Reporting Security Incidents

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CPHS, FHIMSS

HIPAA requires covered entities "implement policies and procedures to address security incidents." There is one implementation specification: to "identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes."

According to the security rule definitions, a security incident is an "attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interface with system operations in an information system." This definition is very broad and inclusive. In fact, it is so broad that many healthcare organizations are having difficulty determining what a security incident is and how it should be reported. This is particularly important when implementing the security provisions for business associates who must report security incidents to the covered entity. Consider that a business associate does not have sophisticated intrusion prevention or even detection systems, but perhaps just a firewall. Is a "ping" on the network considered a reportable incident? (Hopefully not!)

Three basic steps will help you implement effective and efficient security incident reporting:

1. **Clearly define "security incident" for your organization.** The definition in the security rule is a starting point. You must create a workable definition for your organization that is supportive of the definition in the security rule but also workable in communicating to your work force what a security incident is so that they can identify it and report it when it occurs. Organizations may find it useful to distinguish between "security events" and "security incidents," where events are poor practices that have not led to specific harm and incidents involve harm or significant risk of harm.
2. **Institute mechanisms to collect and document all security incidents** through the reporting mechanisms used in your organization. All security incidents should be reported directly or indirectly to one identified source. This may require some changes in the way your present reporting operations occur. Frequently, IT does the bulk of security incident reporting. But physical security services may also log physical security incidents that never are brought together with the IT incidents or compared with privacy breaches.
3. **Respond to the reported security incidents appropriately.** In some cases, it is very important to respond quickly. When responding, it may be necessary to preserve evidence of an attack. For instance, if the security incident is a malicious software attack, then it is important to contain the scope of attack as soon as possible so that that the extent of damage to information systems and electronic protected health information (ePHI) is minimized and the cost to repair the damage is limited. In other cases, the response can be performed quickly with few resources. For instance, if a terminated staff member is found to be accessing ePHI with his or her user ID and password, the help desk should be able to shut off access with that identifier and password immediately, either directly or with communication to the technical support person authorized to terminate access.

Examples of Security Events

- Shared log on
- Password reminder visible at workstation
- Monitor left logged on and unattended
- System access to patient data down with only
- Unencrypted or otherwise unsecured e-mail of protected health information (PHI)
- Maintenance personnel fixing equipment with PHI without supervision by your work force

Examples of Security Incidents

- Someone impersonating an IT technician asking for a password
- Former employee using old ID and password to access electronic PHI (ePHI)
- Virus attack that destroyed current files
- Audit trail with evidence that someone misused someone else's password
- Corrupt back-up tapes with no ability to restore archived data
- Physical break-in with ePHI copied or stolen
- PHI posted on the Internet from a Web portal
- Misdirected e-mail with ePHI
- Terminated employee keeping copies of records with PHI
- CDs including ePHI found discarded without physical destruction

The security incident requirement is designed to help you respond to incidents as they occur and provide evidence in the event of further investigation. The requirement can also help you analyze the security incidents in your organization so that you can perform periodic technical and nontechnical evaluations of your security approach (as required for the evaluation standard). This helps support continual monitoring of your security risk.

The security incident report provides a profile of how risk is changing for your organization. By monitoring attempted and successful incidents, you will be able to detect changes over time by the type of threat and rate of incidents facing your organization. This information can be very valuable in adjusting your risk analysis as the incidents of specific types of threats change, as well as change your interpretation of vulnerabilities based on the success, or lack thereof, of the controls that you put in place compared with the changing environment.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Reporting Security Incidents." *Journal of AHIMA* 76, no.3 (March 2005): 60.