Customer Success Story: **Southwest Washington Medical Center**

Providing fast applications access to thousands of users

"As we added applications and users, the time savings were compounded. An individual clinician can recover up to 30 minutes of productive time each day using single sign-on. We estimate that we save the equivalent of a Full Time Employee's time each day using OneSign."

Christopher Paidrhin, Security and Compliance Officer, Southwest Washington Medical Center

Company

- Employees: 3200, with >3000 affiliated users

Industry

- Healthcare

Applications

- McKesson healthcare applications, Citrix Terminal Services

Challenges

- Thousands of users accessing >100 applications
- Lost productivity handling logins
- Regulatory compliance requirements
- Need to provide optimal service for affiliated physicians

Results

- Improved productivity —ROI within 8 months
- Strengthened security and compliance posture
- Clinicians save up to 30 minutes per day accessing applications

Introduction

Southwest Washington Medical Center, now formally called PeaceHealth Southwest Medical Center, is a major healthcare provider in southwestern Washington state, with over 150 years of serving the region with superior medical care. Repeatedly recognized as one of the 100 top hospitals in the US, Southwest provides a full range of outpatient and inpatient diagnostic, medical, and surgical services to Clark County residents. With over 3000 employees, and part of an organization of 15,000 employees, it is a major employer in Clark County, Washington. Southwest has been using Imprivata OneSign since 2005 to offer single sign-on to its employees and affiliated physicians and their staff.

The business challenge

With 600 beds, Southwest is a middle-tier hospital in a crowded and competitive healthcare market. Hundreds of affiliated physicians either work out of the hospital or refer their patients to Southwest. In addition to its own employees and physicians, more than 3000 external medical staff need access to patient records and applications. Southwest relies on more than 100 separate applications to deliver patient care and run the hospital efficiently, including many modules of the McKesson Horizon healthcare suite. With thousands of users accessing so many applications, basic access management was becoming unmanageable, consuming too much time in every employee's day.

Because Southwest relies on its affiliated physicians and their clinics, it wanted to make it as easy as possible for physicians to use Southwest. That meant addressing the authentication problem. Says Christopher Paidhrin, Security and Compliance Officer for Southwest, "We started investigating single sign-on as a way reduce the 'hassle' factor for physicians using Southwest."

"Identity and access management is the cornerstone of security and compliance. I sleep very well at night knowing [Imprivata OneSign gives me] foundational controls of access to patient information."

- Christopher Paidhrin

Workflow efficiency was another concern. The emergency services department is a Tier 3 trauma center and one of the busiest emergency rooms on the West Coast. Application access cannot get in the way of providing patient care. Paidhrin estimated that a clinical technician would access between 6 and 12 different applications at any time in the day, and might log on dozens of times during the day. Across the entire organization, application access had an enormous cumulative drag on productivity.

Finally, Southwest needs to protect the security and privacy of patient data and adhere to all regulations concerning data access, including HIPAA. A single sign-on solution would provide the groundwork for identity and access management controls that are essential to security and compliance.

The Imprivata OneSign solution

Southwest spent six months evaluating a dozen different single sign-on solutions, and determined that Imprivata OneSign was an ideal match for the hospital's needs. Imprivata OneSign provided the best functionality and price while meeting specific requirements, including:

- Out-of-the-box support for multiple authentication modalities, including biometrics, Active Directory and LDAP integration, RADIUS integration, and different strong authentication factors
- The ability to run concurrent profiles for different versions of the same application – important to support rolling application upgrades
- Easy deployment, requiring on average 20 minutes to create profiles for each application

Initial stopwatch tests determined that users could save 1-5 seconds per login per application, with many users logging in a dozen or more times each day to each application. Based on that, Paidhrin estimated a return on investment within a year.

The organization deployed Imprivata OneSign in 90 days in early 2005, enrolling more than 5000 users in the initial roll-out. Today it serves more than 6000 users, including the hospital's own employees and more than 3000 physicians and medical staff at affiliated clinics in the region.

Before imprivata OneSign

- Clinicians spend up to 30 minutes each day authenticating with different applications
- Adding strong authentication to individual applications is difficult
- Tracking application access for compliance purposes is challenging

After imprivata OneSign

- Users have one login for all of their applications
- Within the hospital facility, users can login with biometrics or passive proximity badges, and access all of their applications
- OneSign automatically tracks and reports all application access

The results

Imprivata OneSign has become a crucial part of the patient care infrastructure at Southwest. The hospital achieved a return on their investment in only eight months. Says Paidhrin, “As we added applications and users, the time savings were compounded. An individual clinician can recover up to 30 minutes of productive time each day using single sign-on. We estimate that we save the equivalent of a Full Time Employee’s time each day using OneSign.”

Imprivata OneSign has handled the hospital’s changing authentication needs in the years since its deployment. The emergency department uses biometric authentication with fingerprint readers, while Southwest has since added passive proximity readers across the hospital, using the employee badge to provide a physical security factor. Individuals simply need to put their card close to the reader and enter a short PIN to connect seamlessly to all of their applications. Southwest currently has 500 passive proximity readers and plans to expand their use for strong authentication within the hospital.

Imprivata OneSign also contributes to the hospital’s security and compliance posture by offering non-repudiable proof of application access in case of an audit or a breach. Says Paidhrin, “Identity and access management is the cornerstone of security and compliance. I sleep very well at night knowing I have foundational controls of access to patient information.”

Imprivata OneSign has met the hospital’s core objectives of providing better service to physicians, improving the productivity of its own workforce, and meeting security and compliance requirements. Says Paidhrin, “I’m a real advocate of single sign-on. The value of Imprivata OneSign is evident to every provider in our network, every day.”

“I’m a real advocate of single sign-on. The value of Imprivata OneSign is evident to every provider in our network, every day.”

- Christopher Paidrhin

imprivata®

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare globally to access, communicate, and transact patient information, securely and conveniently. The Imprivata platform addresses 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/intl

Offices in

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