imprivata®

Imprivata Product Roadmap: Recent Releases and Upcoming Innovation



Q4 2026

A Note Regarding Forward-Looking Statements

The following includes statements regarding planned or future development efforts for our existing or new products or services. These statements are not intended to be a promise or guarantee of future availability of products, services, or features and are not intended to indicate when or how particular features will be priced or packaged. These planned and future development efforts are based on factors known to us at the time of publication and may change without notice. Purchasing decisions should not be made based on reliance on these statements. We assume no obligation to update these forward-looking statements."

Table of Contents

Product Name	Page
Enterprise Access Management	5
Mobile Access Management	6
Mobile Device Access	7
Patient Access	8
Access Compliance	9
Privileged Access	10
Identity Governance & Administration (DACH)	11

Simple and Secure Access Management Platform

Every Complex Workflow, Any User, Any Shared Device

Mobile Access Management (iOS and Android)

Simple and secure access to shared mobile devices and applications that creates personalized user experiences and optimizes workflows



Enterprise Access Management



Privileged Access Security

Privileged Access Management
Enterprise credential vaulting and session management of privileged users and activities

Vendor Privileged Access Management
Secure and connect inbound remote access to critical assets



Access Compliance

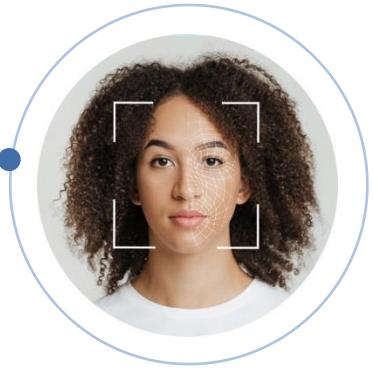
Patient Privacy Intelligence
Patient privacy monitoring that detects and creates alerts for suspicious behavior

Drug Diversion Intelligence
Proactive drug anomaly detection to protect patients and staff



Patient Access Management

Touchless face recognition integrated with leading EHR systems. Accurately identify patients and match them to their correct medical records to reduce denied claims, increase patient safety, and minimize duplicate records



Enterprise Access Management

Overview:

Imprivata Enterprise Access Management (EAM) simplifies and secures access to the devices, applications, and workflows that clinicians rely on to stay focused on patient care and frontline workers rely on to help them work efficiently.

Capabilities include:

- SSO into legacy and standards-based applications
- Badge-tap access to shared workstations, connected medical devices, and virtual desktops
- Re-authentication for in-app workflows
- Fast user switching on shared workstations
- Complete EPCS compliance
- Flexible authentication methods
- Comprehensive access workflow analytics

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

Non-disruptive agent upgrades (Nov. 2026)
Enables Imprivata to roll out security fixes, bug fixes, and minor component improvements without disrupting end user.

Audit record storage in Imprivata Cloud Platform (Nov. 2026)
Offloads audit data to EAM analytics to improve appliance performance and provide convenience, with the ability to store up to 18 months of data.

Modernized individual identity verification for EPCS (Nov. 2026)
Adds new identity verification capabilities for prescribers to support EPCS identity proofing.

Expanded service desk verification (Nov. 2026)
Adds ServiceNow integration, SMS/email verification options, and risk-based security for service desk workflows.

Face identification for shared workstation enhancements (Nov. 2026)
Introduces one-to-many face matching to identify users at shared workstations and simplify access.

Device Trust and stronger platform security (Nov. 2026)
Adds Device Trust, OIDC on the appliance, and security improvements for appliances and the admin console.

Access sensitive screens with MFA or witness signing (Nov. 2026)
Users can reauthenticate or request a witness for sensitive workflow screens without losing their single sign-on session.

Broader integration and regional support (Nov. 2026)
Adds Omnissa Horizon Cloud, France national access enhancements, and eIDAS-related workflow support.

Reporting and analytics improvements (Nov. 2026)
Expands EAM reporting and analytics to provide more visibility into EAM module adoption and feature usage.

Coming innovations

G5 appliance
Will provide a modernized foundation with stronger protection, reliability, and capacity, and with more flexible deployment options.

APG attestation
Users will be able to reauthenticate or request a witness for sensitive workflow screens without losing their single sign-on session.

Appliance level face recognition
Will make facial authentication available entirely on-premises, for environments where cloud usage is not acceptable.

TPM as an authentication factor for Web SSO and Remote Access
Users will be able to authenticate to protected application resources with a trusted platform module (TPM), plus another factor if MFA is required.

VPN-less application access
Will enable users to securely access required internal applications without a VPN by automatically connecting them to only the apps they need at login. This reduces user friction, enforces least-privilege access by group, and improves security and auditability.

Risk-based Authentication for VPN-less remote access
Will enable adaptive authentication for VPN-less access by evaluating real user risk (e.g., network context). This ensures low-risk users get seamless access while high-risk users are appropriately challenged, improving security without adding friction.

Appliance hosted in AWS
Will enable hosting Imprivata appliances on AWS for enhanced selection and adaptability in infrastructure options.

Streamlined workflows for national access in England and France
Will provide native SSO for applications integrated with national healthcare platforms - NHS Care Identity Service 2 (CIS2) in England and Pro Santé Connect in France - for simplified access and streamlined clinical workflows.

Imprivata Analytics for EAM
Will expand EAM analytics to include Identity Threat Detection and Response data integration to enrich insights.

Mobile Access Management

Overview:

Imprivata Mobile Access Management is a comprehensive, end-to-end mobility solution that helps organizations optimize their use of shared iOS and Android devices by delivering:

- Secure device checkout
- Simple access to mobile applications
- Personalized device experiences
- Visibility into device status and assignment
- Automated device management workflows

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

SAML group mapping (September 2026)
MAM console users can be assigned a role based on existing directory group membership.

Launchpad support for ICS Auto-Pairing without Configurator (September 2026)
MAM Launchpads will automatically configure the GroundControl supervision identity private key to be accessible by Apple Configurator on macOS launchpads.

Epic Rover witness authorization using facial recognition (June 2026)
Epic Rover users can perform a "witness" or "dual sign" workflow by authenticating using a second user with facial biometrics.

Support Apple return to service workflows for iOS devices (June 2026)
Imprivata MAM will support Apple Return to Service, enabling rapid device wipes and reprovisioning so users can quickly get the right setup and apps, especially valuable for apps that don't yet support logout.

Support for EAM automatic badge reader (June 2026)
Ability to configure EAM badge readers automatically when connected to a MAM launchpad.

Spanish language support (June 2026)
MAM will be able to support Spanish language use.

Passwordless authentication to mobile apps supporting OIDC (March 2026)
Login to apps like Epic Rover using facial biometrics for passwordless multi-factor authentication through the Locker App.

Improved visibility of device status for department managers (March 2026)
Device management application to provide direct views into device check out status in real-time including who has been assigned each device and where it's been returned.
an authentication modality for remote access with VPN integration.

Coming innovations

Launch apps automatically after check-out
Locker will support automatically launching a third-party app after check-out is completed.

Grab and Go Device support
Allows users to Check-in and Check-out devices without requiring connectivity to a Smart Hub.

Support for FIDO Badges
MAM Tap and Go will support FIDO badges for device check out from a Smart Hub.

Display Launchpad UI in MAM console
Provides MAM Admins with a live view of what the user is seeing when using the SmartHub Display Base.

Support unique thresholds for lost and overdue devices
More granularly remediate lost and overdue devices with unique thresholds to trigger automation workflows.

Limit checkout with Device Groups
Device groups allows admins to set device check out limits by device purpose.

Last known wireless location for iOS devices
Support for customers working with existing systems to be able to gather the last known wireless location for Grab and Go devices

MAM Automatic Out-of-Service
Automatic out-of-service to temporarily remove devices with consistent failures from circulation to prevent degradation of performance metrics and reducing failed checkout experience.

MAM Launchpad support for EAM failover
Support to cache high availability information from the EAM server list the first time the MAM Launchpad connects to EAM.

Log collection and Organization enhancements
Allows admins to remotely trigger log file collection to send directly to their console for organization and viewing.

Mobile Device Access

Overview:

Imprivata Mobile Device Access delivers on the promise of uncompromised security and efficiency by removing barriers to access share shared Android devices with:

- Secure, personalized access to Android devices
- Single sign-on for mobile applications
- Fast user switching with badge-tap on the device

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

Norwegian language support (September 2026)
MDA will be able to support Norwegian language use

Support for 42 Gears MDM (September 2026)
MDA now supports the utilization of 42 Gears MDM

Support for Workday(September 2026)
Web application support to allow users to review their personal Workday profile

Device management dashboard (June 2026)
MDA will have a web-based asset management page to view device information and reporting.

Support OIDC login to Epic Rover (June 2026)
Ability to support OIDC login to Epic Rover for a passwordless experience.

Integrate with Zebra Identity Guardian (June 2026)
MDA now integrates with Zebra Identity Guardian for support of facial biometrics and SSO.

Epic Server side log out (March 2026)
MDA will log out of the Epic Server after user returns the device.

Support for user to enter SIM card PIN (March 2026)
Ability for users to authenticate with their SIM card PIN.

Support for FIDO Badges (December 2025)
MDA will support authenticating to a device using a FIDO Badge.

Support for Emergency Dialers (December 2025)
Staff can initiate emergency calls even when mobile devices are locked.

Passwordless device check out (September 2025)
Customers can use facial biometrics for passwordless multifactor authentication when assigning out a device.

Passwordless device unlock (September 2025)
Customers can unlock an assigned device with facial biometrics.

Support AD Password Update (September 2025)
Consistent password update experience across desktops and mobile devices.

Coming innovations

Epic Rover witness authorization using facial recognition
Epic Rover users can perform a "witness" workflow by authenticating a second user with facial biometrics.

Lock screen branding & wallpaper
Support for users to apply branded lock screens and wallpapers across devices.

Credential learning through autofill
User credentials can be stored to automatically enter at next log in.

Support for Desfire
MDA will support authentication for organizations using Desfire badges.

Capture and report battery health
Ability to capture battery level and battery health data from enrolled mobile devices complied into a report for administrators.

Support for communication apps and notifications
Designate specific applications users can access before completing MDA authentication to enable faster access to time-sensitive clinical applications and workflows.

Facial biometric check out
Ability for users to check out shared mobile devices using Imprivata Facial Recognition for a faster authentication experience

Device management dashboard for department manager
MDA dashboard view for a department manager to help drive accountability and manage devices for their unit.

Last known device location with Wandering Device
Allows administrators to identify when a device's last known network-derived location does not match where the device is expected to belong for better visibility into device location.

Patient Access

Overview:

A face recognition solution designed with privacy at its core to help healthcare organizations eliminate patient misidentification—one of the root causes of denied claims and medical errors. By accurately linking patients to the correct medical record with just a single photo, the solution empowers providers to deliver efficient, error-free care and significantly reduce administrative burdens.

- Address misidentification to reduce denied claims
- Enhance patient safety and experience
- Reduce friction at registration
- Flexible hardware
- Seamless Epic Integration

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

Omnissa Horizon Qualification (August 2026)
Imprivata Patient Access has a documented, sales-supported deployment path for organizations using Omnissa Horizon.

Epic Break-The-Glass Support (July 2026)
Authorized providers can access Break-the-Glass–restricted patient records directly in Imprivata Patient Access. Access is recorded in Epic, allowing providers to continue their work without leaving the application or encountering a generic error.

ID Verification for MyChart Account Recovery (June 2026)
Enables patients to complete identity verification for MyChart account recovery, allowing healthcare organizations to reduce IT Help Desk workload.

Single Photo Identify to Enroll Workflow (April 2026)
Streamlines unscheduled workflows by enabling a single photo to be used for both patient identification and enrollment. This reduces duplicate steps, improves registrar efficiency, and creates a faster, more seamless patient check-in.

Streamlined Re-Enrollment (February 2026)
Registrars can now overwrite an existing facial enrollment within their normal workflow when authentication fails or a patient's appearance has changed.

Simplified Photo Capture Experience (February 2026)
Streamlines the photo capture experience for registrars by replacing numeric scoring with a simple pass/fail (green/red) indicator.

Magic Enrollment Enhancements (January 2026)
In addition to leveraging existing Epic photos for Magic Enrollment, registrars will now receive a notification at the first patient touchpoint when enrollment was completed using an existing Epic photo.

Self-enrollment from Epic Welcome Kiosk (December 2025)
This feature allows patients to complete identity proofing and self-enroll in Imprivata Patient Access from Epic Welcome Kiosks.

Coming innovations

Support for multiple patient identifiers (ECC)
Organizations using Epic Community Connect can use both enterprise and local medical record numbers (MRNs) in Imprivata Patient Access. Registrars can continue using the identifiers they know, while organizations maintain consistent patient records, reporting, and visibility across locations.

Self-Serve Guided Demo
An interactive demo that lets existing Imprivata customers explore the Imprivata Patient Access experience without connecting it to their Epic environment.

Remote Enrollment Patient Consent Support
Organizations can upload and manage their own consent documents and choose where those documents apply. During remote enrollment, patients can review and accept or decline the required documents. Organizations can also access records showing which documents were presented and how each patient responded.

Epic Service Desk Workflow
Service desk agents can remotely verify patients using biometric matching and government ID verification. This is a native Epic workflow that provides trusted verification results to support registration, account recovery, and patient service interactions.

Improve Customer Reporting with EHR + IPA Data
Provides deeper insight into Patient Access performance by combining EHR eligibility data with IPA activity metrics. Customers can easily track adoption, authentication rates, and growth opportunities with straight forward comparisons, trends, and actionable analytics.

Automatic Photo Refresh
Maintains accurate patient biometrics by automatically prompting photo updates every two years to reflect changes in appearance.

Access Compliance

Overview:

Imprivata Access Compliance helps healthcare organizations use AI and behavioral analytics to monitor access activity, identify potential risks, and support privacy, security, and regulatory compliance. **Patient Privacy Intelligence** (PPI) detects inappropriate access to patient information, while **Drug Diversion Intelligence** (DDI) identifies unusual controlled-substance activity that may indicate diversion.

PPI provides healthcare organizations with the tools they need to comply with confidence, protect patient data, and prevent violations

- Proactive & reactive auditing
- Robust reporting
- Efficient investigations

DDI helps organizations manage drug diversion to protect their patients, workforce, and organization while satisfying key regulatory requirements.

- Medication lifecycle auditing
- Use Case Monitoring
- Investigation management

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

Advanced Charting (October 2026)
New chart visualization options and enhanced configurability to support more tailored dashboard and reporting experiences.

Agentic AI Alert Summaries (October 2026)
Kickstart investigations with agentic AI that delivers concise, evidence-based alert summaries and recommended next steps.

First-Time Policy Offender Workflow (June 2026)
Automatically notify, track, and resolve first-time policy violations with configurable email alerts, acknowledgment steps, and automated alert closure, helping to scale enforcement and deter future violations.

Report Results – Details & Access Reports (June 2026)
Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

Report Portfolios (February 2026)
Create predefined groups of audit reports to run and export results asynchronously.

VIP / Watchlist (January 2026)
Create user and patient lists to flag VIP patients or suspicious users for more targeted monitoring in dashboards and reports.

Access Alerts – Investigate (September 2025)
Adds the ability to generate investigations from alerts based on PPI data.

High Risk User Monitoring for DDI (December 2025)
Leveraging One ID technology and our UEBA anomaly detection, monitor high-risk users, drill into access details, and quickly open investigations.

Coming innovations

Unified Patient Privacy Intelligence Model
Optimize risk identification, advancing anomalous workflow model and establishing a foundation for UEBA model expansion.

Flexible Investigation Layouts
Customizable layouts to support a variety of investigation workflows, multiple products, and international regulations.

Redesigned Report Builder
Modernized report creation experience to simplify building governance and compliance reports.

ITDR Integration
Integrate Identity Threat Detection and Response (ITDR) risk data into AIP to expand reporting and enrich identity insights.

Privileged Access

Vendor Privileged Access Management | Customer Privileged Access Management | Privileged Access Management | Agentic Identity Management

Overview:

Imprivata's Privileged Access suite enables organizations to holistically and seamlessly manage and secure all privileged access – whether remote access from vendors, internal users, or outbound to customers.

- Comprehensive, enterprise-grade remote access
- Third-party identity management & onboarding
- Credential management
- Session monitoring
- Least privilege
- Privileged account management

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update

Recently released

MCP Gateway (September 2026)
Control AI agent access to MCPs and their associated tools with delegated authentication, credential injection and audit.

Break Glass (August 2026)
Maintain secure, emergency access to vaulted credentials when the Privileged Access platform is unavailable.

Personal Vault (August 2026)
Allow users to securely store and manage personal credentials within an enterprise-grade vault.

New CPAM User Interface – Initial Release (July 2026)
Experience a modern UI with streamlined workflows that improve navigation and make critical information easier to access within Customer Privileged Access Management (CPAM).

Risk-Based Authentication for Connections (July 2026)
Apply step-up authentication to Privileged Access sessions based on real-time risk, with the ability to revoke access mid-session if risk exceeds defined thresholds.

Just-In-Time Access (June 2026)
Grant time-limited elevated access only when needed through an approval-based workflow. Automatically provision and revoke privileges to enforce least privilege, reduce risk exposure, and support compliance.

Facial Authentication (May 2026)
Add a facial biometric option to MFA, giving locally authenticated users a fast, secure, and convenient way to verify identity.

Agentic Identity Management (April 2026)
Manage AI and agentic identities with the same controls, governance, and visibility as human users—within the Privileged Access platform.

Risk-Based Authentication (March 2026)
Apply step-up authentication to Privileged Access logins based on each user's real-time risk profile, strengthening security without adding unnecessary friction.

Endpoint & Account Discovery (December 2025, March 2026)
Automatically discover endpoints and privileged accounts through scheduled scans, simplifying onboarding into Privileged Access.

Coming innovations

New CPAM User Interface – Full Release
Experience a modern UI with streamlined workflows that improve navigation and make critical information easier to access within Customer Privileged Access Management (CPAM).

MCP Gateway Tool Filtering and Approvals
Control tool level access within MCP services for fine grained control of AI access including human approval processes for AI access requests.

ID Verification
Request ID verification from third-party users as a part of step-up, risk-based authentication to strengthen security.

Non-Credential Vaulted Secrets
Vault secrets, such as certificates or other strings that are not traditional credentials, and control access through check-out processes and our robust permissions.

Identity Governance and Administration (DACH)

Overview:

Imprivata Identity Governance and Administration (IGA) automates identity lifecycle management, enforces a least privileged environment and enables day-one role-based access.

- Governance of lifecycle
- Role-based access controls
- Same day access
- Least privilege enforcement
- Access monitoring
- Certification of active users

Recently released

Expanded Healthcare Integrations
Adding user provisioning for Meierhofer KIS.

Exchange Online Integration (July 2026)
Enables standard Exchange Online workflows to support mailbox archiving and automatic reassignment of users' prior mailboxes upon re-enrollment.

Enhanced Service Portal (July 2026)
Expanded self-service capabilities with secure authentication, improved administration, and a more intuitive user experience.

Reconciliation Alerts and Reverting (March 2026)
Receive real-time alerts whenever manual changes occur. If an unauthorized or erroneous change is detected, you can quickly and easily revert to the previous state, maintaining the integrity of your system.

Interface Improvements for Dedalus Orbis (March 2026)
Improve the Dedalus Orbis interface by enhancing performance and increasing overall stability to ensure more reliable and efficient operations.

Honorary Physician Support (January 2026)
Support for the Station Management to quickly onboard a new honorary physician without the need of the internal IT.

Emergency Logout (October 2025)
In critical situations, immediately lock specific identities across all connected systems—no approvals required. This ensures swift containment during emergencies, minimizing risk and potential damage.

Interface Improvements and Expansions (October 2025)
Interface to SAP I.S.H. med and support for SCIM v2.

Coming innovation

Expanded Healthcare Integrations
Adding user provisioning into Epic, as well as interfaces for Telekom iMedOne, and CGM Medico.

Workday Interface
Enable IGA to query HR employee data from Workday.

Service Account Password Rotation
Automatically rotates passwords for service accounts to strengthen security.

On-Prem Cloud Agent
Connect to on-prem target and source systems from the IGA cloud.

Management Service Containerization
Migrate the management service, including module execution, to .NET Core to enable deployment of Unimate in Docker containers and improve portability and cloud readiness.

Support for Microsoft SQL Active / Active Cluster
Add support for Microsoft SQL Server Active/Active clustering to improve high availability, load distribution, and overall system resilience.

AI-Powered Identity Governance
Leverages AI to automate identity assignments, streamline approvals, and simplify role management for greater efficiency and accuracy.

Click here for more information

Return to Portfolio slide

imprivata®

Roadmap Update


imprivata®