COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 3. March 09, 2023 Are Your Workers Data Protectors or Stewards? For Best Results, Organizations Should Foster Both

By Theresa Defino

In some respects, assuring compliance with HIPAA has always been a challenge because many health care providers, particularly physicians, pride themselves on maintaining patient confidentiality—even when they aren't. Nurses, too, may feel a sense of belonging to an organization whose members all share the same commitment.

But what happens when those individuals physically leave their team and work from home, as did many who could switch to remote work during the pandemic? Would they still be good "stewards" and adhere to policies to safeguard the privacy and security of patient information? Moreover, organizations already struggle to keep their training engaging and productive. What could they do as security threats increase along with remote work to enhance compliance?

These questions puzzled Robert E. Crossler, professor of information systems at Washington State University, and David Biros, chief of information technology management at Oklahoma State University, whose wife is a nurse.

"We were talking about protection motivation theory," one focus of Crossler's research, which involves strategies such as threats, fear and surveillance to influence individuals, he told *RPP.* Biros said he "felt that his wife's experience in the health care space was different, that she ... felt like she was a part of that team, like caring for people and being part of her hospital was part of her identity," Crossler added. She embodied the stewardship theory, which calls for a personal sense of moral responsibility bolstered by support from the organization.

Crossler and Biros, who were joined by coauthor Obi Ogbanufe, an assistant professor in the University of North Texas' Department of Information Technology and Decision Sciences, launched a study to pinpoint which theory alone would work best in a primarily remote environment or whether a combination would. The title of their paper published earlier this year in *Computers & Security* gives away the conclusion: "The valued coexistence of protection motivation and stewardship in information security behaviors."[1]

The researchers presented survey participants with one of three scenarios in which an individual named Terry knowingly violates the employer's specific information security policies by downloading a "customer database" with "sensitive financial and purchase history" on a USB drive for use during travel; remaining logged into an online inventory ordering system even when not using it; and sharing a password because a coworker needs access while Terry is "away on a business trip." There were a few nuances among the scenarios, such as the size of the firm, how long Terry had worked there and job status (mid- or low-level manager).