COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 4. April 30, 2018 Enhanced Review of External Access To EHRs Can Help Thwart Breaches

By HCCA Staff

When patients complain to hospitals that their privacy has been compromised, sometimes the trail of bread crumbs leads to independent physician practices, which often are granted access to the hospital's electronic health records (EHRs) for patients they share. An employee or the physicians themselves may have snooped on a hospital patient, or access may continue after an employee leaves the practice, an invitation for breaches. Without a direct way to enforce HIPAA at independent practices, some hospitals are stepping up their management and oversight of users' access to protected health information (PHI) in the hospitals' EHRs.

"Many health systems grant physician offices access to their computer systems. There is a need to ensure the physician and any office staff have a business need to have that access," says Brian Kozik, chief compliance officer at Lawrence General Hospital in Massachusetts. "We rely on the practice management to conduct HIPAA training which, in an office practice, must clearly highlight no sharing of passwords and no leaving computers logged on. All of this is out of our control."

That hasn't always gone off without a hitch. Recently, Lawrence General Hospital received a HIPAA privacy complaint about a test result, and the hospital tracked it to an independent physician practice. It turned out an employee left their computer on, and another used it to access hospital records. In response, the hospital shut down the practice's access to its EHR system, and the physician fired the employee who snuck into the records. The experience illustrated the importance of monitoring and identifying improper access by physician offices.