MDS Alert

MEDICAL PRIVACY: Got Electronic Health Records? Brush Up on Privacy Basics Before Your Next Survey

CMS directs surveyors to look for these 2 common privacy missteps.

The best advice for staying a step ahead of the survey? Know what the surveyors are likely to do before they arrive on the scene. And a recent survey & cert memo provides a heads up about what surveyors may target related to medical privacy involving electronic health records (EHRs).

Good and bad news: CMS doesn't expect surveyors to assess whether EHRs comply with HIPAA privacy and security rules, the memo states. But the agency does direct surveyors to focus "on how the EHR system is being used in the facility." Examples include whether facility staff members leave computer screens that display clinical record +information "unattended and readily observable and accessible by other patients/residents or visitors."

Also on surveyors' hit list:

Watch out for "documents publicly posting computer passwords." This would be evidence, the memo says, "of noncompliance with both confidentiality and medical record authentication requirements." The memo also directs surveyors to ask themselves:

"Is there evidence to support a complaint allegation that facility staff shared information obtained from an EHR with unauthorized individuals?"

Follow This Expert Advice to Shore Up Privacy

Your facility can use a number of strategies to secure computer screens, as follows, says **Jim Sheldon-Dean,** director of compliance services at Lewis Creek Systems LLC in Charlotte, Vt.

• "Use a viewing filter and/or hood that limits viewing to straight ahead," he advises.

• Set the screen saver to appear after a short time period, such as 30 seconds or a minute, requiring the mouse or keyboard action to "wake it up again," advises Sheldon-Dean.

"If the computer will be unattended, the screen saver should be set to lock access as well as blank the screen," he says.

• "Set a common corner of the screen to move the cursor to, or a common keystroke, to blank the screen." Then "train staff to use it religiously," Sheldon-Dean suggests.

• Rearrange the placement of computers to minimize viewing by people who aren't using the computer.

Take Advantage of These Training Methods

Use multiple training methods to achieve the best results, advises Sheldon-Dean. For example, have users attend group-training sessions during which you always ask them:

"What if it were your data on the screen -- what would you want" done to secure privacy? Also have computer users practice how to blank the screen a few times in front of the trainer so they will know how to do it when back at their workstations, he suggests.

Audit Regularly

"Auditing can be a simple review of who accessed which records," but you have to do it regularly, advises Sheldon-Dean. "You don't have to look at every access for every user every time you audit," but you should audit every user's activity at least annually, he says. Also audit who has accessed patients' records.

"Make sure you include a good sample of patients, including any patients of note (famous or infamous)." Then if you identify unauthorized access, keep digging until you have found the "problem users," Sheldon-Dean suggests.

Once you've done that, "follow through on your disciplinary policies and make your actions known to the other users," Sheldon-Dean advises. And "remember that even well-trained, well-intentioned users" might sometimes be unable to "resist the urge to look at records improperly" in some cases -- for example, if they have an emotional reason for doing so or an issue that involves family, friends, or themselves, he says. So "use technology to limit accesses as much as reasonably possible to help overcome human nature."

Editor's note: To access the CMS memo, which also provides instructions for ensuring surveyors have needed access to EHRs during the survey, go to www.cms.hhs.gov/SurveyCertificationGenInfo/downloads/SCLetter09_53.pdf.