imprivata®

Imprivata Product Roadmap: Recent Releases and Upcoming Innovation

Publish Date: March 30, 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

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

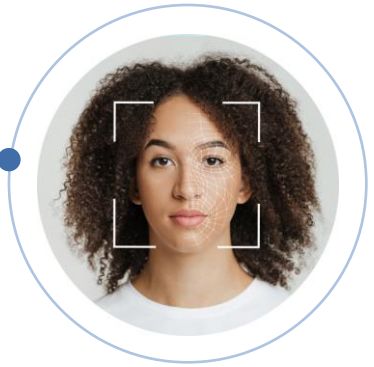
Access Compliance

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



imprivata®

Roadmap Update

Enterprise Access Management

Overview

Imprivata Enterprise Access Management (EAM) offers SSO and user authentication to enable fast, secure access to the devices, applications, and workflows that clinicians and frontline workers need to care for patients and boost productivity. 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

RECENTLY RELEASED

Risk-based Authentication for desktop access, self-service password reset, Web SSO and other workflows (April 2026)
Continuously assess user behavior, context, and location to apply stronger authentication only when risk is elevated - reducing friction for trusted users while helping prevent account takeover and support zero-trust compliance.

VPN-less remote access (April 2026)
Enable access for remote users by replacing the need for traditional VPN connections. Offers enhanced security with fine-grained role-based access control.

Support for Microsoft Authenticator App within EPCS solution (April 2026)
Enables the use of the Microsoft Authenticator app as a TOTP app for EPCS by allowing users to manually type in the Authenticator token code.

Passwordless, agentless EPCS with face authentication (Jan. 2026)
EPCS users can now use face recognition for passwordless EPCS MFA on their desktop or laptop, ensuring convenient, fast, and secure authentication.

MFA for access to offline computers (Jan. 2026)
Provides secure multifactor authentication (MFA) with Imprivata ID on offline devices - supporting remote and frontline users, such as traveling healthcare professionals or police officers, in critical situations without internet access.

Web SSO and remote access support for face authentication (Jan. 2026)
Provides support for face recognition to authenticate into web applications. Support for face recognition as an authentication modality for remote access with VPN integration.

Imprivata Analytics for EAM
New insights on Epic login performance (Mar. 2026) and unusual workstation usage (Dec. 2025); AI summaries for alerts (Dec. 2025).

COMING INNOVATION

Service desk caller identity verification
Will verify user identity with a scanned government ID that's automatically validated and matched - reducing social engineering risk and account takeover while lowering help desk costs.

Identity verification for self-service password reset (SSPR)
Will enable users who can't complete standard SSPR to securely reset passwords using built-in, NIST IAL2-compliant identity verification (ID + biometrics) via OIDC flow - reducing helpdesk reliance while improving recovery speed and security.

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 and Google Cloud
Will enable hosting Imprivata appliances on AWS and Google Compute Engine 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 provide expanded EAM reporting, Privileged Access, and Identity Threat Detection and Response data integration to enrich insights. Deeper visibility into active module and feature usage to drive adoption and optimize licensing.

imprivata®

Roadmap Update

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 managem ent workflows**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

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.

Personalized lock screen enhancements (March 2026)
Displays helpful information like return location and time remaining before device becomes overdue

German language support (March 2026)
MAM can be able to support German language use.

Reboot & Check-In for Express Checkout (December 2025)
Automatically remediate unhealthy iOS devices during Express Checkout, resorting them to a reliable state before next use.

Reboot SmartHubs (December 2025)
IT Admins will be able to reboot hubs remotely to accelerate troubleshooting.

Smart Folders for personalized Launchpad list (September 2025)
Dynamically update Launchpad folders that give console users a clear and focused view of the locations they manage.

Passwordless device check out (June 2025)
'Tap and Smile' with facial biometrics for passwordless multi-factor authentication when checking out a device.

Imprivata Analytics for MAM
Analytics launch with mobile usage and performance insights (March 2025); expanded library with new alerts for device issues and excessive checkout activity (September 2025).

COMING INNOVATION

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

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

Free Range Device support
Allows users to Check-in and Check-out devices without requiring connectivity to a SmartHub

Support for FIDO Badges
MAM will support authenticating to a device using a FIDO Badge.

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

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

Limit checkout by device type
Ability to limit the number of devices that can be checked out by one user during their shift based on the device type.

Support Apple return to service workflows for iOS devices
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.

SAML group mapping
MAM console users can be assigned a role based on existing directory group membership

Spanish language support
MAM will be able to support Spanish language use

Imprivata Analytics for MAM
AI-generated alert summaries, enhanced reporting with advanced charting, and streamlined workflows for policy violation tracking and resolution.

imprivata®

Roadmap Update

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

RECENTLY RELEASED

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

Auto Launch an app(s) at device log-in (June 2025)
Configure an app, or multiple apps, to launch automatically after a user first authenticates to a device

Understand application usage with enhanced analytics (June 2025)
Customers can report on user authentications to applications.

Support for new Android devices and environments (June 2025)
Recent highlights include support for HMD T21 devices and Zebra Workstation Connect.

COMING INNOVATION

Device home dashboard
MDA will have a web-based asset management page to view device information and reporting

Support OIDC login to Rover
Ability to support OIDC login to Epic Rover for a passwordless experience

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

Integrate with Zebra Identity Guardian
MDA now integrates with Zebra Identity Guardian for support of facial biometrics and SSO

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

Customizable fields on lock screen
Allows administrators to configure approved informational elements displayed on the lock screen

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

Support Break-the-Glass workflow in Epic Rover
Support for users to utilize badge-tap for authentication during Break-the-Glass workflows

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

imprivata®

Roadmap Update

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

RECENTLY RELEASED

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.

Display Customer Logo in Patient Facing Workflows (January 2026)
Allows healthcare organizations to display their logo across patient-facing workflows, including enrollment. account creation, and account recovery.

Multi-Appointment Workflow (December 2025)
Verifies the patient's identity once during initial check-in, enabling automatic face authentication for all same-day appointments.

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.

Self-Service MyChart Account Creation (November 2025)
Enables patients to complete self-service identity verification to obtain MyChart credentials and enroll in Patient Access for seamless authentication. A streamlined onboarding experience provides secure and efficient access to MyChart, meeting IAL2 standards.

Emergency Search – Identification for Unresponsive Patients (October 2025)
Identify patients who are unable to self-identify to ensure clinicians have access to the correct medical records.

ID Verification for Self-Service Enrollment (September 2025)
Verifies the patient's identity during self-enrollment in Patient Access (without a registrar), increasing confidence that the enrolling patient is who they say they are.

COMING INNOVATION

ID Verification for MyChart Account Recovery
Enables patients to complete identity proofing for MyChart account recovery, allowing healthcare organizations to reduce IT Help Desk workload.

Single Photo Identify to Enroll Workflow
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 experience.

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 clear comparisons, trends, and actionable analytics—all in one place.

Support for multiple patient identifiers (ECC)
Supports both enterprise and local MRNs for Epic Community Connect environments, ensuring registrars see familiar identifiers while maintaining enterprise-wide continuity. This improves usability, reporting, and visibility across multi-site organizations.

Site-Based Data Access & Permissions (ECC)
Enables service area–based data filtering for Epic Community Connect (ECC) environments, ensuring users only see patient data and reports relevant to their specific site. This improves data privacy, operational clarity, and scalability across multi-site organizations.

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

imprivata®

Roadmap Update

Patient Privacy Intelligence

Overview

Imprivata Patient Privacy Intelligence (PPI) helps protect patient privacy and deliver actionable insights for investigations, documentation, and reporting of privacy breaches. Equipped with artificial intelligence (AI), machine learning, and behavioral analytics, 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**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

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.

Product-Level Data Segregation (August 2025)
New functionality to assign Access Intelligence products (PPI, DDI, etc.) to end users, reports, alerts, and investigations to limit user access to objects owned by other products.

Updated User and Group Administration (August 2025)
Enhanced admin screens for User and Group provisioning and management with added functionality to guide role provisioning.

French Language Support (June 2025)
PPI now supports French language translation of all UI text and timestamp formats (excluding raw audit data).

Expanded Use of Alert Limits (June 2025)
Enforced Policies built from Access Reports can now be set to generate a max number of alerts per policy run, based on AIR score. PPI will automatically close lower risk alerts, which can be reviewed if needed.

Data Retention Configuration per Audit Source (May 2025)
Customers can now configure unique Data Retention Policies (DRP) for each audit source and set specific Archive and Purge schedules, using the new Archive Summary screen.

COMING INNOVATION

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

First-Time Policy Offender Workflow
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
Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

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

imprivata®
Roadmap Update

Drug Diversion Intelligence

Overview

Imprivata Drug Diversion Intelligence (DDI) helps organizations manage drug diversion to protect their patients, workforce, and organization while satisfying key regulatory requirements for managing controlled substances.

- **Medication lifecycle auditing**
- **Use Case Monitoring**
- **Investigation management**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

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.

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

Product-Level Data Segregation (August 2025)
New functionality to assign Access Intelligence products (PPI, DDI, etc.) to end users, reports, alerts, and investigations to limit user access to objects owned by other products.

Updated User and Group Administration (August 2025)
Enhanced admin screens for User and Group provisioning and management with added functionality to guide role provisioning.

French Language Support (June 2025)
DDI now supports French language translation of all UI text and timestamp formats (excluding raw audit data).

Data Retention Configuration per Audit Source (May 2025)
Customers can now configure unique Data Retention Policies (DRP) for each audit source and set specific Archive and Purge schedules, using the new Archive Summary screen.

COMING INNOVATION

First-Time Policy Offender Workflow
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
Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

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

imprivata®

Roadmap Update

Privileged Access

Vendor Privileged Access Management | Customer Privileged Access Management | Privileged Access 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

RECENTLY RELEASED

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.

Secret Unlock & Check-Out (August, December 2025; March 2026)
Enable controlled access to credentials with approval-based unlock and check-out. Enforce time-limited access and automatically rotate passwords after use to maintain security.

HTML5 Client & Audit Playback (September 2025)
Access RDP and SSH sessions and replay audits directly in the browser with high performance—no installs or external tools required.

Device Posture Check Configuration (September 2025)
Enforce device security requirements (e.g., antivirus, updates, UAC) with enhanced administrative controls to ensure only compliant devices gain access.

NIST Requirements in Best Practices Checklist (August 2025)
Align with NIST 800-53 and 800-63 by incorporating their requirements into the built-in best practices checklist.

Access Request Workflows for Internal Users (June 2025)
Require approval-based access requests for internal users, improving control and visibility over privileged asset access.

Next-Gen Connection Manager (June 2025)
Deliver faster, more reliable connections with an enhanced Connection Manager experience.

COMING INNOVATION

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

Risk-Based Authentication for Connections
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.

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

Just-In-Time Access
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.

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

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

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

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

imprivata®

Roadmap Update

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**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

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.

New Service Portal (July 2025)
Fully redeveloped service portal with responsive design and security features to be used as a public portal. Includes MFA integration into the service portal.

Exchange On-Prem (July 2025)
Refreshing the interface and integrating them in the BOBs.

Reconciliation Reporting (April 2025)
Stay informed with detailed reconciliation reports ensuring transparency and control.

Imprivata PAS Integration (April 2025)
Seamlessly manage administrative accounts within Imprivata PAS.

Workflow Troubleshooting (April 2025)
Pause and restart a specific workflow to support debugging. and avoid downtime of target systems.

COMING INNOVATION

Expanded Healthcare Integrations
Adding user provisioning into EPIC, as well as interfaces for Meierhofer KIS, 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.

NTFS Integration into BOBs
NTFS Integration into BOBs and new integrated reporting.

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.


imprivata®