Report on Patient Privacy Volume 24, Number 2. February 08, 2024 OCR: Organizations' Sanction Policies, Enforcement Key Part of HIPAA Compliance

By Jane Anderson

Sanction policies—when crafted appropriately and applied consistently throughout the organization—can help HIPAA-regulated entities support accountability and improve cybersecurity and data protection, the HHS Office for Civil Rights (OCR) said.

"Imposing consequences on workforce members who violate a regulated entity's policies or the HIPAA Rules can be effective in creating a culture of HIPAA compliance and improved cybersecurity," OCR said in a recent bulletin.[1] When workers know there are negative consequences to noncompliance, they become more likely to comply, OCR noted.

In addition, training workforce members on a regulated entity's sanction policy can also promote compliance and greater cybersecurity vigilance by informing workforce members in advance which "actions are prohibited and punishable," OCR explained, adding, "A sanction policy that clearly communicates a regulated entity's expectations should ensure that workforce members understand their individual compliance obligations and consequences of noncompliance."

In 2020, the Office of Information Security and HHS Health Sector Cybersecurity Coordination Center released a threat brief on the different types of social engineering that hackers use to gain access to health care information systems and data.[2] The threat brief recommended several protective measures to combat social engineering—one of which was holding every department in the organization accountable for security.