said Gerry Zack, president of the Society of Corporate Compliance and Ethics & Health Care Compliance Association. “COVID, in a strange way, shined a light on the need to think broadly about risks that haven’t occurred yet, because there is a tendency for people to focus on the risks we are already experiencing,” he said. “As the rate of change accelerates and volatility increases, it is becoming apparent a more holistic approach to managing risk is essential.” There’s a delicate balance, however, because it’s impossible to mitigate every risk. “How far do you go with it? We could put on the list that we could be struck by an asteroid,” Zack said. “There’s no exact science to this.”

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)