Report on Patient Privacy Volume 22, Number 5. May 05, 2022
Family Members Who Snoop: After a 'Warning,' Most-But Not All-Cease, Researchers Find

By Theresa Defino

Although estimates vary, insiders—trusted employees or other workforce members—are responsible for a large percentage of unauthorized or unallowable disclosures of protected health information (PHI). And when it comes to nosing into family members' records, the proportion is likely to be much higher.

That's what gave rise to a new study designed to test whether HIPAA and related policy infractions could be prevented, a new strategy for the health care industry that "traditionally dealt with privacy violations very reactively," according to Nick Culbertson, CEO and cofounder of Protenus Inc.

Protenus' software can "actually audit, using artificial intelligence, every access to every record every day," Culbertson said. This allows the identification of "every questionable activity," but investigating each one is too big a task. Organizations can be strategic about which incidents to explore, he added.

The idea is to "focus on the cases that matter most to us and make sure that we're building workflows to ultimately prevent those incidents from happening in the first place," he added.

Protenus, based in Baltimore, Maryland, "saw a theme throughout our customer base where customers were really focusing their time on energy on really high-risk cases, and this makes sense," Culbertson told *RPP.*

"The interesting thing that we found is that low-risk cases tend to turn into high cases over time," he said. Employees who engage in more minor infractions, such as looking at a family member's record without getting caught, grow bolder in their actions.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login