Health Information Compliance Alert

SECURITY: PROVEN STRATEGIES TO ELIMINATE EMPLOYEES' PHI MISHAPS

Use this professional guidance to protect your patients' PHI from employees' mistakes

An employee's honest mistake can expose your patients' protected health information (PHI), costing your organization - and your patients - millions of dollars.
That means you must act now to decrease the chances that your employees will inadvertently (or maliciously) disclose patients' confidential information. Use this expert advice to guide your security program and keep your patients' PHI out of unauthorized users' hands.

FOCUS ON EMPLOYEE EDUCATION

Before you can expect your employees to protect patients' sensitive health information, you must make them aware of current security measures and how to use them, says **Frank Ruelas**, compliance officer at Gila River Health Care Corporation in Sacaton, AZ.

"You need to develop a sound employee education program that includes security reminders so that people are aware of their responsibility to protect the integrity of data," notes **Chris Apgar**, health care consultant and president of Portland, OR's Apgar & Associates.

What to do: Your security awareness and education campaign can consist of daily or weekly e-mail reminders, security seminars or bulletin-board displays that focus on what employees can do to protect patients' privacy.

Example: In April, you might send out e-mail messages reminding your staff members to activate and password-protect their screensavers. The month of May could be dedicated to password policy reminders.

No matter how you choose to educate and prepare your workforce members to protect the privacy and security of patients' information, you must also make them aware of the consequences of failing to do so, stresses **Barry Herrin**, an attorney with Smith Moore in Atlanta.

"Your employees need to know and understand your sanctions policy," Apgar says. That way, they will be careful to avoid inappropriately releasing patient information or damaging patient files, he adds.

But that doesn't mean you should browbeat your employees over potential mistakes, Ruelas warns. "Focus on the consequences of staffers' actions rather than how they'll be punished," he says. This semantic difference shifts the focus from placing blame on the employee to how an employee can avoid making the mistake, he says.

USE AUDITS TO UNCOVER PROBLEM AREAS

No matter how stringent your security measures or how often your security training, mistakes happen. But a mistake doesn't have to lead to a security or privacy violation. That's where your auditing and monitoring procedures come in, Apgar emphasizes.

"You have to go through your system and applications to figure out which audit capabilities will give you the best information about what activity is occurring around your PHI," Apgar explains. That way, you can see exactly how your employees are viewing or accessing your patients' information, he says.

Next step: Once you've set up your audit controls, you have to monitor the data you log. By monitoring the activity, you can not only pinpoint malicious activity, but you can spot larger trends that might be indicative of a department's training needs or an employee's misinterpretation of his job function, Herrin says.

Try this: Develop a routine process for spot-checking each employee in your organization, Herrin suggests. Make sure your checks show enough activity to determine whether the staff member is performing correctly. Example: You don't want to see just that an employee entered the wrong digit and accessed a record she didn't need. You want to know how long she remained in that record, what she did while there and how she responded to the mistake.

Warning: Don't let your surveillance override your employees' level of comfort, Ruelas cautions. "You must keep a close eye on your workforce while balancing that with their feeling that Big Brother is watching," he explains.

Spin your supervision activities in a positive light so that your personnel don't make mistakes due to fear of messing up, he says. Try it this way: Tell your staffers you are watching to identify problems that need to be looked into, not to find out what they're doing wrong.

The Bottom Line: Your staff members can be your best line of defense against a privacy or security breach. By giving them all the tools they'll need to protect your patients' information, you stand a better chance of avoiding unintentional mistakes, experts agree.