

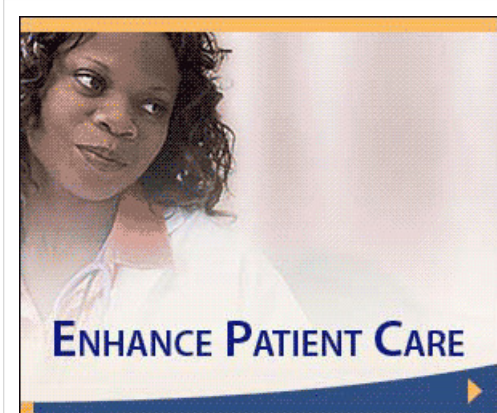
User Authentication Strategies

By Howard J. Anderson
Health Data Management Magazine, 01/01/2010

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.

"ARRA has given renewed focus on privacy and security, but many are not yet in compliance with the original HIPAA rules, much less the updated ones," says Kate Borten, president of the Marblehead (Mass.) Group, a security consulting firm.

ADVERTISEMENT



Under the updated rules, state attorneys general now have the right to enforce the HIPAA privacy and security regulations. Plus, those harmed by a security breach can seek financial damages, Borten says. "I can just see the lawyers getting ready," she says. "We are going to see a real ramping up of complaints now as a result of all the changes."

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."

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."

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.

Three-pronged Strategy

At 442-bed Southwest Washington Medical Center, Vancouver, physicians and nurses use one of three different authentication systems. Most still use a user name and password to gain access to clinical data. Many who work in critical care areas rely on fingerprint scans, while those working in other departments are phasing in use of proximity badges, says Christopher Paidhrin, security compliance officer.

All these approaches are paired with a single sign-on system that enables doctors and nurses to avoid signing on with different passwords to dozens of different clinical systems, the security officer says. The hospital uses a single sign-on system, along with the authentication technologies, from Imprivata Inc., Lexington, Mass.

When phasing in authentication technology, the hospital started by implementing about 200 fingerprint scanners in its intensive care unit, emergency department and other critical care areas where clinicians need rapid access to information, Paidhrin says.

By quickly scanning their finger, clinicians get virtually instant access to all relevant clinical information systems, he notes. "In these areas, the savings of seconds can mean the difference between life and death," Paidhrin says.

While some organizations pair a fingerprint with a password to create two-factor security, Southwest Washington skipped the password step to speed access, the security officer notes. "We use the fingerprint scanners mainly in secure areas, and we have only a very limited number of fingerprints authenticated," he notes.

But when the hospital wanted to beef up clinical information security in other departments, it decided to use a lower-cost, two-factor approach involving proximity badges, Paidhrin notes. That's because caregivers in other departments could afford to wait a few seconds to access a system, he notes. Plus, the proximity badge readers cost half as much as the fingerprint readers.

So far, the hospital has ID badge readers on about 300 of its 2,200 computers, but that amount will triple this year, Paidhrin predicts. Everyone who works at the hospital has a photo ID badge that contains a chip. They already were using the badge for such purposes as gaining access to restricted areas of the building. Now, some clinicians also can swipe the badges near a computer reader to verify their user ID, and then enter a personal identification number to access the clinical systems they're authorized to see.

The hospital rejected using hardware tokens because they feared too many users would lose the devices "People don't lose their ID badges" Paidhrin contends. The hospital also worried that users would find tokens cumbersome to use because they require typing in the new password displayed on the device.

Pragmatic Solution

Because most of its 6,000 workstations are shared by multiple users, three-hospital Duke University Health System in Durham, N.C., wanted to use two-factor authentication to supplement its single sign-on system to help guard against inappropriate access to clinical information.

After weighing fingerprint recognition, the organization went with proximity badges instead, says Karen Rourk, director of ambulatory EMR and desktop development. In tests, Duke found that the fingerprint readers had a high failure rate, she notes. In contrast, leveraging photo ID badges that everyone at the massive delivery system already wore seemed like a more practical approach.

Duke also considered and rejected another form of proximity badges that verifies identity when a user steps near a reader. These active RFID, battery-powered badges proved unreliable, Rourk says, because "if someone walked in between you and the computer, the computer thought you left the room and locked up in the middle of your work. And we had difficulties with users keeping the battery in these badges charged." So Duke, like Southwest Washington, is using passive RFID badges instead, which are not battery-powered and must be held next to the reader to work.

In the past 18 months, Duke has installed badge readers on 4,000 computers. About 10,000 of 14,000 computer users now are using proximity badges, paired with a password, to complete two-factor authentication.

Duke is using badges and single sign-on from Sentillion Inc., Andover, Mass.

"Our workstations are smart enough that if you log into one on the 7200 unit, and then go to any other within the same unit, all you have to do is touch the badge to the reader," Rourk explains. "But if you leave the unit, you have to log in again with a password."

Wider Biometric Use

While Duke and Southwest Washington are banking on proximity badges, OhioHealth in Columbus has concluded that fingerprint scanning is the best two-factor authentication technology for its eight hospitals. The delivery system has been able to achieve a 96.5% positive authentication rate using fingerprint scanners by altering the readers it uses, says Michael Krouse, CIO. Rather than using a freestanding device that requires a finger to be swiped, the hospitals now use keyboards with built-in fingerprint readers, where a user rests their finger.

The biometric authentication, paired with a password, is in use at about 70% of all hospital departments and will be phased in at all units in the months ahead, Krouse says. OhioHealth uses Imprivata's single sign-on and biometrics technology.

For about 4,600 physicians, nurses and others who access systems remotely, Ohio Health is shifting from hardware tokens to phone-based identification.

For example, those who want to access clinical systems remotely via a portal must enter a password. Then their landline telephone, cell phone, pager or PDA rings. Pressing a predetermined button stops the ringing and authenticates the user's identity. The process uses PhoneFactor software from Positive Networks Inc., Overland Park, Kan.

The phone-based system is proving far more practical than tokens because too many clinicians complained of misplacing or forgetting the small token devices when accessing data, Krouse says. "There's always a cell phone or Blackberry on their hip, while a token may or may not be with them at time that they need them," he says.

OhioHealth soon will phase out the last of its 1,000 tokens.

Tokens and Beyond

Geisinger Health System in Danville, Pa., also is phasing out its use of hardware tokens because of the expense involved and the inconvenience for users. But instead of shifting to a phone-based system, the delivery system is turning to new technology called adaptive authentication.

For several years, some 200 physicians who have been pre-approved to view and edit electronic records via a clinical portal have been using tokens, explains David Young, IT program director. The devices are from RSA, the Bedford, Mass.-based security division of EMC.

Geisinger now is in the early stages of phasing in a software-based adaptive authentication system from RSA. The software poses questions to assess clinicians attempting access of clinical systems.

Looking for 'Red Flags'

The Federal Trade Commission's "Red Flags" rule, the effective date of which has been delayed to June 1, requires many businesses, including most health care organizations, to take specific steps to minimize identity theft.

The rule, authorized under the Fair and Accurate Credit Transactions Act, requires any organization that extends credit to its clients to develop and implement written identity theft prevention programs that help identify, detect and respond to patterns, practices or specific activities, known as "red flags," that could indicate identity theft.

The FTC's Red Flags Web site offers resources to help organizations determine if they are covered and how to comply with the rule. It includes an online compliance template that enables organizations to design their own identity theft prevention program. The World Privacy Forum has produced a white paper, available on its Web site, offering advice to health care organizations on Red Flags rule compliance.

The report offers examples of "red flag" incidents that could indicate identity theft. Among them are: a complaint or question from a patient based on the patient's receipt of a bill for another individual; records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient; and a complaint or question from a patient about information added to a credit report by a health care provider or insurer.

A number of software companies are marketing applications designed to detect potential identity theft. Southwest Washington Medical Center, Vancouver, Wash., will be using two applications to detect suspicious activity on its computers that could signal attempts at ID theft or other privacy violations, says Christopher Paidhrin, security compliance officer. The organization will use auditing software from FairWarning Inc., St. Petersburg, Fla., to monitor its clinical systems and ArcSight Inc., Cupertino, Calif., for other applications, Paidhrin says.

"We'll be looking for anything out of the ordinary," the security officer says, such as someone trying to create their own financial account.

Complying with the Security Breach Rule

Hospitals, physician group practices and other provider organizations should be reviewing their internal policies as well as working with their business associates to prepare for compliance with updated federal data privacy and security regulations, many experts advise.

New federal requirements under the American Recovery and Reinvestment Act governing the notification of breaches of protected health information bring major changes to the HIPAA privacy and security rules, says Steven J. Fox, a partner in the Washington law firm Post & Schell. "You do have to really start over with HIPAA," he says. "You're going to have to do completely new education and training."

And that training will need to continue on a rolling basis during the next year as new guidance and rules are published to replace an interim rule from the Department of Health and Human Services that became effective on Sept. 23, he says.

At Southwest Washington Medical Center, Vancouver, Wash., all staff members were required to take a course on the updated privacy and security rules by the end of last year, says Christopher Paidhrin, security compliance officer. He notes that the breach notification provisions require every health care organization do a risk assessment for every incident to determine the degree of harm.

Health care organizations must update their privacy and security policies and procedures to ensure an adequate response to breach incidents, Fox notes. Providers also should mobilize rapid response teams to handle breach incidents in a timely manner, he advises. Organizations will not qualify for Medicare/Medicaid incentive payments for meaningful use of electronic health records until any outstanding HIPAA privacy/security investigations are complete and the organization is compliant, the attorney stresses.

As a result of ARRA, business associates must comply with the HIPAA privacy and security rules effective Feb. 17, 2010. Business associates also will be subject to the same tougher penalties as covered entities, such as hospitals and physician groups, for privacy and security violations.

Business associates are organizations that provide a service for a covered entity and use protected patient information to provide that service. Business associates now must notify providers when a data security breach involving patient data occurs.

At the American Health Information Management Association convention, Mary Thomason, senior compliance consultant at Intermountain Healthcare, a Salt Lake City, Utah-based delivery system, offered this advice:

* Be certain that all business associate agreements spell out all the details on the timing and content of security breach notifications. "You want to know quickly if there's been a breach," Thomason said.

* Make sure you have current contact information for key business associate staffers who handle privacy/security issues. Intermountain also told its associates who to contact in case of breaches.

For more information on related topics, visit the following channels:

- Data Security
- Electronic Health Records
- Mobile Tech
- Systems Integration
- Hospitals
- Group Practices

©2010 Health Data Management and SourceMedia, Inc. All rights reserved.

SourceMedia is an Investcorp company.

Use, duplication, or sale of this service, or data contained herein, is strictly prohibited.