



IMPRIVATA HEALTHCARE DIVISION: SIMPLIFYING AND SECURING USER ACCESS TO PATIENT INFORMATION



ACCESS TO PATIENT DATA IS TIME CONSUMING AND FRUSTRATING

Healthcare Information Systems (HIS) have increased the efficiency of healthcare processes and improved patient safety, but because all patient data is not available in a single application, physicians and nurses must constantly log in and out of many different applications, using multiple passwords, to do their jobs. This is a frustrating process that consumes a significant amount of time—time better spent with patients, not at the workstation.

In dynamic healthcare environments where time is critical and clinicians need information, passwords are not only frustrating and disruptive, but they introduce audit and compliance issues when they are shared by users. Add to this the cost and resource burdens to the IT helpdesk for password resets and it's clear—passwords = headaches!

LESS TIME WITH COMPUTERS— MORE TIME WITH PATIENTS

Fast Access to Workstations and Applications

Using authentication devices proven in demanding healthcare environments, such as finger biometrics or ID badges, Imprivata OneSign® speeds access to workstations while securely initiating clinical workflows.

When coupled with the convenience of single sign-on, Imprivata OneSign eliminates password headaches by providing users with seamless access to all clinical applications without the need to remember and manage constantly changing passwords. With no more passwords to manage, IT helpdesk costs for password resets are reduced, and staff are free to work on other projects.

Fast Access to Patient Data

Imprivata OneSign works natively with Fusion by Carefx™, the leader in context management, to automate retrieval of patient records from different applications and

synchronize their context. A single view of a patient's complete health information dramatically reduces the time it takes to search for specific patient data. With all patient information available in real-time, clinicians can make better medical decisions—resulting in better patient outcomes.

Transparent Security

Imprivata OneSign simplifies the security of clinical workstations, patient data, and transactions, allowing users to quickly switch desktops between users, automatically lock unattended workstations, and positively identify users at the workstation, application, and transaction levels.

All along the way, Imprivata OneSign centrally monitors and reports on all access activity to easily demonstrate compliance with patient privacy requirements.

BENEFITS OF IMPRIVATA ONESIGN

- Fast access to workstations, applications, and patient data—from any workstation
- Alleviates password headaches—improving clinician workflows, productivity, and satisfaction
- Secures access to patient information—protecting patient privacy
- Lowers password management costs and burdens on IT helpdesk

WHAT'S INSIDE THE BOX

BUILT-IN SUPPORT FOR FINGER BIOMETRICS

Imprivata OneSign supports Dell, Lenovo, HP, Fujitsu, Motion, and other laptops with embedded UPEK or Authentec swipe sensors, as well as external UPEK and Authentec USB readers that may be mixed and matched on workstations or personal desktop machines. With just one enrollment, your users can authenticate to the network with a simple swipe or scan.

BUILT-IN SUPPORT FOR MULTIPLE CARD TYPES

Imprivata OneSign supports active and passive proximity cards, Windows smart cards, building access cards, and many National Health and government ID cards, including:

- RF Ideas, PCprox USB readers that support a variety of smart cards technologies, including HID, Casi-Rusco, Indala, Mifare, Crescendo, iClass, and others
- Ensure Xyloc active proximity cards and readers.

RAPID SINGLE SIGN-ON ENABLEMENT FOR ALL APPLICATIONS

The Imprivata OneSign Application Profile Generator® provides administrators with an easy-to-use, drag-and-drop interface that dynamically profiles all of an application's sign-on behaviors. Single sign-on enablement is rapid, and does not require any scripting or modification of application code.

SELF-SERVICE PASSWORD RESET

Clinicians can reset their primary domain passwords—securely and conveniently—without making burdensome and costly calls to the IT helpdesk.

ONESIGN FASTPASS™—FAST AND SECURE ONE-TOUCH LOGIN TO PATIENT INFORMATION AT ANY WORKSTATION

Imprivata OneSign allows a clinician to log in to a workstation using a proximity badge or fingerprint and a second factor (e.g. password or PIN) at the beginning of their work shift, and then roam to other workstations and authenticate just by tapping their badge or scanning their fingerprint—providing the convenience they demand, without sacrificing security.

ONESIGN PROVEID—TRANSACTION-LEVEL STRONG AUTHENTICATION

OneSign ProveID allows an application to leverage strong authentication services to positively identify a user at any point in an application's transactional workflow. For example, OneSign ProveID can enforce the positive identification of a user prior to drug disbursement.

ONESIGN SECURE WALK-AWAY—PROTECTING UNATTENDED DESKTOPS FROM UNAUTHORIZED ACCESS

OneSign Secure Walk-Away closes a critical security gap in the protection of confidential patient information records by automating the process of securing the desktop when a user 'walks away'. OneSign Secure Walk-Away uses a combination of computer vision, active presence detection, and user tracking technologies to identify an authenticated user and automatically locks the desktop upon their departure. OneSign Secure Walk-Away supports different clinician workflows, including demanding shared workstation environments where multiple users require constant fast and secure login and logout to patient information records.

SHARED WORKSTATIONS AND FAST USER SWITCHING

Imprivata OneSign supports workflows for shared workstations, including fast user switching between multiple, concurrent Windows desktops, as well as secure fast user switching on top of a generic kiosk desktop. Workstation security is increased with configurable "hot key" screen locking, inactivity lock/logoff policies, and screen locking by tapping a proximity card/badge.

CITRIX AND TERMINAL SERVICES SUPPORT FOR ROAMING SESSIONS

Imprivata OneSign supports Citrix and terminal services-hosted applications, automatically roaming the user's remote sessions when they log in to Imprivata OneSign, and keep locking the desktop of the user's previous workstation when they roam to a different workstation. Fast user switching is particularly valuable when an application has built-in workflows that require it to continue one session while different users sign in and out



“The nice thing about Imprivata OneSign is that it is architected in a way that is non-intrusive to the applications — it never touches the application code and it does not require an agent on the server.” *Christopher Paidhrin, HIPAA and Security Officer, ACS/Southwest Washington Medical Center*

CONTEXT MANAGEMENT SUPPORT

Many organizations require a context management interface for clinical applications (CCOW or other interface) to handle context switching between various applications. Imprivata OneSign natively interfaces with Fusion by Carefx™ to provide a complete view of patient data. Together, they create a user-driven, patient-centered clinical workspace that synchronizes context across multiple applications, increasing user productivity and patient safety.

USER PROVISIONING INTERFACE

Imprivata OneSign natively interfaces with Courion, Fischer International, and IBM/Tivoli for Day One user productivity and security. New employees have instant, seamless, and secure access to the data they need as soon as they are on board. There’s no need to distribute application passwords to users, and everything is centrally managed.

AUDIT, MONITORING, AND CONSOLIDATED REPORTING

Imprivata OneSign records all local and remote network authentication, computer, and application access events (even down to the application screen level) in a centralized database. At the push of a button, administrators can

Application	User	Domain	Application Credentials
Telnet	user1	sample.com	administrator
Telnet	user2	sample.com	administrator
Self-Service Portal	user3	sample.com	user3/sample.com/MS Active
Self-Service Portal	user1	sample.com	user3/sample.com/MS Active
OneSign Administrator	User1	sample.com	administrator/teak.eng/MS A

run any number of Web-based reports to discover, for example, which users are sharing passwords, who accessed which applications, and all the application accounts that belong to a particular user. This ensures rapid responses to audit inquiries that would otherwise require manual viewing and collation from independent system logs.

THE IMPRIVATA ONESIGN PLATFORM

Imprivata OneSign seamlessly integrates strong authentication, application single sign-on, user provisioning, context management, and event reporting to enable centralized access policies that enforce every aspect of access across all users, rights, locations, and conditions.

Managed from a single administrative console, the Imprivata OneSign Platform is delivered in a secure, self-contained appliance. Non-invasive to your organization's existing IT infrastructure, Imprivata OneSign requires no changes to user directories or applications, nor additional staffing or specialized management skills.

TECHNICAL SPECIFICATIONS

Desktop Operating Systems

- Windows 2000 Pro, Windows XP Professional, Windows XP embedded, Windows Vista, Windows Server 2000, Windows Server 2003, Windows Server 2008

Administration Console Requirements

- Microsoft Internet Explorer 6.1 or later running on supported Windows operating systems

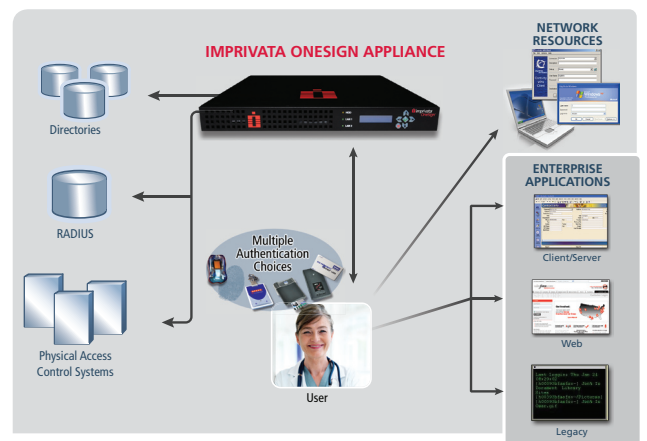
Directories Supported

- Microsoft Active Directory, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID), Novell Netware, Novell eDirectory, IBM Tivoli LDAP
- If needed, single sign-on benefits can be extended to users who do not exist within the organization's core directories, e.g., visiting physicians or students, through a OneSign directory

Strong Authentication Methods Supported

- Fingerprint biometrics, active and passive proximity cards, smart cards, many National Health and ID cards, One-Time-Password, and USB tokens

Designed for flexible and rapid enterprise deployment and easy integration, Imprivata OneSign's appliance-based approach dramatically minimizes implementation time, infrastructure needs, and installation costs—accelerating your return on investment and lowering your ongoing support costs.



Application Environments Supported

- ALL browser-based applications running in Internet Explorer 5.5 SP2 or higher on supported Windows OS
- ALL Mainframe, AS/400, UNIX, other legacy applications accessed via terminal emulators (TEs)
- ALL Win32 client-server or client applications on supported Windows OS
 - Windows applications
 - Java applications
 - Custom and legacy applications running on a supported Windows OS
- ALL clinical applications, including Cerner, Eclipsys, Epic, GE Medical, Healthland, McKesson, Meditech, and Siemens Medical

Context Management

- Interoperability with Carefx provides end-users with single sign-on (SSO) to network resources and to both CCOW and non-CCOW applications

Appliance

- Pair of ready-to-use, redundant 1U rack-mountable appliances. More appliances can be added for disaster recovery or to scale for large and/or geographically dispersed enterprises



Imprivata Healthcare Division: Simplifying and Securing User Access to Patient Information

Belgium | Germany | Italy | Singapore | UK | USA

1 877 ONESIGN | 1 781 674 2700 | www.imprivata.com