Codify
BY AAPC

Health Information Compliance Alert

Security Strategies: 3 Steps Help You Catch Illegal Employee Behavior

Use these pointers to sniff out your staffers' suspicious activities.

If you think your greatest risk for a security breach is on the outside of your organization, you could be leaving your patients' confidential information vulnerable to an employee's criminal intentions.

More data leaks result from employees' behaviors -- either because they failed to follow your policies and procedures or because they set out to steal your clients' data -- than from any other method. And when in-house breaches occur, they often make headline news.

You cannot wait for a major breach to uncover your staff's malicious activity. Rather, use this simple step-by-step guidance to develop an audit control process that will spot illegal behavior before it ruins your compliance efforts.

1. Define Standard Operating Procedures.

Before you can evaluate your employees' behaviors, you must define what's normal by figuring out exactly how you operate, says **Matt Johnson,** a security consultant for **AltaPacific Technology Group** in Fresno, CA.

For example, you must know how information flows into, through and out of your organization; when and to whom you will send e-mail attachments; and what behavior will be normal for each type of data-accessing employee -- clinical, technical and administrative.

2. Determine Abnormal Behaviors.

After you've thoroughly defined your standard operations, you can pin down the types of behavior that you'll consider anomalous.

Example: You may decide that no clinical employees will e-mail attachments or that technical staff should not access patients' billing information without permission.

Next: Set up your audit controls to recognize those anomalies and notify you when they occur. "Most practice management applications have the built-in ability to log and record this information," Johnson says. But you must ensure you turn on each of these controls, he stresses.

3. Consider Random Versus Specific Audits.

A policy that warns your personnel that you will audit their activities on a random basis could be the perfect deterrent to malicious behavior, experts note.

However, that practice doesn't allow your employees to develop trust in and loyalty to your organization, stresses **Greg Young,** information security officer for **Mammoth Hospital** in Mammoth Lake, CA.

"We prefer to act on suspicions because it allows us to be more specific with our audits," Young explains. Those suspicions can arise from your audit control notification system or from noncompliant behavior that comes to your attention on a day-to-day basis.

Problem: Watching all your employees all the time can be difficult. Solution: Encourage your staff members to report any behavior or actions they find questionable.

Good idea: Establish an anonymous telephone hotline or e-mail account that your staffers can use to contact you without fear of coworkers' disapproval. This could also alleviate their worry that management will rope them into an investigation, Young advises.

Keep in mind: Many of your employees' activities are better suited to random audits, notes **William Hubbartt,** health care consultant in St. Charles, IL.

Example: Your technical staff is tasked with destroying all media that your healthcare office no longer uses, such as floppy disks, on a bi-monthly basis. Rather than waiting for a problem with the destruction process to show up -- say, records surfacing in a dumpster -- you may decide to randomly audit the process every three or six months.

The Bottom Line

No matter how you set up your audit process, you must explain to your staff members what you expect from them -- and what sanctions you'll apply if they violate your policies and procedures, Johnson stresses. Discuss the audit process and its consequences in your training sessions and in any employee handbook.

By stressing your organizations' commitment to intense scrutiny of suspicious activity, you'll likely reduce the possibility that employees will violate your policies and procedures, Young points out.