imprivata®

Optimize access and security

"Our doctors and nurses love OneSign because it took what was a very cumbersome login process for them and turned it into what they call 'swipe and go'."

Dr. Karim Jessa, Emergency Physician and Director of Medical Informatics, Mackenzie Health

Organization

Location: Southern Ontario
Industry: Healthcare
EMR: McKesson

Challenges

- Generic logins created risks with security and patient privacy
- Network (user-specific) logins were bogging down the clinical staff
- Password reset calls swamped the IT Helpdesk; drove costs up and user satisfaction down

Results

- Imprivata OneSign delivered automated access management and single sign-on
- Eliminated manual logins, saving each care provider at least 15 minutes during every shift
- Streamlined workflow enabled physicians and nurses to improve productivity
- Greatly reduced Help Desk calls, freed IT staff to work on more strategic projects

Mackenzie Health is a major regional healthcare facility that serves Southwest York, Ontario, one of Canada's fastest growing regions. Its primary facility is the large, community-based Mackenzie Richmond Hill Hospital which was formerly known as York Central Hospital. At its Richmond Hill facility, Mackenzie Health provides emergency, inpatient, ambulatory, continuing, and long-term care services to more than 500,000 community residents. Mackenzie Health also serves as the regional center for provisioning of other services, such as stroke and chronic kidney disease care, behavior management, and Autism programs.

Mackenzie Health recently received an expanded mandate from the Ontario Ministry of Health and Long-Term Care to build a new facility. When the new Mackenzie Vaughan Hospital is completed, it will bring high-quality healthcare services to even more residents of the Greater Toronto Area.

The business challenge

Many years ago, Mackenzie Health care providers routinely accessed hospital workstations and desktops using generic log-ins. To ensure easy access, the staff kept logins simple, usually reflecting the machines' locations. The log in for a shared workstation in the Emergency Department, for example, would be a username like "Emergency" and a password such as "Emerg123". For any care provider who did not know them, logins could often be found on a sticky note under the keyboard or stuck to the monitor.

That approach made for very easy access, but it also was exposing the hospital to risks in areas including regulatory compliance, information security, and even patient safety. For example, at that time, the loose access enabled by generic logins was not in line with data privacy and security requirements set forth in the Personal Information Protection and Electronic Documents Act (PIPEDA).

Generic logins also were impeding care providers' efforts to work more productively. To perform tasks such as accessing their email accounts and

“In the ER, we looked at login times and saw that most of our clinicians were typing in their credentials on average between 30 and 60 times per shift.”

- Dr. Karim Jessa, Emergency Physician and Director of Medical Informatics, Mackenzie Health

individual work files, backing up their work on the hospital’s network and working more securely to protect themselves and their patients, physicians, nurses and other care providers required user-specific login credentials.

Fixing one problem creates another

To address their security and privacy issues, and to boost staff productivity, the Mackenzie Health IT team eliminated generic logins and transitioned to user-specific network logins. Although this change was a major cultural shift, Mackenzie Health’s IT team rolled it out effectively and staff adoption went smoothly.

Not long after the change, however, the IT group noticed a new problem. Staff members were having trouble remembering their usernames and passwords. Not unlike other hospitals, Mackenzie Health has numerous clinical systems and applications from many different vendors deployed in its environment. Many of these systems are not LDAP integrated, and have varying requirements for username and password strength, expiration times and resets. This created a lot of password complexity which was a burden for users. For physicians especially, there were too many log-ins required to access to the resources and patient information they needed to do their jobs. When care providers forgot their passwords, or when their profiles took too long to load, they would experience frustrating disruptions to their workflows.

The focal point for the care providers’ frustration was the Help Desk. At the time, Mackenzie Health had two full-time IT employees covering that area. As password reset calls mounted, the team struggled to keep up with call volumes, and often their responses were delayed. At that time, over 80% of Help Desk calls were user requests for password resets.

Exacerbating this problem was the fact that although the hospital was a 24/7 operation, the Help Desk was open only during normal business hours. Therefore, password reset calls that came in between 5 PM and 8 AM would potentially receive delayed responses. Password reset call volumes and response times continued to climb. These delays did not sit well with the care providers, who could face time-critical, life or death situations at any time of the day or night.

Another issue that began to emerge was the impact of user-specific logins on clinical staff productivity. Some physicians used up to four different applications and portals at any given time, each requiring different sets of credentials. These physicians and other care providers began complaining about excessive login requirements starting to impact the amount of time they had with patients.

“In the ER, we looked at login times and saw that most of our clinicians were typing in their credentials on average between 30 and 60 times per shift,” said Dr. Karim Jessa, Emergency Physician and the Director of Medical Informatics at Mackenzie Health Richmond Hill Hospital. “Some physicians were logging in 60 to 80 times per shift. At roughly 20 seconds per login, that amounted to between 15 to 25 minutes per clinician per shift. We wanted to find a way to reduce those login efforts and free up that time for our people to spend focusing on patients.“

The Imprivata OneSign solution

After thoroughly evaluating several options, Mackenzie Health selected the Imprivata OneSign® solution to address its authentication and access management challenges. The hospital implemented OneSign Single Sign-On and OneSign Authentication Management with fingerprint biometrics.

Imprivata OneSign provides Mackenzie Health's clinical staff with faster, easier, and more secure access to all of the hospital's key clinical systems and applications, and the patient data they contain. By removing the barriers that frustrated and distracted its doctors and nurses, including the need for repeated, manual logins, Imprivata OneSign has helped to optimize Mackenzie's clinical workflows. Today, with just a swipe of their fingerprint, Mackenzie's care providers are instantly logged in to their desktop and automatically signed in to their applications—without having to type a single username or password. Logging out is just as fast and easy.

"We chose Imprivata OneSign for several reasons," said Vince Ranieri, Senior System Network Analyst for Mackenzie Health. "It provided solid support for and was easy to integrate with our McKesson EHR and the several other McKesson applications we have widely deployed. For clinicians, it got the job done in a transparent way – adding valuable, time-saving functionality with basically no overhead. And from the IT perspective, the OneSign user interface is very intuitive. So activities like reporting, and managing our implementation – rolling out new capabilities or extending them to additional departments – is really easy. Also, the Imprivata team is very knowledgeable and responsive to any support needs that come up."

Results

Once Mackenzie Health completed its initial deployment of Imprivata OneSign, password reset calls to the Help Desk were significantly reduced. By removing the issues that caused those calls, Imprivata OneSign dramatically reduced care provider frustration and increased their use of the hospital's EHR system and other technical resources. Imprivata OneSign also freed up Mackenzie Health's Help Desk staff members to work on supporting other strategic IT initiatives.

By enabling No Click Access®, Imprivata OneSign is now saving at least 15 minutes per shift for every one of Mackenzie Health's doctors, nurses and other care providers. That translates into more than an hour each week that Mackenzie Health's care providers can spend focusing on their patients rather than on accessing technology.

"Our doctors and nurses love OneSign because it took what was a very cumbersome login process for them and turned it into what they call 'swipe and go'," said Dr. Jessa. "The bottom line is that with Imprivata OneSign, Mackenzie Health is able to strike an optimal balance between information access and security. It clears away hurdles and stumbling blocks that suppress care providers' adoption and use of powerful technologies. We're very happy that with Imprivata OneSign, Mackenzie Health has overcome those challenges."

"For clinicians, it got the job done in a transparent way – adding valuable, time-saving functionality with basically no overhead."

- Vince Ranieri,
Senior System Network Analyst,
Mackenzie Health

imprivata®

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

0S-CSS-Mackenzie-0318