Health Information Compliance Alert

Point of Care Testing DON'T LET HANDHELD METERS WALK AWAY

Now is the time for health care providers to close the gap between their HIPAA strategy rooms and their nursing units.

There's a part of the information system at the hospital that still remains largely unnoticed by HIPAA preparers: point of care testing. This program often uses handheld meters that test and record things such as blood glucose at the patient's bedside and store electronic results. The results are later uploaded to a point of care information system and then further uploaded to the laboratory information system.

First, because the devices store PHI, they need to be secure, instructs Harry Smith, president of Timberlne Technologies. "So, hopefully, when [nurses] put in a user id, there's also a password," Smith explains.

The equipment should be locked up, as well, suggests Jill Burrington-Brown, a practice manger with the American Health Information Management Association. Point of care testing instruments that contain PHI could be "stored in the drug room when it's not being used so it's not out" where unauthorized people could access it, she offers.

There are a variety of devices available, and they have different capabilities, including a variety of lockout features, explains Marcy Anderson, director of training for Medical Automation Systems. However, password and user identification lockout features must be maintained in order to keep information secure, Anderson warns. So, when an employee terminates, the point of care coordinator needs to disable that employee's logon.

Second, you need to know how the meters transmit information to the POC information system. If any of the transmissions use the Internet, then that information needs to be encrypted, Smith asserts. How you tackle this requirement will depend on what types of devices your point of care team uses.

"Our stand on HIPAA is we do whatever the policy is for that hospital, but basically we have no problem because we're just transferring the information which is all within the hospital setting," explains Anderson.

"The biggest thing is really going to be educating the staff" on keeping PHI private, Burrington-Brown tells Eli. "The worst thing is to be sloppy," she says. All the passwords in the world will make little difference if users don't sign off from devices.