Health IT OUTCOMES

Guest Column | April 11, 2016

Multi-Factor Authentication Gains Traction In Healthcare

By John Harris, Chief Technology Officer, SIGNiX

In the early days of the Internet, there wasn't a lot of user information stored on websites and publicly accessible databases. The only thing a user went to a healthcare website for was to check office hours or find a phone number. She wouldn't need to access sensitive materials because the majority of them weren't stored electronically. As for medical records and billing transactions — it was all paper, all the time.

As systems evolved, offices have automated much of the administrative functions of healthcare and begun using digital technology to facilitate transactions and collect, store, and retrieve information. Now patients and healthcare professionals alike are making and verifying appointments, getting lab results, and accessing personal health information (PHI), meaning that today organizations store the personal information of millions of users digitally. It is incumbent upon professionals to keep that information safe.

So, like all industries using digital processes, the healthcare industry adopted common authentication protocols — specifically a username/password combination that allows the user to gain access to his own information while blocking access to others.

The problem with that system is it depends on end users to use password discipline. This may come as a big surprise: they don't. A full 73 percent of online account holders use the same password for multiple accounts, per a recent ***TeleSign report***. So, if a hacker gains access to

a person's account via a data breach, all the other accounts for that person can become vulnerable due to the stolen credentials. That problem is multiplied because typically hackers aren't only accessing one person's account, but hundreds or thousands at a time.

Today, the healthcare industry is under enormous scrutiny with regard to data protection. Simultaneously, we're moving toward a system that values, and even demands, the efficiency of the paperless office environment. We need to devote fewer resources to printing, signing, filing, and storing paper and enhance security and authentication — all while improving both the bottom line and the patient experience.

The best answer is multi-factor ***identity authentication***. This process instills confidence in the end user that data is safe because it combines two or more identity authentication methods to establish her identity. It works by combining something you know (such as a username/password combination) with something you have (such as a text message code on your mobile phone). By combining two or more distinct protocols, you decrease the likelihood of someone using stolen credentials to attack your systems by 52 percent, according to the 2015 Annual Report to Congress on the Federal Information Security Management Act.

Multi-factor authentication also supports regulatory compliance. The Health Insurance Portability and Accountability Act (HIPAA) requires entities to verify and authorize the identity of a person seeking access to electronic PHI. Also, the U.S. Drug Enforcement Agency now specifically requires multi-factor authentication for electronic prescribing.

Because of its role in ensuring both security and compliance, multi-factor authentication has grown dramatically within the healthcare industry. Since 2010, use of multi-factor authentication among non-Federal acute care hospitals has grown 53 percent, according to the ***Office of the National Coordinator for Health Information Technology***.

And while it might seem like a deterrent to hassle patients, doctors, or administrators for proof of identification more than once, there are many options available to choose from — so you can pick two or more that will do the job with the least amount of disruption to the user experience.

The first step in multi-factor authentication will include at least one of these protocols:

- **Email authentication**, where you send the user an email link she clicks on to verify she has access to the registered email account;
- **shared secret questions**, which allows a user to set up question/answer combinations as part of the registration process, then verify he can answer them when he attempts to log in;

- **Know Your Customer (KYC) protocols** that use social security and birthdate to verify identity; or
- **Knowledge-Based Authentication (KBA)**, which uses not only the social security number and birthdate but also asks the user to answer questions based on information the system can pull from public databases, such as the make of car you drove three years ago or the address you lived at 10 years ago.

The second step of multi-factor authentication will include something you have with you, like a one-time code sent to a mobile phone via a text message or a security token that changes its code every few minutes.

In today's litigious world, multi-factor authentication can help protect healthcare organizations from bad data breaches and resulting lawsuits. So while it may be an extra step, with criminal data hackers on a constant prowl for personal information — and particularly health information — it is one worth taking.

About The Author

John Harris is the Chief Technology Officer at SIGNiX, a Chattanooga-based digital signature solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers the only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security.