![Imprivata logo]

Imprivata Enterprise Access Management with SSO

Shared and single-user clinician access with single sign-on, fast user switching, EHR integrations, virtual desktop, and secure browser access

Streamline clinical workflows, simplify EHR access

Imprivata has a strong understanding of healthcare's unique IT requirements and offers a broad portfolio of advanced, healthcare-specific solutions that have been successfully deployed worldwide. Imprivata Enterprise Access Management (EAM) provides secure and convenient access to electronic health records (EHRs) and patient data, so providers can focus on patient care, not technology.

Increase provider satisfaction, protect patient data

EAM enables healthcare organizations to leverage the full benefits of their technology investments by building transparent, seamless, and convenient security into clinical workflows that streamline the clinicians' experience. By removing barriers that frustrate and distract care providers, like repetitive manual logins and complex passwords, EAM saves providers valuable time and increases provider satisfaction. In summary, EAM:

Benefits:

- Provides fast, secure access to patient information for every major EHR

- Replaces passwords, improves security, and supports HIPAA compliance requirements

- Enables fast, secure access into on-premises or cloud applications for all users from any device, anywhere

- Offers the industry's broadest integrations for thin/zero clients, virtual desktops and secure browsers

- Saves providers up to 45 minutes each per shift

- Streamlines clinical workflows by delivering No Click Access® to clinical and administrative applications, including those on-premises and in the cloud. With just a tap of a badge, or swipe of a fingerprint, or detection of a face, providers are instantly logged in to their desktop and automatically signed in to their applications without typing a single username or password.

- Protects patient data and helps healthcare organizations meet HIPAA compliance requirements by preventing credential sharing, securing protected health information (PHI) on unattended workstations, and enabling easier and more thorough auditing and reporting of workstation and application access.

Key features of Imprivata Enterprise Access Management for healthcare

Single sign-on and password management

Studies show that, by eliminating the need to repeatedly type usernames and passwords, providers can save as much as 45 minutes every day[1]. EAM supports a broad range of authentication methods and devices, including face or fingerprint biometrics, that can instantly identify providers for desktop access without disrupting their workflows or thought processes.

EAM largely eliminates the need for passwords. If clinicians forget their password, self-service password management capabailities let them quickly and easily reset it using modern security approaches like face recognition and Imprivata ID mobile push, reducing help desk calls and improving overall productivity.

Secure, fast user switching for shared workstations

Shared workstations are common in healthcare settings, but user-specific logins can be time-consuming and frustrating for providers. In the past, organizations have attempted to use generic Windows logins, but these and other workarounds expose various security and manageability issues. Instead, EAM enables secure, fast user switching between concurrent Windows desktops or kiosk workstations, reducing login times, all while protecting patient data.

Secure Workspace Access (formerly Virtual Desktop Access)

Imprivata Secure Workspace Access simplifies and expedites desktop access and application single sign-on for virtualized environments. These time savings, combined with the roaming capabilities of virtual desktops, deliver convenient mobility for providers. Imprivata Secure Workspace Access provides API-level support for VMware, Citrix, and Microsoft RDS. Imprivata also partners with the leading thin and zero client hardware and device vendors, including Dell Wyse, HP, Samsung, Texas Instruments, and Teradici. In addition, Imprivata provides integrations with Secure Enterprise Browsers (SEB) like Island Browser.

Embedding the Imprivata agent at the device level provides an unparalleled level of integration, which gives clinicians seamless access to their desktops, clinical applications, and patient data, regardless of the technology environment.

Cloud access via the Imprivata cloud identity provider

The Imprivata cloud identity provider (IDP) is a component of EAM that enables fast, secure access to SAML 2.0 web applications. This IDP allows users to access cloud applications from any device, from any location. The Imprivata cloud IDP also integrates with EAM badge-tap access to deliver near passwordless authentication into corporate devices, including shared workstations.

> "Imprivata [Enterprise Access Management] integrated with desktop virtualization has given clinicians secure and convenient access to patient data wherever and whenever they need it. This has resulted in improved physician satisfaction, increased clinical efficiency and ultimately helped to deliver improved patient care."
>
> – **David Wendt,** RPh, CIO, Franciscan Missionaries of Our Lady Health System

1. "Best Practices: Single Sign-On Drives Productivity, Security, and Adoption When Used with EHR at The Johns Hopkins Hospital" — IDC Health Insights: Healthcare Provider IT Strategies. BEST PRACTICES #HI238582, Judy Hanover, IDC

Integration and interoperability with EHR and clinical systems

EAM has been integrated and deployed with every leading EHR and with most of the more specialized solutions and clinical applications. EAM also provides tight integration with the Imprivata Connector for Epic to support Epic-specific workflows.

Seamless access to on-premises and cloud applications

Imprivata enables fast and secure access to on-premises and cloud applications from private or shared workstations to support healthcare's hybrid environment. With seamless access into cloud applications and deep integrations into EHRs and on-premises clinical applications, healthcare organizations have multiple ways of delivering single sign-on from any device and any location.

Ease of deployment, application profiling, and keeping up-to-date

One of the key advantages of EAM is how relatively easy the solution is to deploy and keep current. It's easy to enable new applications for single sign-on and keep application profiles and EAM software up-to-date. The Imprivata Application Profile Generator (APG) has an intuitive Graphical User Interface (GUI) that enables administrators to use "drag and drop" functionality to easily profile applications. Imprivata also makes regular updates to EAM, adding new capabilities, and seamlessly accommodating new releases from EHR, virtualization, secure browsers, and desktop partners, as well as from other technology vendors.

Innovative, secure walkaway technology

EAM secure walkaway capabilities offer healthcare's only solution that leverages the power of Bluetooth Low Energy (BLE) and the ubiquity of mobile devices to secure PHI on shared workstations without disrupting clinical workflow or patient care. Locking and unlocking of workstations is based on the presence of the user's mobile device, which removes the burden of passwords and disruptive inactivity timeouts.

Complete monitoring and simplified reporting

EAM records all local and remote network authentication and application access events in a centralized database within a hardened virtual or physical appliance. The Imprivata Appliance provides out-of-the-box reports that give administrators full visibility into system and application access and enable rapid response to audit inquiries that would otherwise require IT professionals to perform manual, time-consuming examinations of multiple system or application logs.

imprivata®