

Imprivata Enterprise Access Management with MFA for Clinical Workflows

Fast, convenient, authentication for clinical workflows

Imprivata Enterprise Access Management (EAM) with multifactor authentication (MFA) for Clinical Workflows improves security and regulatory compliance by enabling fast, secure authentication for clinical workflows.

To deliver safe, effective, and compliant patient care, providers are often required to authenticate clinical transactions such as medication ordering, witnessing medication wasting, computerized physician order entry (CPOE), and blood administration, among others. However, adding a layer of security introduces potential inefficiencies that can frustrate providers and impede patient care.

EAM with MFA for Clinical Workflows transforms clinical authentication workflows by replacing passwords with fast, convenient methods such as the tap of a proximity badge, swipe of a fingerprint, or Hands Free Authentication. The solution also integrates with leading EMRs and other clinical applications to give providers a seamless, authentication experience and create a robust audit trail for all transactions with patient health information.

By using EAM with MFA for Clinical Workflows, organizations can improve security and compliance while increasing provider satisfaction and allowing more time for patient care.



Key benefits:

- Increases provider efficiency by replacing passwords with innovative and convenient authentication
- Integrates seamlessly with leading EMRs and other applications to enable fast, secure clinical authentication workflows
- Improves regulatory compliance and auditing with increased visibility into user interactions with PHI
- Simplifies authentication management with a single, centralized platform for all workflows

Seamless integration with leading EMRs and clinical applications

EAM with MFA for Clinical Authentication offers productized API-level integration with the leading EMR and other clinical applications. This tight integration streamlines clinical authentication workflows for providers by making it easy and convenient to re-authentication within their existing workflows. A single instance of EAM with MFA for Clinical Workflows will work across the ecosystem of EMRs and clinical applications, giving providers a consistent experience while reducing the total cost of IT ownership.



Fastest, most convenient two-factor authentication

EAM with MFA for Clinical Workflows offers the broadest range of convenient and innovative authentication options to best meet various clinical workflow requirements. Providers are only prompted for authentication methods that are available and allowed, which streamlines in-process authentication and improves efficiency. Some of the supported authentication options include:

- Proximity cards that enable authentication with the simple tap of a badge
- Hands Free Authentication, a breakthrough authentication technology that wirelessly retrieves and verifies a one-time password from a provider's mobile device, even if it is locked and/or in the user's pocket, delivering unparalleled speed and convenience with a solution that also meets the DEA two-factor authentication requirements for electronic prescribing of controlled substances (EPCS).
- Push token notification that gives users fast, convenient authentication from a mobile device
- Fingerprint biometrics, including options that meet DEA requirements for EPCS
- Conventional software one-time-passwords (OTP) tokens

Comprehensive auditing and reporting

EAM with MFA for Clinical Workflows offers detailed reporting capabilities to establish a secure, auditable chain of trust for clinical authentication workflows. EAM with MFA gives organizations better visibility into how, when, and where providers interact with patient health information to safeguard PHI and meet regulatory compliance requirements. Comprehensive reporting tools document the credential enrollment process and user authentication, storing the data in a centralized location for simplified compliance reporting.

For more information about Imprivata EAM with MFA for Clinical Workflows, visit:

<https://www.imprivata.com/solutions/ehr-optimization>

Comprehensive identity and two-factor authentication

EAM with MFA for Clinical Workflows is part of a comprehensive identity and multifactor authentication platform for fast, secure authentication workflows across the healthcare organization. EAM with MFA makes security invisible by offering a broad range of innovative, convenient, and DEA-compliant authentication methods, including Hands Free Authentication, push token notification, and fingerprint biometrics. EAM with MFA combines security and convenience by enabling fast, secure authentication across clinical workflows while creating a secure, auditable chain of trust wherever, whenever, and however clinicians interact with patient records and other sensitive data.

For more information, visit: <https://www.imprivata.com/products/access-management/enterprise-access-management/multifactor-authentication>



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. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables 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

Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.

