Timber! Lax Audit Log Monitoring Can Bring Down a Healthcare Organization

Save to myBoK

Timber! Lax Audit Log Monitoring Can Bring Down a Healthcare Organization

What's Expected by OCR, and Your Attorneys, with PHI Access Logs

By Chris Apgar, CISSP

Electronic health records (EHRs) and other health IT applications used in the healthcare industry generate a serious number of audit logs. Many healthcare providers only look at audit logs when something bad happens, like exposed snooping or a breach of protected health information (PHI). If audit logs are only reviewed when a suspected privacy or security incident occurs, you really don't know what other suspicious activity is going on and going unreported. That's why it's wise to implement processes to monitor audit logs proactively so you can address potential threats or unauthorized access to PHI before it becomes a headline and the regulators show up on your doorstep.

No Log Review Equals 'Willful Neglect'

In the preamble to the HIPAA Omnibus Rule of 2013, the US Department of Health and Human Services (HHS) offered its opinion on audit logs and how it intends to enforce audit log reviews. HHS noted that if you're generating audit logs and you don't review them, that will be considered "willful neglect." Oftentimes the lack of audit log monitoring on a proactive basis is discovered by the HHS Office for Civil Rights (OCR) after a breach is reported to the agency. OCR investigates all breaches involving 500 individuals or more, and investigates some smaller breaches, usually when smaller breaches are reported multiple times by a single covered entity (CE). By then it's too late to address log reviews and that may lead to a finding of willful neglect. A finding of willful neglect can get very expensive very quickly.

Last year, Memorial Healthcare System (MHS) paid OCR $5.5 million to settle potential violations of the HIPAA Privacy and Security Rules and agreed to implement a robust corrective action plan.[1] The monetary settlement should be enough to wake up all healthcare providers. That's not the only expense, though. A "robust corrective action plan" often involves bringing in a third-party vendor to assist with compliance efforts and a requirement to prove to OCR that steps have been taken to address the deficiencies discovered during its investigation. Corrective action plans are formal and often require a significant expenditure in dollars and staff time to address any deficiencies noted, as well as report these changes to OCR.

MHS reported to OCR that a breach of PHI occurred impacting 115,143 individuals. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI without detection from April 2011 to April 2012, affecting 80,000 individuals, according to HHS.[1] Although it had workforce access policies and procedures in place, one of the primary reasons for the monetary settlement was because MHS failed to regularly review records of information system activity on applications that maintain ePHI—despite having identified this risk during several risk analyses conducted by MHS from 2007 to 2012.

OCR indicated in its press release on the incident that, "As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen." The MHS resolution agreement and corrective action plan can be found at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial.[3]

Automating Audit Log Monitoring Ideal

As the above example shows, it is well worth the upfront investment to monitor audit logs on a regular basis. Not only are there regulatory implications for not reviewing audit logs, there are also legal implications. For example, in the event a covered entity is sued and a discovery request is made that includes all audit logs generated by the EHR, the opposing counsel could find suspicious event evidence in the provided audit logs that lends credence to the opposing party's case. If the lawsuit was in relation to a breach of PHI, it can be argued that the reason the organization did not discover the breach sooner—and before any alleged harm occurred to the plaintiff—was because they did not regularly review audit logs.

Sorting through audit logs can be daunting, and sometimes virtually impossible if you are attempting to review the logs manually. It would be difficult to find anomalies that could be an indication that PHI is being accessed by an unauthorized individual. It is far better to acquire an automated audit logging tool to do the job for you and send alerts when suspicious activity occurs. As an example, if an employee usually accesses 15 charts a day and suddenly the employee is accessing 500 charts a day, that should be a red flag that bears investigating. This red flag would likely be detected by audit monitoring tools.

There are two different types of audit monitoring tools that need to be assessed and, where feasible, acquired and rolled out. One falls into the category of what is called a security incident and event management (SIEM) solution to monitor network activity and detect potential intrusions. SIEM solutions are generally supported by and fed logs by firewalls and intrusion detection or prevention tools. The SIEM solutions aggregate all of the log files, analyze them, and then send alerts as appropriate so suspected security incidents can be investigated. When alerts are sent and incidents investigated often, then CEs and business associates (BAs) can address the identified risks before a breach occurs or network penetration does any damage.

SIEM solutions are valuable in this day and age where cybercrime continues to rise. It really doesn't matter the size of the CE or BA—the bad guys are out to get you. It's a good idea to implement protections to reduce risk and the potential for patients' PHI to be exposed to cybercriminals. SIEM solutions come in a variety of levels of sophistication and varying price tags. Organizations should assess their network environment to make sure, first, that they've deployed firewalls and an intrusion detection or prevention solution that can feed the data to a SIEM. After that, it's a matter of evaluating SIEM solutions and picking one that matches an organization's security needs and budget.

Most healthcare providers have implemented an EHR and, unfortunately, SIEMs generally won't monitor audit logs for EHRs. A separate tool is needed to monitor EHR logs and send alerts to the right person if an anomaly is detected. Using this tool would allow organizations the ability to review audit logs on a proactive basis. There are a few sound solutions on the market that can help small to large CEs actively monitor audit logs. More often than not, the tool selection will be governed by how much money an organization has available to spend. Solutions range in cost from a few thousand dollars a year up to over $100,000 per year.

Examples of Audit Log Monitoring Vendors

Two audit log monitoring vendors that are worth evaluating (if you have the budget) are FairWarning and Iatric Systems. Both are decent tools and will support identifying problems before they can harm an organization or its patients. A downside is that the cost of these tools is not within the budget of most small- to medium-sized CEs. The annual subscription generally runs between $75,000 and $100,000 per year. For smaller organizations with less financial resources there are at least two other tools that are worth evaluating. The first is Maize Analytics, which costs approximately $35,000 per year. The other is Spher, which is priced by the number of providers and starts at $100 per month per provider. All four of these vendors' tools are offered on a subscription basis. As illustrated by the above range of options, the excuse for not proactively monitoring audit logs is dwindling. Meanwhile, the outcome of not monitoring audit logs becomes very expensive very quickly through the cost of crime, fines, and damage to one's reputation.

Regular review of audit logs is not just done to satisfy the regulators and the lawyers. It helps protect an organization from attack internally and externally, and protects patients' privacy. Unauthorized access comes in a number of forms—ranging from curious staff looking at the charts of VIP patients to attacks on the scale of the recent massive Equifax and Anthem breaches. A SIEM is a good tool to protect against cybercrime and, to some extent, unauthorized changes to an organization's network infrastructure. When properly configured, SIEM tools will alert users to suspicious activity when it happens, giving them the opportunity to investigate and mitigate any risk.

One of the challenges when first rolling out a SIEM and the tools that feed the SIEM, such as firewalls and intrusion detection or prevention tools, is that these tools need to be tuned. If they are not properly tuned, an organization will get a fair number of false positive alerts and conduct investigations that are unnecessary. It usually takes a bit of time to install and tune these tools, though the extra work is worth it in the long run. Following tuning, providers can assume the threats they are alerted to by the system are real and need to be investigated.

On the EHR side of the equation, automated monitoring of EHR logs goes a long way to detect what are often internal threats, such as snooping. It's better to have a tool send you an alert than an irate patient calling you because someone was snooping in their chart or stole their medical identity. Healthcare providers need to be prepared to protect patients from unauthorized access to their charts and, at the same time, protect their own reputation. Many patients will change healthcare providers if they don't trust their ability to protect PHI.

During a conversation with one of the vendors listed in this article, the vendor said that in a recent rollout of an EHR monitoring tool for a large healthcare delivery system their product turned up 1,500 instances of snooping after it was first installed and activated. While this may include a number of false positives, it illustrates how providers will not really know that bad things are happening unless they look. The purpose of audit log monitoring is to better protect an organization and its patients from the increasing risks associated with internal threats and cybercrime. Audit log monitoring also helps keep providers out of trouble with OCR if a breach does occur—allowing the provider to prove regular audit log monitoring is taking place.

Monitoring Pays Off

Yes, a provider can manually review audit logs. But this practice generally won't be able to detect many incidents due to the sheer volume of audit logs. Now that the price of EHR audit monitoring tools has come down, there is little excuse to not invest in a solution that will identify threats that can damage your network, result in a breach of PHI, and harm your organization and its patients.

Notes

1. Department of Health and Human Services. "$5.5 million HIPAA settlement shines light on the importance of audit controls." Press release. February 16, 2017. www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html.
2. Ibid.
3. Ibid.

Chris Apgar (capgar@apgarandassoc.com) is CEO and president of Apgar and Associates, LLC.