imprivata®

Protect Patient Data and Streamline Clinical Workflows with Imprivata OneSign

"After looking at a number of different solutions available on the market, we selected Imprivata OneSign to introduce a Single Sign-On solution which could be supported with a robust combination of strong authentication options like badges and tokens."

Kevin Meerschaert, Systems Engineer and First Line Service Coordinator, AZ Groeninge

Organization

- Employees: 2,800
- Fifth largest hospital in Belgium

Industry

- Healthcare

Challenges

- Meet ISMS:ISP regulation requirement
- Protect patient data without disrupting clinical workflows
- Eliminate password sharing

Results

- Dramatically streamlined clinical workflows
- Security of patient data "improved exponentially"
- No Click Access™ to roaming desktops

Introduction

AZ Groeninge is a not-for-profit organisation that was formed through the merger of four hospitals: Kliniek Maria's Voorzienigheid, Onze-Lieve-Vrouwehospitaal, Sint-Niklaasziekenhuis and Sint-Maartenziekenhui, and is the only general hospital in Courtrai. AZ Groeninge is also currently the fifth largest hospital in Belgium with 1,100 beds and 2,800 employees including 300 doctors and 1,800 nurses. As well as making diagnoses and performing treatments, the organisation provides an educative and informative role within regional healthcare. It accommodates several specialised facilities and services including robotic surgery, a Eusoma-accredited Breast Clinic, a fertility centre, a radiotherapy unit and a cancer centre.

A new hospital is currently being built in Kennedylaan where the majority of AZ Groeninge's departments will ultimately be located when the project is completed in 2016. The new hospital will offer the organisation the opportunity to develop its research projects even further by introducing new services, care programmes, sub-specialisation in specific medical areas and cooperation with general practitioners and other healthcare institutions.

AZ Groeninge invests heavily in the training of its staff and was awarded the international 'Investor in People' award in 2007.

The Business Challenge

The development of AZ Groeninge's care programmes is an ongoing commitment and one which ensures the hospital is able to anticipate and meet the ever-changing needs of the surrounding community. As well as managing communication between its different medical departments, AZ Groeninge also works closely with other hospitals in the area to best support the local patient community, so sharing information securely is vital. The need to secure access to sensitive patient information meant that AZ Groeninge needed a robust privacy and security policy which could meet with Belgium's

“While our clinicians and other staff members want to do the right thing with regard to security, they can’t let it impact the treatment of their patients. With too many passwords, they were tempted to use each other’s log-on details to access patient information and applications they needed to provide care.”

- Kevin Meerschaert

strict security regulations. These include the ISMS:ISP (Information Security Management System – Information Security Policy) which every hospital must implement if they have a connection to the cross point database, which holds information about every person registered in Belgium.

Over the past few years the importance of security within healthcare has grown considerably in Belgium as the industry shifts from paper to electronic records, and the benefits of sharing and tracking data become clear. As a result, patient information within healthcare has become more tightly regulated. For example, the central Government has introduced random external audits which put pressure on hospitals to ensure that systems are highly secure. In light of this increased focus on security, AZ Groeninge has introduced an Internal Security Advisor role. Every hospital in Belgium has a legal obligation to employ an information security consultant to develop and manage its security strategy and identify security risks or infringements, flagging them with the IT management team and board members.

Alongside the Internal Security Advisor, the hospital board and IT department decided that changes were needed to improve the security of data yet also offer flexibility without disrupting clinical workflows. Many of the hospital’s applications were controlled by a bespoke password policy which meant that care providers had many different log-on credentials and complex passwords for specific applications. No password change policy was in place for these applications which meant that, although care providers weren’t forced to change their passwords on a regular basis, security was lax.

Kevin Meerschaert, systems engineer and first line service coordinator at AZ Groeninge explains: “While our clinicians and other staff members want to do the right thing with regard to security, they can’t let it impact the treatment of their patients. With too many passwords, they were tempted to use each other’s log-on details to access patient information and applications they needed to provide care. As well as compromising the security of patient information, the continual logging in and out of applications slows the provider’s workflow and consumes time that would be better spent treating patients.”

The Solution

“After looking at a number of different solutions available on the market, we selected Imprivata OneSign to introduce a Single Sign-On solution which could be supported with a robust combination of strong authentication options like badges and tokens,” said Meerschaert. For security and convenience, the IT team replaced the existing practice of logging in and out of the network, desktops and applications with passwords many times a day, with the use of physical access badges and tokens for strong authentication. This means that staff no longer struggle with log-ons/offs and there is no temptation to share or write down passwords. Instead care providers simply swipe their badges to access patient information. Additionally, AZ Groeninge is integrating single sign-on and strong authentication with desktop virtualization so that users can access the information they need to treat their patients from any workstation or device – from anywhere. Care providers can authenticate once with their badges and credentials, then throughout their shifts they can swipe their badges to log-on and off of their virtual desktops. Their sessions follow them as they treat their patients, running securely in the background when they are logged off, and appearing exactly as they were left when they swipe their badge at the next workstation.

The Imprivata OneSign solution also allows care providers to log-on remotely, wherever and whenever they need to, and the IT team has provided tokens for physicians who require access to the medical portal and patient data from outside the organization. This more flexible method of working means that the care process can be taken outside of the hospital, allowing care providers to access patient information at any of the four hospitals – or even elsewhere - quickly and securely.

The Results and Benefits

"The integration of SSO, strong authentication and desktop virtualization has had an enormous impact on productivity, and is a great example of how technology can be applied to enhance the care delivery process. By providing fast and secure access to sensitive patient information – in seconds rather than minutes - we are speeding clinical workflows and improving the quality of care – all while meeting with regulations."

AZ Groeninge has also been able to improve its access reporting with this integrated solution. Every night, the audit logs created by Imprivata OneSign are exported, analysed and a summary is generated. Using OneSign, AZ Groeninge can track employee access events to provide real-time, aggregated reporting of when, how and from where an employee gained network and application access. This increased level of knowledge surrounding the data staff are accessing helps monitor and prevent fraudulent activity, as well as helping the hospital to comply with regulations.

"With the knowledge that the security of our patients' data has improved exponentially with the introduction of Imprivata, we are extending the implementation to bring the same benefits to other areas of the hospital. Our aim is to introduce a laptop on the wards so that all our clinicians have access to the patients' complete medical history – from anywhere."

"With the knowledge that the security of our patients' data has improved exponentially with the introduction of Imprivata, we are extending the implementation to bring the same benefits to other areas of the hospital."

- Kevin Meerschaert

imprivata®

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata's single sign-on, authentication management and secure communications solutions enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care.

Over 2 million care providers in more than 1,000 healthcare organizations worldwide rely on Imprivata solutions. Imprivata is the category leader in the 2012 and 2013 Best in KLAS Software & Services Report for SSO, and SSO market share leader according to HIMSS Analytics.

For further information
please contact us at:
1 781 674 2700
or visit us online at
www.imprivata.com

Offices in:
Lexington, MA USA
Santa Cruz, CA USA
Uxbridge, UK
Paris, France
Nuremberg, Germany
Den Haag, Netherlands

CS-AZ-Groeninge-Ver1-0314