Balancing Security and Clinical Workflow Concerns: A Precarious Act

Healthcare organizations strive to keep data safe while making it easy for clinicians to access

> **If you make things too hard, the system is either not going to get used or clinicians will simply outsmart it and find workarounds."**
>
> **– STEVE FURSTENAU**
> Director of Technical Business Development
> Imprivata

When an East Coast hospital implemented an electronic medical records system several years ago, leaders gave all clinicians a user name of "doctor" and a password of "password." As such, it was easy for clinicians to log into the system without skipping a beat. Unfortunately, it was easy for unauthorized users and malicious hackers to get into the system as well.

Requiring clinicians to use unique passwords, however, would mean that they would need to remember passwords at crucial points during the clinical workflow. "Physicians and nurses use many devices in various locations as they log-in anywhere from 50 to 75 times a day. So, this could seriously slow them down and could eat up to an hour of time a day," said Steve Furstenau, Director of Technical Business Development at Imprivata.

More troubling is the fact that the constant logging in can disrupt the care process. "Doctors are typically in the zone, focusing on trying to figure out what is going on with the patient. Anything that takes that focus away is a major distraction because they've got to stop their medical thinking and try to figure out, 'OK, did I use my kid's name? My dog's name? What numbers did I put into this?'" he said.

Striking a balance between security and clinical workflow efficiency is a conundrum that healthcare IT leaders have been wrestling with for some time. The challenge rests in maintaining high levels of security while making the sign-in process unobtrusive. "If you make things too hard, the system is either not going to get used or clinicians will simply outsmart it and find workarounds," Furstenau said.

Finding the right balance

Proximity badges – smart cards that can be read without inserting them into devices – make it possible to meet security and workflow requirements, when used correctly. To start, RFID readers should be integrated into devices, as external readers are difficult to use because they are often placed in difficult-to-reach locations. In addition, proximity badges should enable users to not only sign on to devices but access all needed applications.

Perhaps most important, leaders should address the fact that proximity badges can be stolen. A two-factor authentication process that includes identifying the user via the chip on the card as well as requiring them to enter a personal identification number (PIN) can help. To make this process less onerous, organizations should only require users to provide the PIN once or twice a day. "Once the badge has essentially been proven not to be stolen, users can simply tap the badge on the device to access the system," Furstenau said.

Making the identification process easier for clinicians becomes especially important when striving to comply with stringent U.S. Drug Enforcement Administration (DEA) requirements for the electronic prescribing of controlled substances. For this care process, hands-free authentication can make the required two-factor authentication more convenient by remotely retrieving the second factor from the prescriber's locked mobile phone. When used with fingerprint biometrics, there is no need to enter a password. As such, the prescriber can simply scan their finger and keep their mobile phone in their pocket.

Adoption strategies

For clinicians to embrace these systems, though, implementation teams need to make a good first impression. "If clinicians have a bad experience at the beginning, organizations will probably never get their buy-in and the solutions will fail," Furstenau said.

Demonstrating the process during learning fairs could help get users on board. "If you can get around 15 or 20 percent of people to really understand it, then there will always be somebody around to help out new people or those who don't understand," he explained.

When users embrace an integrated security system, total cost of ownership (TCO) benefits quickly accrue. "In the old days when people were getting locked out of their accounts, they would call the help desk and a lot of money would be spent on the help desk side of things," he said. With easy-to-use systems in place, healthcare organizations can save money by reducing the burden on help desk staff and also increasing clinical productivity.

The TCO benefits don't end there, though. "If you have an environment that is physician-friendly and the hospital

down the road doesn't, guess where the physicians are going to bring their patients? They're going to bring them to the environment that's easier for them to work in. And, an orthopedic surgeon can bring in anywhere between $20 million to $25 million to a hospital annually," Furstenau explained.

Of course, the greatest value comes in the form of improved care. "Anything you can do to make security easier benefits the clinical process because then people aren't wasting their time doing non-clinical tasks. There's enough of that today with clinicians being required to perform so many electronic record keeping tasks," Furstenau concluded.