Health Information Compliance Alert

Security: IN THE HIPAA MARATHON, 'WALKING' COULD WIN THE RACE

Keep your compliance plan in shape with regular monitoring

You've spent months developing policies and procedures in order to comply with HIPAA's privacy rule deadline - so what comes next? Now is the time to begin monitoring your staff so you can knock out compliance violations before they occur. Here's how to get started:

CONDUCT A WALKTHROUGH

The Basics: Much like the safety audits your office already performs, a walkthrough can prevent violations before **HHS' Office for Civil Rights** gets involved. Whether inspections are announced or executed without your staff's knowledge, experts agree that they should be done at least annually for all departments and more often for high-risk areas. "If you've found a problem area, then you want to do [walkthroughs] more often than [once a year] to get things really ironed out," suggests **Patricia Johnston**, a consultant for **Texas Health Resources** in Arlington, TX.

Though not mandated by the privacy rule, third party or anonymous reviewers are often an efficient, if costly, method of examining your facility's HIPAA compliance program. "The big thing is making sure that nobody knows what's going to happen because you want to see what people are doing on a day-to-day basis, not what they're doing on their best behavior," posits **Robert Markette**, an attorney with Indianapolis' **Gilliland & Caudill**.

The types of violations often caught in walkthroughs range from simple mistakes - like leaving confidential faxes unattended or discussing PHI in public areas - to trickier situations that may have been overlooked. Many times the problem is not a procedural violation, but an issue that hasn't been thought through all the way, Markette says.

FOCUS ON YOUR FRONT LINES

"Focus on [areas with] a significant amount of interaction with the public or ... patients," advises **Brian Gradle**, an attorney with the D.C. office of **Hogan & Hartson**. Waiting rooms, elevators and even fax machines are all areas where information can accidentally be heard or viewed by the public, Gradle offers.

Example: In a recent walkthrough, Markette noted that though the office had obviously positioned computer monitors so that they could not be seen from the waiting room, staff members hadn't considered the glass entryway to be an area of risk. "As you walked in, you could look right over the employee's shoulder," he observed.

"Any time a privacy official is on the ground walking through, they should have their eyes and ears open," claims Gradle. However, experts agree that while privacy officials should conduct informal walkthroughs frequently, there must be some method to document and track violations, and there must be follow-ups.

To solidify the process of monitoring HIPAA compliance, Johnston developed a walkthrough checklist (see sample checklist, this issue). As a tangible record of violations, the checklist should be based on the privacy policies and procedures central to your organization. It can also include how many times the violation was obser-ved. "It gives you something to start tracking to see if you see any improvement or not," Johnston explains.

The Next Step: Once the walkthrough has been performed and the violations logged, compliance officers and others can review the document to see what went wrong and where. "The two main areas we look for are our training and the clarity of our policies," Johnson points out. If a violation is observed multiple times, you have to ascertain the causes behind it.

Some questions you should ask are shown in image in this article.

By pinning down answers to these questions, you can streamline your facility's procedures, and thereby avoid glaring HIPAA violations.

SET THE EXAMPLE

Tip: Remember to take HIPAA violations seriously, if and when they do occur. That means you'll have to outline and impose sanctions according to the gravity of the violation. Not only does failure to apply penalties jeopardize your compliance program - it's also against the law not to have a sanctions policy in place.

Following your sanctions policy will benefit you in the long run, Markette explains, as it proves to your employees the importance of maintaining privacy standards, while at the same time preventing them from using past inconsistencies to excuse or eliminate their responsibility to protect health information.

Word To The Wise: To correct the problems encountered during the walkthrough, experts concur that it is best left to the discretion of the privacy officer to determine how and when a sanction will be imposed. Usually, that officer complies with the overall HR sanctions policy; however, as the issues move in the direction of malicious and willful breaches of privacy, higher levels of sanctions - including termination - must be applied.