Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: Heed 10 Expert Tips To Protect Your Organization Against 'Insider Threats'

Hint: Establish a 'baseline' to spot suspicious employee behavior.

Although the thought of a nameless hacker attacking your network system may make you shake in your boots, an "insider threat" is far more common and can do just as much damage to your organization. Thankfully, however, you can take certain steps to prevent and mitigate the effects of insider threats.

What Is an Insider Threat?

"Although there has been a lot of recent publicity about external threats to the information systems of healthcare providers, covered entities need to also consider and proactively address threats from within their organization," such as their employees and contractors, healthcare counsel **Elizabeth Hodge** and partner attorney **Carolyn Metnick with Akerman LLP** tell Health Information Compliance Alert.

According to the United States Computer Emergency Readiness Team (US-CERT), a malicious insider threat is a current or former employee, contractor, or business partner who meets the following criteria:

- Has or had authorized access to an organization's network, system, or data; and
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Case in point: "As a recent example of an insider threat, the U.S. Department of Justice just announced that a former employee of a Florida hospital was recently sentenced to three years in federal prison after accessing protected health information [PHI] from more than 600 patients and using that information to file false tax returns," Hodge and Metnick illustrate. "The court records evidence that the employee had received regular training on HIPAA compliance."

Although insider threats aren't always malicious or intentional, they can be just as detrimental to your organization as an outside cyberattack or theft. US-CERT offers the following steps to protect your electronic PHI (ePHI) from insider threats:

1. Look for Threats in Enterprise-Wide Risk Assessments

You should consider threats from insiders (employees) and business associates (BAs) in your enterprise-wide risk assessments. You may identify security threats by conducting a security risk assessment or a more thorough test of system-wide vulnerabilities, Hodge and Metnick say.

Also consider your workforce's privacy knowledge, note Hodge and Metnick. "Many employees do not know how to identify socially engineered emails or other security threats. Employees should be trained on identifying socially engineered emails."

Additionally, you should avoid directly connecting with your BAs' information systems, and have employees, contractors, and BAs sign non-disclosure agreements or confidentiality agreements as necessary.

2. Clearly Document & Consistently Enforce Policies & Controls

Review and revise your security and privacy policies at least on an annual basis and whenever there is a relevant change in the law, Hodge and Metnick advise. Ensure that your employees know the location of your privacy policies and procedures (ideally, you should give them a copy) upon starting employment.

You can also raise privacy and security awareness within your organization by providing regular updates on privacy matters, including email blasts, posters, and/or in-service lunch training sessions, Hodge and Metnick suggest. Centralize information about policies and procedures and helpful links, and consider sending emails about opportunities for additional training and learning.

Key: Ultimately, management needs to cultivate and support a privacy culture and the privacy message should filter down into the workforce ranks.

"Many insider threats can be prevented when an organization makes information privacy and security part of the corporate culture," Hodge and Metnick note. "This includes demonstrating to employees that management buys into protecting the privacy and security of the organization's data. The culture of privacy and security is then reinforced through policies and procedures that are clearly and consistently communicated to the organization through ongoing training and awareness programs."

3. Raise Awareness of Insider Threats During Employee Training

Make sure you train employees to keep their eyes open and report suspicious behavior of other employees that may pose a security threat, Hodge and Metnick say. "Start privacy training upon hiring (coordinate it with other training such as records management, code of conduct, etc.)."

Next step: Then, measure and assess employees post-training to help make training more effective and to confirm employee understanding.

4. Monitor & Respond to Suspicious or Disruptive Behavior

Beginning with the hiring process, you should monitor and respond to suspicious or disruptive behavior. Start by determining a baseline of employee user behavior, and then regularly audit employee usage of systems to determine if employees are trying to access information that is outside the scope of their job, Hodge and Metnick recommend.

If you have employees who deviate from the baseline, depending on their position, you should monitor them more closely.

5. Inventory All Your Assets

Maintain a complete inventory of all electronic equipment, data systems, and applications that contain or store ePHI, Hodge and Metnick advise. Incorporate these assets into your risk analysis that examines potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Also, prioritize your assets by value to determine which assets are likely to be significant targets, Hodge and Metnick offer.

6. Implement Strict Password & Account Management Policies

You should put in place strict password and account management policies and practices. Make sure employees change their passwords regularly (every three months), Hodge and Metnick recommend. And ensure that their passwords are complex, with at least eight characters and a combination of at least one number, one symbol, and both capital and lowercase letters.

7. Enforce Separation of Duties & Least Privilege

You should tailor training to employee roles and routinely audit user access permissions at least annually, Hodge and Metnick advise. Remove permissions that are no longer needed.

8. Monitor & Control Remote Access

You should monitor and control remote access from all endpoints, including mobile devices.

"Employers should be able to remotely wipe all employer information on a mobile device upon loss, termination, or threat," Hodge and Metnick note. "Consider the pros/cons of using company-owned mobile devices versus employee-owned mobile devices."

9. Develop a Comprehensive Employee Termination Procedure

When you terminate an employee or an employee leaves the organization, make sure you remove all system access.

10. Develop a Formalized Insider Threat Program

Your formalized insider threat program should allow employees to report threats anonymously with no retaliation for reporting threats, Hodge and Metnick say.

Some other tips from US-CERT for protecting against insider threats include:

- Anticipate and manage negative issues in the work environment;
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities;
- Institute stringent access controls and monitoring policies on privileged users;
- Institutionalize system change controls;
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions;
- Implement a secure backup and recovery process;
- Establish a baseline of normal network device behavior;
- Be especially vigilant regarding social media; and
- Close the doors to unauthorized data exfiltration.

Resource: For more guidance on protecting against insider threats, go to http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017.