Health Information Compliance Alert

Security Compliance: Train Your Staff To Respond To Password Requests

Your tech team must ask these questions before doling out users' passwords.

Your shoddy authentication procedures could allow data thieves to make off with your patients' data -- especially when providing password support to offsite employees. Provide your tech team with these pointers to ensure they properly verify all users before handing out sensitive information.

Authenticate All Remote Users

Your technology staff member may recognize a remote user's name or voice and be tempted to skip over your authentication procedures. You must impress upon all staffers the importance of verifying each and every caller before giving them any password information, says **Frank Ruelas,** director, corporate compliance with **Gila River Health System** in Sacaton, AZ.

Experts offer these field-tested examples as possible security questions for your staff members:

Question #1: Can you provide two types of identification?

"We used to ask for the last four digits of users' Social Security numbers," says **Michael Gagnon,** director of infrastructure and chief security officer at **Fletcher Allen Health Care** in Burlington, VT.

With the increased focus on security, Gagnon now assigns his users a Personal Identification Number to use instead of the Social Security number, he says. You should ask for at least two forms of identification to make it more difficult for data thieves to hack into your system.

Try these other methods of identification: Hire date, home telephone number, number of years employed or badge number.

Good idea: Note in your policy what type of ID you'll require so that remote users can be prepared with answers.

Watch out: Crooks can easily obtain employee information through social engineering, Gagnon warns. If your user produced two pieces of commonly hijacked information -- such as a Social Security number and a department telephone number -- you should request a further method of authentication.

Question #2: How many clinicians are on schedule today?

If you have any doubts about a caller's authenticity, ask them a site-specific question, Gagnon suggests.

The best question? "A tricky one, such as, 'How is Dr. O'Brien doing?' when there is no Dr. O'Brien at that site," he offers.

You can also ask about a personnel type if you know there is no need for those staffers at the site -- such as asking someone claiming to be a home user about lab techs or asking a home health worker about visiting physicians.

Question #3: What are the names of two documents you worked on yesterday?

You can also ask the caller to pinpoint a file they modified or an e-mail they sent in the past 24 hours, Ruelas advises. "It's rare that a hacker would notice these types of small details," he explains.

Call Users Back With Answers

If the remote user correctly answers your authentication questions, your tech staffer can reset her password and share the new information with her. But don't do it all in one phone call. "Contact the user through a telephone number you can verify, such as her cell phone or pager number," Ruelas recommends.

Important: Configure your system to accept the temporary password only once. Then set up a continuous loop that forces the user to create a unique, strong password that no one else knows.

The bottom line: Your offsite employees will inevitably forget their passwords or enter them incorrectly enough times to cause your system to lock down their accounts. By coaching your staffers on how to handle legitimate callers, you'll stand a better chance of weeding out any criminals trying to steal your patients' PHI.