Best Cybersecurity Practices for Healthcare Organizations

Insider-Caused Data Loss

Prepared by:
Kathryn Carey and Aleksandra Vold
BakerHostetler

LORMAN®
Published on www.lorman.com - December 2019

INTRODUCING
Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 110+ live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 3,800 courses available
- ☑ **Videos** - More than 1,900 available
- ☑ **Slide Decks** - More than 3,000 available
- ☑ **White Papers** - More than 1,900 available
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Best Cybersecurity Practices for Healthcare Organizations – Insider-Caused Data Loss

Written by Aleksandra Vold and Kathryn Carey

This article is part of a series of blog posts exploring the recommendations and guidance Health & Human Services (HHS) provides to healthcare organizations in its Cybersecurity Best Practices *report. For previous articles in the series, click here.*

While any security incident may cause an entity heartburn, when the incident is traced back to an insider, the feeling turns to heartache in an instant. While there is a certain element of pity associated with a run-of-the-mill hack, admitting to patients, regulators and staff that a fox was invited into the henhouse by the entity gives an air of complicity.

Didn't you do a background check? Why weren't you closely surveilling and logging that type of staff activity? What's the bad guy's name? Did you fire the person? What else did the person have access to? How do you know everything the person accessed? Does the person have a history of violence or mental health issues? How could you have hired someone like this?!

These are the uncomfortable questions posed in the wake of an intentional insider-perpetrated incident (in addition to all the normal post-incident questions about the security measures that were in place). Accidental data loss often creates slightly less panic, but the questions still have an undercurrent of “how could you employ this person (who isn’t cautious enough to make sure the attachment/email address/fax number is correct)?” And frequently, whether intentionally or accidentally, the administrators and the public are often asking the same questions.

The report on cybersecurity best practices (Report) attributes accidental and intentional insider-caused data loss to the following:

- Files containing sensitive data accidentally emailed to incorrect or unauthorized addressees.
- Lack of adequate monitoring, tracking and auditing of access to patient information on EHR systems.
- Lack of adequate logging and auditing of access to critical technology assets, such as email and file storage.
- Lack of technical controls to monitor the emailing and uploading of sensitive data outside the organization’s network.
- Lack of physical access controls.
- Lack of training about social engineering and phishing attacks.

To help combat these issues, the Report provides some practices to consider for each entity size.

For Small, Midsize and Large Entities

Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors. For small entities, the Technical Volume suggests that staff education should include how to recognize phishing techniques, leveraging an encryption add-on within the email system to make it easier for workforce members to send information in a protected format, and stressing the importance of being "extra careful" when sending and receiving emails containing PHI. For midsize and large entities, the guidance is much more robust and delves into how to make the education as effective and sticky as possible. (See Section 1.M.D on page 18 of the Technical Volume for Medium and Large Health Care Organizations.) No matter what the entity size, evidence of these training modules and emails should be kept, as an OCR investigation will likely ask an entity to prove it was keeping up with workforce education.

For Midsize and Large Entities

Implement and use workforce access auditing of health record systems and sensitive data. At the heart of this recommendation is HIPAA's "minimum necessary" principle, which requires entities to allow access to only as much PHI as is necessary for a particular workforce member to do his or her job. This also helps shrink the potential scope of PHI that a particular user can accidentally or intentionally misuse or disclose. Importantly, access controls that effectuate the minimum necessary standard are relevant not only during user account creation. When a user changes jobs or ends his or her relationship with the covered entity, there are other triggers for evaluating and limiting or ending access to PHI.

During the access provisioning stage (at the start of employment or the beginning of a new role), the Technical Volume suggests the following:

- Identify common systems that all users will need to access and the most basic access rights required for each of those systems, and define them in organizational policies, procedures or standards. Procedures should be established to ensure consistent provisioning of basic access rights, and an automated tool may be considered to help boost accuracy and reliability.
- Establish procedures and workflows for provisioning access required to information and systems beyond the most basic needs. Entities should pay special attention to cloud-based systems and consider a two-part process that allows users to request access but requires a second individual to approve the request prior to granting access. A common approach is to designate an employee's supervisor as the approving party.

For deprovisioning, the Technical Volume recommends entities adhere to the following principles:

- Establish procedures to terminate access to user accounts, and execute them promptly at the time of termination. This too could be an automated process triggered after receiving notification of termination from the system of record (usually the HR system). Whether manual or automated, the termination should include steps to prevent active sessions (e.g., email logins on mobile phones) from remaining active after the employee leaves the organization.
- Establish an "urgent termination" process outside the normal termination procedures to be used in cases of sensitive termination, such as an involuntary termination.

- Ensure that termination procedures include both critical business systems and ancillary or auxiliary systems, particularly cloud-based systems accessible outside the entity's network, as these systems will remain accessible to the user if only system-based deprovisioning occurs.
- Build automatic timeouts for nonuse in critical systems. These timeouts can catch edge cases where deprovisioning procedures are not executed, ultimately reducing the exposure to unauthorized access.

Implement and use privileged access management tools to report access to critical technology infrastructure and systems. The Technical Volume acknowledges both the inherent weakness of password-based authentication and the fact that there is currently no alternative. That said, the Technical Volume does provide four password authentication practices for entities to consider:

- Centralized authentication: This allows an entity to manage access rights and passwords from a central location, allowing for timely deprovisioning and enterprise-wide password standards. Once hackers find a way into a system and a valid user name (neither of which are difficult given social media and search engines), they use tools to try "dictionary words" hundreds of times a second in search of the one used as a password. Entities should consider implementing the following password management policies to help thwart these brute-force, dictionary attacks: 1) Limit how frequently a user can attempt to enter his or her password. 2) Use cryptographically strong hashing and salting for password storage. 3) Use passphrases in place of passwords. Require a minimum of eight characters and permit up to 64 characters and spaces. 4) Implement dictionary-based password checking and compromised password blacklists. Prohibit users from establishing risky passwords, such as those used in previous breaches; repetitive or sequential characters; or context-specific words (such as a name of a service, username or derivatives thereof).

- Privileged account management: Entities likely have privileged administrative accounts, which gives an IT administrator god-like access to some or all systems and applications within the organization to perform tasks like provisioning, testing, software deployments and updates. The Technical Volume warns entities to provision at least two accounts to an IT administrator: one account for use completing day-to-day activities and a separate administrative account with access only to systems required by the IT administration function. This is because the use of privileged accounts during normal day-to-day business may expose these accounts to malware attacks, giving an attacker elevated access to the organization's environment. To limit this exposure, the Technical Volume suggests the following controls for managing privileged accounts: 1) Ensure that the passwords set for service accounts are large and complex (at least 32 characters, preferably 64). 2) Rotate these passwords on a defined frequency, but certainly if the password is ever compromised. 3) Escrow privileged systems' credentials, making them unique for each system or device. 4) Link privileged access to problem, change or service tickets in the organization's ticketing system. 5) Require the use of a jump server when elevating privileges, and ensure full recording and auditing of the jump server. 6) Require brokered access to a privileged account that registers which user is using the privileged account and records all actions taken. 7) Require multi-factor authentication for all privileged accounts used interactively. 8) Conduct regular reviews of privileged access. 9) Limit actions that privileged accounts can take by using access control lists. Check for the use of sensitive commands and alert the IT or Information Security department if there is misuse.

- Local application authentication: Where applications do not support a centralized authentication model, entities must maintain solid access control procedures to manage user accounts. This requires designating a responsible IT owner who will manage and regularly review these accounts to prevent continued access by an employee after he or she leaves the organization. The Technical Volume recommends the following extra controls: 1) Designate an IT owner for each legacy/cloud-based system. 2) Establish a distribution list in the organization that includes IT owners as members, and submit terminations to the distribution list as they occur. 3) Ensure that IT owners comply with standard operating procedures for the onboarding, review and, most importantly, termination of users.

- Monitor authentication attempts: Monitor both regular and privileged user accounts for security and compliance purposes.

Implement and use data loss-prevention tools to detect and block leakage of PHI and PII via email and web uploads. DLP tools can ensure that sensitive data are used in compliance with an organization's policies, detecting when defined types of information are moved in potentially policy-violating ways. For more on this issue, please see our post about loss or theft of equipment or data.

The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.