How to Optimize

Epic Clinical Workflows with Imprivata

Imprivata OneSign® gives care providers fast, secure access to patient information by combining single sign-on with strong authentication enabling No Click Access™, a tap of a badge or a swipe of a fingerprint and they are logged into their desktop and applications.

As an Epic-approved, third-party vendor Imprivata leverages Epic’s authentication APIs. The Imprivata OneSign Connector for Epic provides the best user experience possible when signing in, signing out or signing off on documentation for encounters, orders or prescriptions within Hyperspace.

Using Imprivata OneSign enhances EpicCare™ from the perspective of several different stakeholders:

- **Care Provider** workflows are streamlined increasing adoption by keeping the focus on patient care instead of technology.
- **Clinical Leadership** meet their organizational goals due to the increased care provider adoption. Meeting Meaningful Use objectives while at the same time lowering their risk of HIPAA violations.
- **IT** can future proof their environment and give care providers one way to access systems with just a tap of a badge or swipe of a fingerprint. Imprivata OneSign is the leading authentication management platform that technology vendors such as Citrix, VMware, Teradici, Wyse/Dell are standardizing on.

This paper discusses the OneSign Connector for Epic capabilities in more detail.
STREAMLINE CLINICAL WORKFLOWS

The Imprivata OneSign Connector for Epic is designed to support a variety of environments including Epic-only, Epic together with other clinical and non-clinical applications, secondary authentication and strong authentication.

Epic-only Environments

Most hospitals are moving to Epic to centralize their EMR and remove disparate best of breed systems from their environment. Giving care providers one system to access means they only have that one username/password to remember. But keep in mind that this password still must change on a regular basis and care providers have to enter this username and password at each location they are at during any given day/shift. Whether they are moving from patient room to patient room during rounds or exam room to exam room—each patient encounter typically equates to at least one login to EpicCare, sometimes more. For example they have to follow-up to check on test results for a patient they saw earlier in the day. Studies show as many as 70 logins each day for the most mobile care providers.

Epic + Other Applications

Epic certainly minimizes the number of applications a care provider needs to access to get the full record of a patient but it doesn’t always eliminate all applications. Most organizations still have other clinical applications such as Dragon or non-clinical applications such as email, timecards or schedules that need to be accessed and of course with the migration to Epic not all applications are migrated at the same time so access to these other applications is necessary. This is where single sign-on comes in—managing all username/passwords for all applications care providers access—clinical or non-clinical.

Secondary Authentication

During some workflows within EpicCare care providers must re-enter their password. This is typically part of workflows that require a ‘sign-off’ such as ordering, chart signing or ePrescribing. Depending on the regulations, policies and procedures in your environment care providers need to take the extra time to re-enter their password for these workflows. OneSign No Click Access replaces the re-entry of the password with just the tap of their badge or swipe of their fingerprint they are signed off on these critical tasks.

Strong Authentication

Depending on the regulations, policies and procedures in your environment that are driven by federal and state regulations a stronger form of authentication maybe needed as a second factor. Imprivata OneSign supports a broad range of authentication modalities including those identified by the below regulations such as fingerprint, OTP and badge + password.

- Ohio State Board of Pharmacy: Strong authentication requirements for medication orders, administration and dispensing.
- EPCS: US Drug Enforcement Agency (DEA) requirements for Electronic Prescribing of Controlled Substances (EPCS). For more information on EPCS, see the Imprivata white paper A Planning Guide for Electronic Prescriptions for Controlled Substances (EPCS).
- I-STOP New York State legislation: Mandating the use of electronic prescriptions for all prescriptions (including controlled substances) in the state of New York effective January 1, 2015.
ELIMINATE COMMON HIPAA VIOLATIONS

Credential Sharing

When you rely on passwords alone, people will share credentials, even if they know they shouldn’t. And credential sharing is a HIPAA violation. Using Imprivata OneSign eliminates the problem of credential sharing. People don’t have to know and remember their passwords to dozens of applications, either.

“Deployment of OneSign has eliminated all excuses for sharing credentials by making user login and application access both fast and easy.”

Ben Exley, Service Desk Manager at Mercy Health System

Generic Accounts

Similar to shared accounts, many hospitals have ‘generic’ accounts set up on shared workstations. HIPAA regulations require that you identify each individual accessing healthcare information, which means the end of generic accounts. No Click Access and fast user switching supported by OneSign makes it easier for care providers to comply with these regulations.

Unattended Workstations

Imprivata OneSign protects the privacy and security of patient data on unattended workstations in several ways:

- Care providers can simply tap their badge or swipe their fingerprint to lock the workstation without signing out of their applications.
- OneSign supports desktop idle time-outs—adjusted according to workstation location.
- OneSign Secure Walk-Away® leverages active presence and facial recognition technologies to identify when the authenticated user leaves and re-authenticates them upon return.

FUTURE-PROOF YOUR ENVIRONMENT

Change is the only constant in Healthcare IT. Adding Imprivata OneSign to an Epic environment insulates the care providers from underlying change in effect future-proofing the IT environment. How care providers access systems remains consistent even as the underlying infrastructure changes.

New Clients

Using Imprivata shields users from changes to the client environment, leaving your options open to make changes down the road. OneSign integrates with both Citrix and VMware desktop virtualization. Imprivata also works with Teradici Pl-over-IP® zero clients from vendors such as HP and Dell.

New Versions of Epic

The Imprivata OneSign Epic Connector uses Epic APIs, which is backward compatible in new versions of Epic.
**New Applications**

Whether you are upgrading existing applications or adding new ones to the clinical environment, you can easily profile them for single sign-on. The OneSign® Application Profile Generator streamlines the process of supporting new applications.

**New Authentication Technologies**

Because Imprivata OneSign supports a broad range of authentication factors, you can add or change factors as your needs change. For example, physicians writing prescriptions for controlled substances may need different authentication factors for signing those prescriptions. Using OneSign, you can support a number of different factors in different environments.

**DEPLOY ONESIGN IN PARALLEL WITH EPIC**

One key to the success of any EpicCare implementation is identifying and streamlining workflows, to aid in overall adoption and care provider satisfaction. Imprivata OneSign works seamlessly with the Epic workflow capabilities, including Epic Logout and Secure. In addition, OneSign can extend this workflow optimization to include other clinical and non-clinical applications. The Imprivata team has extensive experience in workflow analysis and tuning.

Your strategy for integrating OneSign will depend on the status of Epic in your environment.

**New Epic Installations**

There are good reasons to focus on rolling out Epic and not adding any other solutions to the project schedule that could impact the rollout. But before you make your final decision you should think about how OneSign can have an impact to care provider adoption. When OneSign is integrated with the Epic roll-out, all it takes is a few extra minutes to train and enroll the users as part of the overall deployment. Many customers find that OneSign is so desirable that care providers start asking for it once they see a colleague use it.

“No arm twisting was required to get our employees to use OneSign. Anything you don’t force on people that makes their lives easier is going to be well received. As word of OneSign spread throughout the organization, people couldn’t wait to get it.”

Ben Exley, Service Desk Manager at Mercy Health System

**Phased Adoption in Existing Epic Installations**

It’s also possible to use a phased adoption of OneSign in the Epic environment, if you cannot do a big-bang roll out of OneSign. You can configure Epic Hyperspace to use either the OneSign Connector or the native Epic login screen based on workstation, and phase in OneSign by department or facility.

© 2012 Imprivata, Inc.
SUMMARY

Adding Imprivata OneSign to the EpicCare environment actually reduces complexity and risk of EMR adoption.

- It reduces the complexity of the environment from the care provider’s perspective by eliminating clicks required to access patient records on a daily basis, in multiple locations.
- It lowers risk for the healthcare organization by embedding security and compliance measures in the EpicCare environment.

The Imprivata team has extensive experience working with hospitals, physician practices and clinics to achieve successful implementations of OneSign with EpicCare. Their accumulated best practices can help Epic teams integrate this technology.

ABOUT IMPRIVATA

With over 2 million users and 900 healthcare customers, Imprivata is the #1 provider of secure access solutions for healthcare. By strengthening user authentication, streamlining application access and simplifying compliance reporting across multiple computing environments, customers realize improved workflows, increased security and compliance with government regulations.

Imprivata has received numerous product awards and top review ratings from leading industry publications and analysts, including a Strong Positive rating in Gartner’s 2011 Marketscope for ESSO, the #1 ranking in the KLAS SSO Performance report and the #1 rating in 2010 Best in KLAS and Category Leaders report. Headquartered in Lexington, Mass., Imprivata partners with over 200 resellers, and serves the access security needs of customers around the world. For more information, please visit www.imprivata.com or follow us on Twitter at @Imprivata.