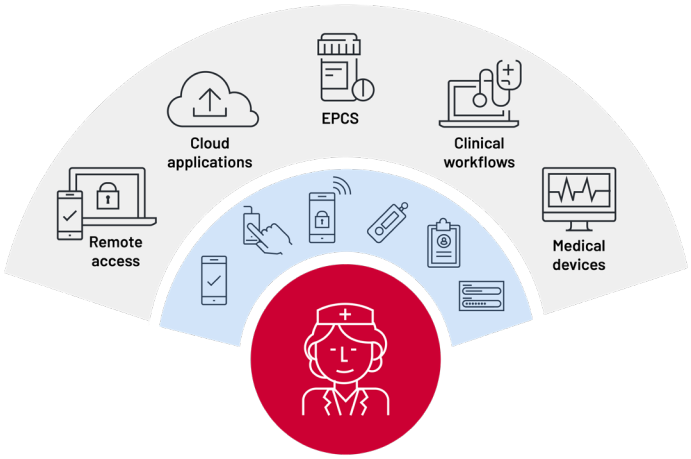
imprivata

DATASHEET

Imprivata Enterprise Access Management with MFA

Advanced authentication including passwordless solutions for clinical workflows, EPCS, and remote access

The need for advanced multifactor authentication (MFA) is being driven by an ever-expanding attack surface and regulations mandating two-factor authentication. But hospitals need the flexibility to ensure that multifactor authentication workflows meet the needs of their clinicians, no matter the use case. Passwordless authentication methods such as face recognition enable fast and easy access for clinicians, and provide improved security over passwords, especially when combined with another factor.



Imprivata Enterprise Access Management (EAM) with MFA provides orchestration, integrations, and passwordless authenticators for fast, secure authentication that provides the flexibility organizations need. EAM combines security with convenience by offering a broad range of innovative and convenient authentication methods such as face recognition, badge tap or Imprivata ID push tokens for secure, frictionless access.

EAM meets evolving healthcare needs by delivering passwordless authentication and MFA across use cases such as clinical workflows, electronic prescribing of controlled substances (EPCS), and remote access.

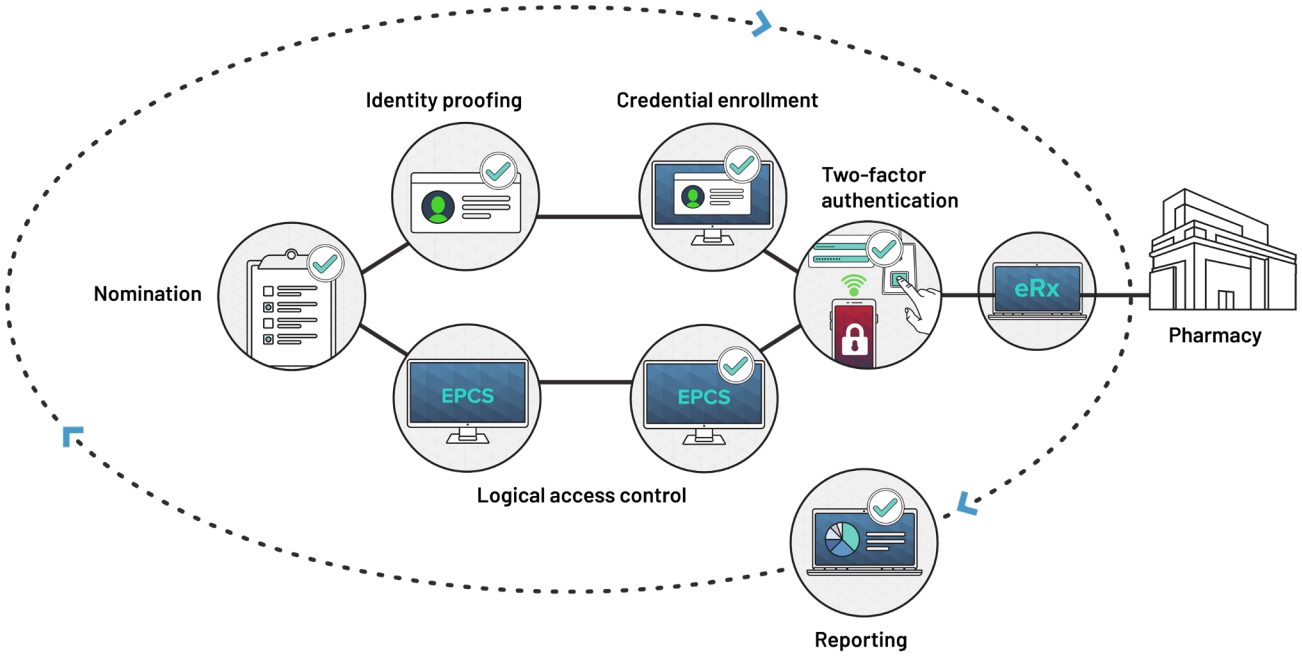
Clinical workflows

In healthcare environments, EAM improves security and regulatory compliance by enabling fast, secure authentication for clinical workflows. Imprivata transforms clinical authentication workflows by replacing passwords with fast, convenient methods such as the tap of a proximity badge, touch of a fingerprint, or Hands Free Authentication.

The solution also integrates with leading EHRs and other clinical applications to give providers a seamless authentication experience, where they are only prompted for authentication methods that are available and allowed. EAM for clinical workflows offers detailed reporting capabilities to establish a secure, auditable chain of trust for clinical authentication workflows. This gives organizations better visibility into how, when, and where providers interact with patient health information to safeguard PHI and meet regulatory compliance requirements.

EPCS workflows

EAM simplifies EPCS workflows by delivering a complete solution for provider identity proofing, supervised enrollment, and two-factor authentication, while providing the broadest range of DEA-compliant two-factor authentication modalities. It integrates directly into the e-prescribing workflows of leading EHR applications and streamlines order signing by only prompting providers for what authentication methods are available and allowed. This simplifies and secures EPCS workflows, while helping organizations comply with federal and state-level rules and regulations.



Platform integration with leading EHRs

EAM offers productized API-level integration with the leading EHR and e-prescribing applications. A single instance of EAM will work across the entire ecosystem, regardless of how many EHRs and e-prescribing applications are used in the network. This enables a consistent provider experience, while reducing the total cost of IT ownership.

Remote access workflows

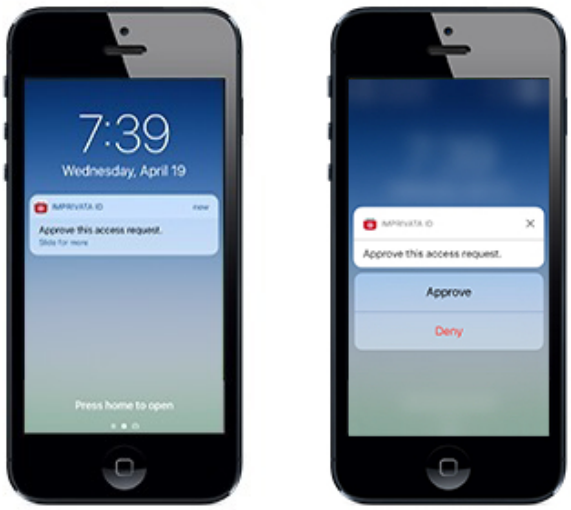
Healthcare and other sectors harboring sensitive digital information continue to be victimized by large-scale, high-profile data breaches. Malicious attackers employ highly targeted, sophisticated social engineering techniques to gain access to sensitive data.

EAM for remote access improves security by enabling two-factor authentication for remote network access, cloud applications, and other critical systems and workflows. The solution also offers convenient authentication methods such as push token notifications that can be leveraged across workflows, allowing organizations to add a layer of security that's familiar, fast, and efficient for users.

Improve security across the enterprise

With remote access gateways and cloud applications, along with Windows servers and desktops, EAM for remote access improves security by delivering holistic, enterprise-wide two-factor authentication across critical business, IT, and clinical workflows.

Together with Microsoft 365, EAM integrates with Azure AD conditional access, which simplifies MFA workflows for users without compromising security. This gives customers a single, phone-based token (Imprivata ID) to support numerous workflows, enabling customers to consolidate vendors and ensuring a consistent authentication experience for users.



Anywhere, anytime self-service device management

EAM for remote access lets users self-enroll their mobile device from any device, anywhere. Cloud-based self-service device management delivers fast and frictionless enrollment, which improves the end user experience and reduces the administrative burden of helping users enroll new devices. This enables organizations to scale the enforcement of two-factor authentication quickly and efficiently for remote access to the entire enterprise.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3328-2025_EAM-DS-multifactor-authentication_healthcare