Health Information Compliance Alert

Security Compliance: You Can Safely Send Instant Messages --" Here's How

Think sending instant messages will shut down your systems? Think again.

Allowing your employees to use an instant messaging service is a surefire path to security disaster, right? Not necessarily. This step-by-step plan will show you how to implement instant messaging without leaving your facility vulnerable to a

security breach.

1.-Consider Your Immediate

Feedback Needs

If you're like most health care organizations, you've probably outlawed instant messaging services like those provided by AOL, Yahoo! and MSN.com. But there are some great reasons to allow staff to send instant messages (IMs), says **David**

Kirby of Kirby Information Management Consulting in Durham, NC.-

"Using IMs can improve your productivity and efficiency," Kirby says. Example: An elderly patient presents with persistent coughing and fever. Your frontline staffers send an IM to a contact person on the patients' care team explaining her

symptoms. The care team member sends an IM back requesting that the patient be sent to an exam room.

The difference: With traditional operations, your reception staff must stop working to track down and call a member of the patient's care team. With IMs, your staffers can easily manage patient flow without much disruption.

2. Select the Most Secure Option

Still, instant messaging is not bulletproof, experts caution. Important: To protect your patients' PHI, you must either use a service designed to work only within the walls of your institution or find a commercial solution that allows you to manage

security or privacy issues for medical enterprises, Kirby stresses.

That rules out almost all commercial IM services, but it does leave room for homegrown solutions. Action plan: Work with your technology team to determine if your organization would benefit from IM use and the best way to provide that service.

3.-Draft a Usage Policy

Once you've evaluated the benefits of instant messaging versus the drawbacks, you must determine how and when you'll allow staffers to use it.

Best: Use IMs for day-to-day operations. For all other message relays, such as financial or personal health information, rely on your e-mail system, suggests **Tom Walsh** with Overland Park, KS-based Tom Walsh Consulting.

Important: You should only send sensitive information through e-mail, using your e-mail system's priority feature to

reflect any urgency. For an immediate response, simply call the recipient rather than sending a message, Walsh says.

Your IM use policy must also outline who will create each staff member's IM profile, who will be allowed to use the service and how to terminate that use, Walsh notes.

4.-Audit All IMs -- or Audit None

One major wrinkle you must iron out before you begin using an IM service is how -- or if -- you'll audit the information exchanged, says **Judith Moore**, HIPAA coordinator for Adena Health System in Chillicothe, OH. Adena's decision: "We don't

permit our employees to send or receive anything through instant messaging because we can't track or audit that information," Moore explains.

Another way: You could group IMs with telephone conversations, Kirby offers. If you choose this route, you must decide between these two options:

1) You store all messages. All instant messages are stored. Designate an area on your network for these messages. Audit plan: Audit stored IMs on a regular basis just as you do other system activity. As with retained e-mails, any IMs you store

will provide an evidence trail that is subject to legal discovery.

2) You store no messages. Your facility does not retain any IMs just as it does not record phone calls. Good idea: Configure the IM service to maintain a record of who sent instant messages each day and the time each message was sent, Kirby

says.

Caution: You cannot design your IM service to keep important business information from being recorded. Therefore, if you are not storing messages, then no key business and health care information can ever be included.

The bottom line: Before you send IMs, you must be confident that you are willing to accept the inherent risks to your organization's security, Moore counsels. This plan will help you navigate those risks without sacrificing your security-rule

compliance program.