Imprivata Product Roadmap: Recent Releases and Upcoming Innovation

Publish Date: January 9, 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

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

Enterprise Access Management
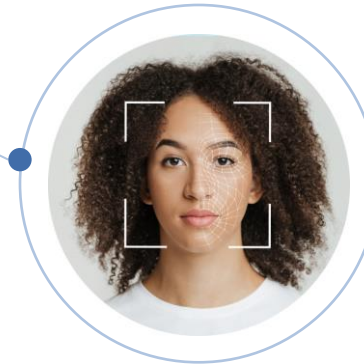
Access Compliance

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) 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

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)
Secure offline multi-factor authentication (MFA) using Imprivata ID to assist remote workers in critical situations, such as traveling healthcare professionals or for frontline personnel, like police officers in remote areas without internet access.

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

Biometric consent on behalf of the employer (Jan. 2026)
EAM can obtain employee biometric consent on behalf of the employer for the use of face recognition to comply with regulations governing the use and storage of facial biometric data.

Badge tap + Face Auth. on Shared workstations (Oct. 2025)
'Tap and smile' access to shared Windows workstations through proximity badge tap combined with face recognition as 2nd factor. Eliminates routine password entry at shared workstations while preserving strong assurance.

Integration with Epic Monitor (Oct. 2025)
Enables clinicians to tap their badge on a digital monitor in the patient room and present a user specific Epic dashboard. This can replace the in-room whiteboard.

Island browser support (Oct. 2025)
SSO for the Island browser, which is designed to be more secure and controlled centrally by an organization.

COMING INNOVATION

Risk-based Authentication for Desktop Access, Self-service Password Reset, Web SSO and other workflows
Will continuously evaluate risk signals such as user behavior, context, and location for EAM to apply stronger authentication when risk is elevated. This reduces unnecessary friction for trusted users while helping prevent account takeover, and meet compliance requirements, for a consistent, zero-trust-aligned access experience.

ID verification for self-service account recovery and password reset
Will let users authenticate by scanning a government-issued ID, which is automatically validated for authenticity and matched to the requester. By verifying a user's identity before recovery actions are completed, organizations can significantly reduce the risk of social engineering and account takeover while minimizing help desk costs.

Appliance hosted in AWS, Google Cloud, and OpenShift
Will enable hosting Imprivata appliances on AWS, Google Compute Engine, and RedHat OpenShift for enhanced selection and adaptability in infrastructure options.

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 remote access
Enable application access for remote users by replacing the need for traditional VPN connections. Enhanced security with fine-grained role-based access control.

Support for Microsoft Authenticator App within EPCS solution
Will enable the use of the Microsoft Authenticator app as a TOTP app for EPCS by allowing users to manually type in the Authenticator token code.

Streamlined workflows for national access in England and France
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.

Mobile Access Management

imprivata®
Roadmap Update

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**

RECENTLY RELEASED

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.

German language support (December 2025)
MAM will be able to support German language 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.

Simplify deployment of new Launchpads and Smarthubs (September 2025)
Automatically configure badge readers with Enterprise Access Management to quickly enable check out workflows.

View, Cancel, and Audit Bulk Operations (September 2025)
Provide visibility and actionability to bulk operations workflows

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

Improved admin permissions for large organizations (June 2025)
Admins can have unique user roles and permissions at different levels of an organization.

Personalized lock screen with Express Check Out (June 2025)
A personalized lock screen enables quick identification of device users while promoting accountability.

More intuitive display for Check In and Check Out (March 2025)
Introducing a Launchpad display for our clinical users to improve end user satisfaction and success rates while checking in and out mobile devices.

COMING INNOVATION

Improved visibility of device status for department managers
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.

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

Support for MSAL sign-in
MAM will support the ability to sign in to apps that support MSAL.

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.

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

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

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.

Support for new Android applications (June 2025)
Recent highlights include support for BetsMate and Infor Factory Track.

Configure device status based on charging (March 2025)
Admins can configure whether devices lock and/or logout when charging to streamline workflow and promote security.

Support for additional Android Devices (March 2025)
Recent highlights include various HMD devices, Honeywell CT37, and Samsung S25 Ultra

COMING INNOVATION

Epic Server side log out
MDA will log out of the Epic Server after user

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

Support "badge free" workflow with facial recognition
MDA will support facial recognition when users are accessing their device, in place of a PIN

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

Support for user to enter SIM card PIN
Ability for users to authenticate with their SIM card PIN

Customized lock screen
A customized lock screen can be set across devices

Support clock display on lock screen
A clock display lock screen can be set across devices

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

Support for MSAL sign-in
MDA will support the ability to sign in to apps that support MSAL

Support for Desfire
MDA will supports authentication for organizations using Desfire badges

Patient Access

Roadmap Update

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

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

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, supporting accurate care delivery and promoting patient safety.

ID Verification for Self-Service Enrollment into Patient Access (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.

Leverage Existing Epic Photos 'Magic Enrollment' (June 2025)
Streamlines the enrollment process by leveraging existing patient photos from Epic. This capability eliminates the need for in-person enrollment, enables instant access, and significantly enhances operational efficiency, thereby delivering faster time to value.

Reporting By Location (June 2025)
Organizes Patient Access reports by location to help admins and managers understand usage at a more granular level. Activity data by location is available to view in a new informative dashboard.

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.

Enrollment Utilization
Gain visibility into the number of patients actively enrolled in Patient Access to better understand utilization.

Re-enrollment Workflow
Enables registrars to easily overwrite existing enrollments photos and quickly create new enrollments for patients.

Magic Enrollment Notification
Adds prompt to notify a Registrar that a patient was enrolled via Magic Enrollment (Epic photo import) the first time they are verified.

Remove Photo Scoring from Registrar UI
Simplifies the photo capture process by replacing numeric scores and three-color indicators with a clear green (pass) or red (fail) result.

8

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

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.

Investigation List (March 2025)
New Bulk Actions and customizable Views on "Investigation List" page, replacing all functionality on classic screens.

COMING INNOVATION

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

Report Portfolios
Create predefined groups of audit reports to run and export results asynchronously.

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

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

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.

Investigation List (March 2025)
New Bulk Actions and customizable Views on "Investigation List" page, replacing all functionality on classic screens.

COMING INNOVATION

Report Portfolios
Create predefined groups of audit reports to run and export results asynchronously.

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

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.

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

Endpoint Discovery (December 2025)
Automated discovery of endpoints through recurring tasks for easy addition to Privileged Access.

HTML5 Client & Audit Playback (September 2025)
Deliver seamless, high-performance RDP and SSH access and audit playback directly in the browser—no Connection Manager, downloads, or external tools required.

Device Posture Check Configuration (September 2025)
Enforce device posture checking and user requirements such as anti-virus, enabled updates, and enabled UAC, with new administrative controls.

Secret Unlock & Check-Out (August 2025, December 2025)
Provide users with the permission to unlock credentials to view passwords when necessary and require they complete a form to do so. Trigger automated password rotation after use to maintain credential security.

NIST Requirements included in Best Practices Checklist (August 2025)
NIST 800-53 and 800-63 requirements are now available in the best practices checklist.

Access Request Workflows for Internal Users (June 2025)
Improve control over access to privileged assets by internal users by requiring users to request approval before access is granted.

Next-Gen Connection Manager (June 2025)
The next generation of the Connection Manager provides a more reliable and faster connection experience for users.

Credential Rotation (April 2025)
Improve the security of privileged credentials by automating password rotation based on certain events or time-based triggers, powered by a new job engine. Now supports Active Directory, local Windows accounts and SSH.

COMING INNOVATION

Additional MFA Options
Provide locally authenticated users with expanded MFA options for added flexibility, including facial biometric authentication.

Privileged Account Discovery
Building upon endpoint discovery, automated discovery of privileged accounts through recurring tasks for easy addition to Privileged Access.

Secret Check-Out Approvals
Expand the unlock capabilities for secrets with check-out processes requiring forms, approvals and time limited exclusive access for credentials.

Break Glass
Ensure continued access to vaulted credentials in the event that PAM isn't available.

Imprivata ITDR Integration
Detect and respond to privileged access threats in real time to keep your most critical assets secure.

New CPAM User Interface
Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available within Customer Privileged Access Management (CPAM).

Personal Vault
Grant users the ability to store their own unique credentials in a secure enterprise vault.

11

Identity Governance and Administration (DACH)

Roadmap Update

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

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
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.

Multi-Contract Support (January 2025)
Native support for multiple employee contracts for one identity.

COMING INNOVATION

Reconciliation Alerts and Reverting
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.

NIS2 Event Registration
Use IGA Workflow to manage an NIS2 event to be sure that legal deadlines are maintained.

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.

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