imprivata®

How to optimize Epic clinical workflows with Imprivata OneSign

Imprivata OneSign gives care providers a fast and secure way to access patient information. The solution combines authentication management and single sign-on capabilities to enable No Click Access. With just a tap of their ID badge or swipe of their fingerprint, users are instantly logged into their desktops and applications.

As an Epic-approved, third-party vendor, Imprivata leverages Epic's authentication APIs. The Imprivata Connector for Epic provides care givers with a consistent, high-quality user experience when they log in or out, and sign off on documentation for encounters, orders, or prescriptions within Epic 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 can meet their organizational goals related to increased care provider adoption and achieving CPOE and Meaningful Use objectives while mitigating HIPAA violation risks.
- IT teams can future-proof their environments and give care providers a way to access systems with just a tap of a badge or swipe of a fingerprint.

For hospitals and clinics using the EpicCare EMR, the Imprivata Connector for Epic strikes the optimal balance between security and productivity by enhancing EpicCare deployments with advanced single sign-on and authentication management capabilities. By providing care providers with faster and easier ways to access and use patient information, the Imprivata Connector for Epic enables care providers to spend more time focusing on patients and less time dealing with technology.

This paper discusses the Imprivata Connector for Epic capabilities in more detail.

Streamline clinical workflows

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

Epic-only environments

Many hospitals in the U.S. are moving to Epic to centralize their EMR and reduce the number of disparate systems in their environments. Giving care providers just one system to access instead of many means they only have to remember one username and password. Passwords must still be changed on a regular basis, however, and care providers have to enter their usernames and passwords at each location they work from during a shift. Whether they are moving between patient rooms during rounds or exam rooms – each patient encounter typically requires at least one login to EpicCare. For example, care providers may have to follow-up to check on test results for a patient they saw earlier in their shift. Studies show as many as 70 logins each day for the most mobile care providers.

Epic and other applications

EpicCare certainly minimizes the number of applications a care provider needs to access a patient's record, but it doesn't always eliminate all other applications. Most organizations still have other clinical applications such as Dragon Dictate, or non-clinical applications such as email, or time and schedule management apps. During a migration to EpicCare, clinicians' access to these other applications and systems needs to be properly maintained. This is where single sign-on comes in—managing all username and passwords for all the applications care providers need to access—clinical or non-clinical.

Secondary authentication

During some workflows within EpicCare, care providers must re-enter their passwords. This is typically part of workflows that require a "sign-off" such as medication orders, charting, or e-prescribing. This secondary authentication is time-consuming and can cause frustration. Imprivata offers Imprivata Confirm ID as an integrated authentication platform which supports a broad range of authentication transactions, including DEA compliant EPCS, MAR (Medication Administration Reporting), etc.

> "Deployment of Imprivata OneSign has eliminated all excuses for sharing credentials by making user login and application access both fast and easy."
>
> - Ben Exley, Service Desk Manager,
> Mercy Health System,
> Janesvile, Wisconsin

The No Click Access and fast user switching supported by Imprivata OneSign makes it easy for hospitals to comply with regulations by eliminating the use of generic accounts – while still affording care providers the fast and easy access they need.

Mitigate common HIPAA compliance risks

Credential sharing

People often share their passwords, even when doing so is a violation of policy, or a likely HIPAA violation. Imprivata OneSign eliminates the problem of credential sharing. When care providers are not required to remember complex and frequently changing passwords, they have no need to share credentials.

Generic accounts

At many hospitals there are 'generic' accounts set up on shared workstations. Any clinician can access these account using simple, generic – and usually obvious – usernames and passwords. HIPAA regulations require hospitals and other healthcare organizations to be able to identify each individual who accesses patients' healthcare information. This requirement makes the use of generic accounts to access patient data constitutes a HIPAA violation. The No Click Access and fast user switching supported by Imprivata OneSign makes it easy for hospitals to comply with these regulations by eliminating the use of generic accounts – while still affording care providers the fast and easy access they need.

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.
- Inactivity timers can automatically secure a workstation after a set period with no usage, and the length of time-outs can be adjusted according to workstation location.

Future-proof your environment

Change is the only constant in healthcare IT. Adding Imprivata OneSign to an Epic environment insulates care providers from underlying change, in effect future-proofing the IT environment. With Imprivata OneSign, care providers can access their systems and applications in the same familiar way, even while changes are being made to the underlying infrastructure.

New clients

Using Imprivata OneSign shields users from changes to the client environment, which gives hospital IT teams flexibility and options if further changes are needed in the future. Imprivata OneSign integrates with Citrix, VMware and Microsoft RDS desktop virtualization environments, and works with Teradici PI-over-IP zero clients from vendors such as HP and Dell.

New versions of Epic
The Imprivata Connector for Epic uses Epic APIs, and is backward-compatible with earlier versions as new releases of EpicCare become available.

New applications
If organizations upgrade existing applications or add new applications to the clinical environment, they can easily profile them for single sign-on. The Imprivata OneSign Application Profile Generator streamlines the process of supporting new applications with a fast, easy, step-by-step process.

New authentication technologies
Because Imprivata OneSign supports a broad range of authentication factors, organizations can add or change factors as their needs evolve. Imprivata OneSign makes it easy to deploy and support different factors in different environments and for different workflows.

Deploy Imprivata OneSign in parallel with EpicCare

One key to the success of any EpicCare implementation is identifying and streamlining workflows. This is important because it boosts overall adoption and increases care provider satisfaction. Imprivata OneSign works seamlessly with the Epic workflow capabilities, including Epic Logout and Secure. In addition, Imprivata 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 Imprivata OneSign will depend on the status of the EpicCare deployment in your environment.

New Epic installations
There are good reasons to focus solely on rolling out EpicCare and not adding other solutions to the project that could impact the rollout. But before making a final decision about whether or not to deploy the two solutions simultaneously, consider the impact Imprivata OneSign can have on care provider adoption. When the solution is integrated with the EpicCare 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 Imprivata OneSign is so desirable that care providers start asking for it once they see colleagues using it.

Phased adoption in existing Epic installations
For organizations that prefer a phased approach to these types of IT and infrastructure changes, Imprivata OneSign gives IT teams and easy solution. Epic Hyperspace can be configured to use either the Imprivata Connector for Epic or the native Epic login screen. This enabled the roll out to be managed on a facility-by-facility or department-by-department basis.

> “No arm twisting was required to get our employees to use Imprivata OneSign. Anything you don’t force on people that makes their lives easier is going to be well received. As word of Imprivata OneSign spread throughout the organization, people couldn’t wait to get it.”
>
> - Ben Exley, Service Desk Manager,
> Mercy Health System,
> Janesville, Wisconsin

Imprivata OneSign works seamlessly with the Epic workflow capabilities, including Epic Logout and Secure.

Summary

Adding Imprivata OneSign to the EpicCare environment improves deployment in several ways by:

- Reducing the complexity of the environment from the care provider's perspective by eliminating clicks required to access patient records from multiple locations.
- Mitigating compliance risks for the organization by embedding security measures in the EpicCare environment.
- Encouraging faster and more complete care provider adoption.

The Imprivata team has extensive experience working with hospitals and other healthcare delivery organizations, as well as physician practices and clinics, to achieve successful implementations of Imprivata OneSign with EpicCare. The Imprivata team's accumulated best practices can help Epic teams effectively integrate their new technologies.

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