

CYBER SECURITY GIRL STRIKES AGAIN!

SUNDAY, JANUARY 10, 2010

HIPAA Authentication Strategies

Some health care organizations have yet to take significant action to comply with the original HIPAA privacy and security rules, which were never vigorously enforced. Now that those rules have been beefed up under the American Recovery and Reinvestment Act, with increased enforcement and tougher penalties, many observers expect more hospitals, physician groups and others to gear up their data security assurance efforts.

The updated federal regulations, in fact, do not specify the security technologies providers must use. "The law says that if you don't want to have to notify the government of security breaches, then you should use new technologies to prevent breaches," Borten notes. "But I regret that the law doesn't require the use of the technologies."

Two Key Steps

Of course, the best way to comply with the privacy and security rules is to make sure only authorized individuals have access to patient information. Borten argues that all organizations should encrypt all patient data and adopt two-factor user authentication, such as a password paired with a fingerprint scanner. But she contends that many-perhaps most-organizations have yet to take either step.

And any data security effort should start with a thorough risk assessment, as required under federal law, notes Eric Nelson, privacy practice leader at the Lyndon Group, a Newport Beach, Calif.-based consulting firm.

What technologies are needed to ensure patient data is secure depends on the size of the organization, Nelson says. "A small group practice where only a few people have access to the information probably doesn't need a high-tech security solution," Nelson says. "It could be as simple as encrypting the information on the computers and installing locks on the doors. A large organization is a completely different matter."

As they ramp up efforts to implement clinical information systems, many hospitals, clinics and other provider organizations are investing in a variety of user authentication technologies to help safeguard clinical information.

These include:

- * biometric systems, such as fingerprint scanners, iris scanners or palm vein pattern detectors;
- * hardware tokens, small devices, often in the form of a key fob, that generate random passwords that then must be typed;
- * proximity badges containing chips that, when placed next to a reader, automatically confirm the user's ID;
- * phone-based authentication, which uses a clinician's telephone, cell phone, pager or PDA to help verify their identity; and
- * adaptive authentication, which uses specialized software to assess a user's risk potential and pose a series of questions based on personal information they've provided.

In many cases, providers are pairing two-factor authentication with single sign-on systems, which enable physicians, nurses and others to access all appropriate systems once they authenticate themselves.

[healthdatamanagement](#)

POSTED BY TRACY AT [10:37 AM](#) 

LABELS: [HIPAA](#)