H&HN
HOSPITALS & HEALTH NETWORKS®

Cybersecurity

Why Two-Factor Authentication Can Help Keep Your Data Safe

Hospitals can choose from several options to improve digital privacy, protection and compliance.

May 12, 2016 *John Harris*

Like locks on a door, one identity authentication method is good, but two are better. This security philosophy has gained traction in hospital information technology. It's called two-factor authentication — using two different means to verify an identity before an individual is allowed to view electronic files, such as health records and digital billing invoices, or to sign documents electronically.

As its name implies, two-factor authentication (also referred to as multifactor authentication) validates the identity of a person attempting to access files using two separate means. Most often, two-factor authentication combines something you know (a username and password, personal information, an account number) with something you have (a one-time code sent via a text message to your mobile phone) or something intrinsically part of you (your fingerprint, your voice).

Adoption of two-factor authentication at nonfederal acute care hospitals has increased 53 percent since 2010, according to an Office of the National Coordinator for Health Information Technology brief released in November. In fact, well over half of larger hospitals (63 percent) and medium-sized hospitals (59 percent) have two-factor authentication capabilities.

Breaches and attacks on data

This rise in two-factor authentication in hospitals arises from necessity.

Data breaches could be costing the health care industry $6 billion annually, with the average breach

continued on next page

estimated to cost an organization more than $2.1 million, according to independent research firm the Ponemon Institute in its 2015 Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. Sixty-five percent of health care organizations in the study said they had experienced electronic information-based security incidents in the two previous years, and half of all organizations surveyed said they had little or no confidence in their ability to detect all patient data loss or theft.

Finally, and perhaps most alarming, criminal attacks on health care organizations had increased 125 percent over five years, making them the No. 1 cause of data breaches in health care at the time the report was compiled.

People are maliciously targeting health care data and documents. They're looking for a way in, and if security is weak and one dimensional, they're often finding it.

Federal mandate

For hospitals and health care organizations, two-factor authentication is not just a feather in the cap of the information technology department. It's a security and privacy measure that fulfills federal mandates and in some cases is required by law.

The Health Insurance Portability and Accountability Act requires covered entities to verify that a person seeking access to electronic protected health information has the authority to do so and to confirm that users are who they claim to be. Two-factor authentication, of course, fulfills this need twice over.

Other governing laws are more direct in their mandates for two-factor authentication. In 2010, the U.S. Drug Enforcement Administration added the requirement of two-factor authentication for electronic prescribing to its interim final rule Electronic Prescriptions for Controlled Substances, stating, "Authentication based only on knowledge factors is easily subverted because they can be observed, guessed or hacked and used without the practitioner's knowledge."

The U.S. Food and Drug Administration also expressly requires two-factor authentication to submit information electronically (Code of Federal Regulations, Title 21, Part 11). For organizations using electronic records and e-signatures to submit documents to the FDA, a single method of authentication won't do.

continued on next page

Choice of methods

The use of two factors to prove a file seeker's or e-signer's identity should balance usability and security for the specific documents and transactions at hand. The more sensitive the files, the stronger the authentication factors should be. When in doubt, it's generally wise to err on the side of security.

Typically, two-factor authentication will combine any two of the following methods:

- **Email verification:** One of the simplest forms of identity authentication, email verification uses the email service's username and password credentialing process as its gatekeeper. Once people gain entry into their email and click a link, they are successfully authenticated and have access to the digital documents.
- **Text message verification:** Text message authentication validates people by requiring they submit a one-time PIN code they've received via a text message to their mobile phones. The codes are unique and random for each user with each access attempt. Given the ubiquity of smartphones, text message authentication is one of the more convenient methods for pairing something you have (the phone) with something you know.
- **Hard token authentication:** People may use hardware for another level of authentication. This could be a personally identifiable key fob or a security token to grant access to electronic documents or e-signature transactions.
- **Biometric authentication:** Biometric authentication uses technology to verify biological traits such as a fingerprint, iris or retina pattern, or voice. Using biometrics for authentication purposes remains relatively novel.

Though a fully paperless health care industry has not yet arrived, e-signatures, electronic health records and other digital processes are becoming the new normal. And the new normal demands cyber fortification at every barrier, including the front door — the entry point of data. Like a deadbolt, two-factor authentication adds strength, and it greatly improves digital privacy, protection and compliance.

John Harris *is the chief technology officer at SIGNiX, a digital signature solutions provider in Chattanooga, Tenn.*