Product watch

Maize Analytics audit log tool

by Chris Apgar, CISSP

Information systems activity review is a fancy way of saying you need to monitor your network and your applications including who is looking at and manipulating your patient information. That can be an expensive, or even almost impossible, proposition when it comes to regular monitoring of access to patient information stored in electronic health records (EHR). Two of the well-known automated audit logging tools on the market, FairWarning and Iatric, are well outside the budget for small- to medium-sized covered entities (CE). The manual option, checking audit logs by hand, is slow and ineffective.

Enter Maize Analytics' affordable audit monitoring tool. The tool supports automated monitoring of EHR activity and identifies anomalies that could represent unauthorized access to patient records.

Automated and reliable

Maize Analytics won't replace traditional information security log monitoring tools that monitor firewalls and intrusion detection systems. However, it will automate the analysis of EHR logs in a way not supported by EHRs such as Allscripts. Manual monitoring is like looking for the proverbial needle in the haystack and is not an effective method to detect unauthorized access to EHRs.

Many EHRs require manual monitoring to check for unauthorized activities and can't detect patterns of access or determine whether an employee unecessarily accesed multiple patients' records. Therefore, audit logs may only be reviewed on a reactive basis or when it's suspected that someone inappropriately accessed a patient's medical record; however, such a policy can leave a CE open to charges of willful neglect.

In the preamble to the Omnibus Rule, HHS noted that if audit logs are maintained, it would be willful neglect if those logs are not monitored. Manual random log monitoring is not effective in detecting patterns and suspicious activity across the EHR. If unauthorized access occurs, it often goes undetected until a complaint is made or a breach occurs.

Maize Analytics provides a solution that, unlike FairWarning and Iatric, is not merely a rules-based engine. It looks for patterns and employs heuristics rather than, for example, checking if the employee has the same last name or the same address as the patient. Maize Analytics functions the way advanced anti-malware software might: detecting potential threats rather than simply identifying already known ones. Traditional rules-based software, both anti-malware and audit log monitoring, simply look for certain signatures that were previously detected and added to the software's database. But Maize Analytics' automated audit logging tool analyzes potential patterns of misbehavior as well as known patterns.

To scan for anomalies, data must be extracted from the EHR and loaded into Maize Analytics' tool. The extracted data must include medical record accesses (date, time, and patient that the employee accesses in the EHR), encounters (date and time of an event occurring in the hospital), employee information, and patient information, such as ICD-10 codes.

The analysis can be run nightly or on an ad hoc basis. A report is generated that targets anomalies that may represent unauthorized access, in contrast to a rules-based analysis, which may generate a number of false positives that require busy staff make time to investigate.

The Maize Analytics tool can be run on a single workstation, in a data center such as on a server, or even in the cloud environment. The tool can be successfully run in large, complex EHR environments or smaller environments, making it suitable for smaller CEs.

Maize Analytics is not affordable for all CEs. However, the investment can put CEs in a better position to detect unauthorized activity far sooner than waiting for a complaint to be filed by an unhappy patient, and fulfills HHS' EHR audit log monitoring requirements. More information about Maize Analytics can be found at *www.maizeanalytics.com*. ■

EDITOR'S NOTE

Apgar is president of Apgar & Associates, LLC, in Portland, Oregon. He is also a BOH editorial advisory board member. Opinions expressed are that of the author and do not represent HCPro or ACDIS. This information does not constitute legal advice. Consult legal counsel for answers to specific privacy and security questions. Email your HIPAA questions to Associate Editor Nicole Votta at *nvotta@hcpro.com*.