U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

November 2017

Insider Threats and Termination Procedures

Data breaches caused by current and former workforce members are a recurring issue across many industries, including the healthcare industry. Effective identity and access management (IAM) policies and controls are essential to reduce the risks posed by these types of insider threats. IAM can include many processes, but most commonly would include the processes by which appropriate access to data is granted, and eventually terminated, by creating and managing user accounts. Making sure that user accounts are terminated, so that former workforce members don't have access to data, is one important way IAM can help reduce risks posed by insider threats.

Your Employee Just Quit!

When an employee or other workforce member leaves, it is extremely important that covered entities and business associates prevent unauthorized access to protected health information (PHI) by ensuring that the former workforce member's access to PHI is effectively terminated. Also make sure that mobile devices like laptops and smartphones are returned, and if the use of ePHI on personally-owned phones or other devices is permitted, that those devices are cleared or purged of ePHI. In addition to addressing the risks associated with the potential unauthorized access of ePHI by former workforce members, effective termination procedures also reduce the risk that inactive user accounts (for example, user accounts that are not being used or are inactive, but are not fully terminated or disabled) could be used by a current or former workforce member with evil motives to get access to ePHI.

Time to Exit the Building!

Procedures to terminate access to ePHI should also include termination of physical access to facilities. Procedures to terminate physical access could include changing combination locks and security codes, removing users from access lists, and ensuring the return of keys, tokens, keycards, ID badges, and other physical items that could permit access to secure areas with ePHI.

Tips to prevent unauthorized access to PHI by former workplace members:

- Have standard procedures of all action items to be completed when an individual leaves – these action items could be incorporated into a checklist. These should include notification to the IT department or a specific security individual of when an individual should no longer have access to ePHI, when his duties change, he quits, or is fired.
- Consider using logs to document whenever access is granted (both physical and electronic), privileges increased, and equipment given to individuals. These logs can be used to document the termination of access and return of physical equipment.
- Consider having alerts in place to notify the proper department when an account has not been used for a specified number of days. These alerts may be helpful in identifying accounts that should be permanently terminated
- Terminate electronic and physical access as soon as possible.
- De-activate or delete user accounts, including disabling or changing user IDs and passwords.
- Have appropriate audit procedures in place. Appropriate audit and review processes confirm that procedures are actually being implemented, are effective, and that individuals are not accessing ePHI when they shouldn't or after they leave.
- Address physical access and remote access by implementing procedures to:
  - take back all devices and items permitting access to facilities (like laptops, smartphones, removable media, ID badges, keys);
  - terminate physical access (for example, change combination locks, security codes);
  - effectively clear or purge ePHI from personal devices and terminate access to ePHI from such devices if personal devices are permitted to access or store ePHI;
  - terminate remote access capabilities;
  - terminate access to remote applications, services, and websites such as accounts used to access third-party or cloud-based services.
- Change the passwords of any administrative or privileged accounts (like admin, root, sa) that a former workforce member had access to.

Resources:

- **Security Rule Paper Series: Administrative Safeguards** https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es
- **NIST 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule** http://doi.org/10.6028/NIST.SP.800-66r1