



Imprivata Product Roadmap: Recent Releases and Upcoming Innovation

Publish Date : March 31, 2025





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.”

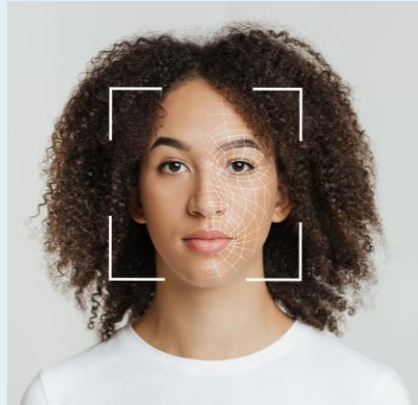
Table of Contents

Product Name	Page
<u>Enterprise Access Management</u>	5
<u>Mobile Access Management</u>	6
<u>Mobile Device Access</u>	7
<u>Patient Access</u>	8
<u>PatientSecure</u>	9
<u>Patient Privacy Intelligence</u>	10
<u>Drug Diversion Intelligence</u>	11
<u>Privileged Access Security</u>	12



Using digital identity to maximize productivity, security, and ROI

Imprivata Access Management



Imprivata Privileged Access Security

Clinician Access Management

Enterprise Access Management

Simple, secure access to workstations, applications, and clinical workflows

Enterprise Access Management Analytics [NEW]
SSO and user access workflow analytics to drive actionable insights

Mobile Access Management

Security, optimization, and management of shared mobile devices at scale

Mobile Device Access

Secure, real-time access to shared devices and apps

Medical Device Access

Fast, convenient access to connected medical devices

Patient Access

Patient Access

Touchless **facial [NEW]** and **palm vein** recognition to improve patient safety and experience

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

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

Customer Privileged Access Management

Enterprise remote support for service providers and technology vendors

Enterprise Access Management

(formerly OneSign and Confirm ID)

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 login to single-user Windows PCs (April 2025)

Secure and frictionless access login to single-user Windows desktops using facial recognition.

Enhanced self-service password reset (April 2025)

Adds SMS as an authentication factor for self-service password resets. This enhances security around user credentials and reduces reliance on security questions.

Entra ID only joined devices for hybrid directory architectures (April 2025)

Benefits customers who want to take advantage of Entra ID features, such as auto provisioning and remote device provisioning, but are not ready to migrate off Active Directory. Support is limited to Entra ID only joined devices within hybrid environments.

Faster Imprivata Analytics for EAM (March 2025)

Imprivata Analytics customers can now receive near-real-time EAM data, expediting issue detection and response and reducing impact.

Android support for Mobile EPCS (December 2024)

Extends the use of facial biometrics for EPCS signing from a mobile device (via Epic Haiku and Canto) to Android devices, giving providers more flexibility when prescribing controlled substances.

Azure Virtual Desktops for user access (November 2024)

EAM integrates with AVD on Windows for both single-user desktops and shared workstations (kiosks), enabling seamless badge-tap access to roaming AVD desktops.

COMING INNOVATION

Passwordless Multifactor Authentication (MFA) login enhancements

Secure and frictionless access by adding a device-bound passkey leveraging the trusted platform module (TPM) in Windows 10 and Windows 11 devices to the facial biometrics.

Facial Recognition as an Authentication Factor in SSPR

Will provide a fast and secure way to authenticate that is phishing resistant to reset passwords and regain access to critical systems.

Passwordless desktop EPCS with face recognition

Will provide DEA-compliant face recognition for e-prescribing controlled substances.

Tap and go and EPCS on shared Mac computers

Imprivata agent for tap and go, and EPCS signing, on shared macOS computers. Will leverage native macOS account management for reduced overhead and will add passwordless SSO to Epic and Citrix Storefront apps.

MFA for access to offline computers

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

Integration with Epic Monitor

Enable clinicians to tap their badge on a digital monitor in the patient room, presenting a user specific Epic dashboard, often replacing the in-room whiteboard.

NHS England Care Identity Service 2 modern authentication support

Native EAM integration with the new NHS Care Identity Service 2 (CIS2), delivering simplified NHS Spine access and streamlined clinical workflows on the new, replacement Spine service.

Compliance with new PHI security policy in France

High assurance level authentication and SSO for applications integrated with Pro Santé Connect, a French centralizing authority for identity providers.

Appliance in AWS and Google Cloud

Enables hosting Imprivata appliances on AWS and Google Compute Engine, offering customers enhanced selection and adaptability in their infrastructure options. 5

Mobile Access Management

(formerly GroundControl)

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](#)

RECENTLY RELEASED

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.

Comprehensive analytics (March 2025)

Improve reporting and analytics for with more data, customizable dashboards and proactive issue detection.

Support for additional Android Devices (March 2025)

Recent highlights include various HMD devices, Honeywell CT37, and Samsung S25 Ultra

Support for additional mobile apps (March 2025)

Recent highlights include various iProcedures iPro Anesthesia and Tissue Analytics

Simplify Launchpad management and configurations (January 2025)

Develop organization specific, pre-configured Launchpad installations to remove the need for manual configuration.

Faster Check Out experience for iOS devices (January 2025)

Improve the time it takes to check out a device for end users

Streamlined MFA workflow for checked out iPhones (August 2024)

Users are now prompted for their password or Imprivata PIN immediately when checking out a device to avoid additional steps when accessing applications

Support for additional Android Devices (August 2024)

Recent highlights include Samsung A15 and Samsung xCover 6 Pro

Simplified device refreshes, at scale (August 2024)

Support the bulk erasure and retiring of devices for faster time to value with device refreshes.

Native Epic Rover Logout (May 2024)

Update a user's presence status in Epic when devices are checked in to eliminate irrelevant alerts sent to checked in 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 device check out

'Tap and Smile' with facial biometrics for passwordless multi-factor authentication when checking out a device.

Improved admin permissions for large organizations

Admins can have unique user roles and permissions at different levels of an organization.

Improve Usability of the Dashboard

Improvements to help MAM administrators understand where issues are that need their attention as well as recommendations for manual interactions.

Smart Folders for personalized Launchpad list

Dynamically updated Launchpad folders that give console users a clear and focused view of the locations they manage.

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

Simplify deployment of new Launchpads and Smarthubs

Automatically configure badge readers with Enterprise Access Management to quickly enable check out workflows.

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**

RECENTLY RELEASED

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

Support for additional mobile apps (March 2025)

Recent highlights include various iProcedures iPro Anesthesia and Tissue Analytics

Deliver consistent workflows regardless of connectivity (December 2024)

Support for "offline mode" to enable device access when there is no network connectivity.

Support for new Android devices and applications (December 2024)

Recent highlights include integration with Zebra HC20 devices as well as support for Navenio and British National Formulary applications.

Support for new Android devices and applications (August 2024)

Recent device highlights include integration with Samsung A15, Samsung xCover Pro, various Google Pixel model, and Honeywell CT60. We've also introduced support for new applications such as Zebra Workcloud Connect, Manhattan Active, Diktamen, Nordic Health Group, and more.

Enable secure access for more environments and use cases (May 2024)

Support for Android workstations and devices with external badge readers.

Mobile Device Access Analytics through EAM Analytics Platform (May 2024)

Robust analytics capabilities provide unparalleled visibility into user access workflows across your shared mobile devices environments to drive actionable insights, remediate security gaps, and reduce operational burden and IT overhead.

COMING INNOVATION

Understand application usage with enhanced analytics

Customers can report on user authentications to applications.

Passwordless device check out

Customers can use facial biometrics for passwordless multifactor authentication when assigning out a device.

Passwordless device unlock

Customers can unlock an assigned device with facial biometrics.

Support for MSAL sign-in

MDA will support the ability to sign in to apps that support MSAL

Support for FIDO Badges

MDA will support authenticating to a device using a FIDO Badge

[Click here for more information](#)

[Return to Portfolio slide](#)

Patient Access

(formerly Imprivata Biometric Patient Identity)

Overview

Designed with privacy in mind, Imprivata Patient Access is a facial recognition solution that enhances patient safety and experience by streamlining check-ins and accurately linking patients to their medical records with a single photo, helping to ensure efficient and error-free healthcare delivery.

- **Improved patient identification accuracy**
- **Enhanced patient safety and experience**
- **Streamlined registrar workflows**
- **Flexible hardware**
- **Seamlessly integrated with Epic**

RECENTLY RELEASED

Self-Service Identification (March 2025)

With integration into Epic Welcome kiosks, patients can identify themselves, significantly easing the workload on registrars and speeding up the check-in process. Strengthened security measures with enhanced liveness and spoof detection capabilities, helping to ensure that the system is interacting with a real person and not a fraudulent representation.

Data Retention Controls (February 2025)

Introducing the ability for customers to set data retention controls to help support compliance with pertinent biometric privacy regulations.

Duplicate Proofing (December 2024)

As an extra safeguard to help prevent misidentification errors, Imprivata Patient Access will help ensure that each face is enrolled only once. (Allows for the enrollment of identical twins.) This critical feature helps maintain a one-to-one match between a patient and their medical record.

Configurable Enrollment Age (October 2024)

Tailor the patient enrollment experience by setting a minimum age for eligibility in healthcare facilities, helping ensure alignment with compliance and patient care standards.

Two-Factor Authentication with Imprivata ID for Patient Access Admin UI (October 2024)

Added ability to require Imprivata ID as a second factor of authentication when logging into the Patient Access Admin Console to further protect PHI.

Image Refinement for Patient Privacy (June 2024)

Improve how images are displayed by cropping backgrounds, focusing solely on the patient to protect privacy and improve the clarity of identification photos.

COMING INNOVATION

Self-Service Enrollment into Patient Access

This feature enables patients to enroll in Patient Access (without a registrar) so that when they return for future visits, they can streamline their check-ins by checking in via Patient Access at a kiosk or registrar.

ID Proofing for Self-Service Enrollment into Patient Access

For a patient self-enrolling in Patient Access (without a registrar), ID proofing verifies the patient's identity to offer increased confidence that the patient enrolling is who they say they are.

Reporting By Location

Patient Access reports will be organized by location which will help admins and managers understand usage at a more granular level. Activity data by location will be available to view in a new informative dashboard.

Patient Access Integration with Imprivata Access Management Portal

Customers will be able to access their Imprivata products through a single portal, streamlining the log in experience for users.

Enrollment Photo Updates at Authentication

This will allow registrars to update enrollment photos if they notice significant appearance changes or elapsed time since enrollment. This will help maintain accuracy.

Support for Multiple Patient Identifiers

Allows healthcare organizations to display various patient identifiers, ensuring registrars can use the ones they are most familiar with for their tasks.

[Click here for more information](#)

[Return to Portfolio slide](#)

PatientSecure

Overview

Imprivata PatientSecure uses palm vein biometric identification to accurately and securely identify patients, reducing identity errors, preventing fraud, and improving workflow efficiency across healthcare systems. This touchless authentication solution ensures positive patient identification at any point of care, enhancing patient safety and satisfaction.

- **Accurate Patient Identification**
- **Enhanced Patient Safety**
- **Fraud Prevention**
- **Workflow Optimization**

RECENTLY RELEASED

Improve Admin Console Experience (January 2025)

Admin console will display frequently performed actions front and center for quick access and streamlined workflows.

System Health Dashboard Enhancements (January 2025)

System Health Dashboard now provides status and/or alerts about additional system components to help keep PatientSecure running smoothly.

Epic Welcome Kiosk Integration Language and Date Enhancements (September 2024)

Language support additions - Our customers serve diverse patient populations who speak many languages. PatientSecure's integration with Epic kiosk gives patients a better check-in experience by expanding language support to include French, Arabic, Korean, Chinese, Haitian Creole and Bengali.

Location date format setting - PatientSecure presents date formats according to the language selected at the kiosk. Now customers have the option for the PatientSecure date format to remain consistent with Epic.

Parallel PatientSecure and Imprivata Patient Access (September 2024)

Epic customers will be able to run either PatientSecure (Palm Vein) or Imprivata Patient Access (Facial) at each point of registration.

Display Patient's Preferred Name for Improved Patient Experience (May 2024)

Allows for a more personal patient check-in experience.

Scheduled Reporting Enhancements (May 2024)

We have added an option to email a notification regarding the outcome of a scheduled report. When a scheduled report fails, PatientSecure provides the option to re-run the report using the original parameters.

COMING INNOVATION

Notification when Left Palm is Detected

While the palm vein scanner will work well with either hand, consistent presentation of the same hand is required to authenticate patients. For consistency and patient comfort, the best practice guideline is to enroll and authenticate the right hand unless the right hand is permanently unavailable. This feature notifies the registrar when a left hand is being scanned to minimize the chance of left-hand scans.

Registrar Control to Start Scan Option

Adding the option for registrars to control the start of the enrollment scan capture to allow time to instruct the patient on hand placement.

Enrollment Quality Visibility and Reporting

PatientSecure will now provide an enrollment quality score to help troubleshoot issues like inconsistent authentication.

Opt-Out Workflow Enhancements Streamlines Workflows with:

- Consistent language
- Understanding of patient-driven versus registrar-driven causes
- More opt-out reasons allowed
- More prominent last opt-out information at verification and enrollment

Collect Product Analytics for Key Product Functions

This feature will time key product functions to help customers understand performance.

Patient Privacy Intelligence

(formerly FairWarning)

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

Investigation List (March 2025)

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

Dashboard Library (December 2024)

Enhance user and analyst workflows with the ability to install best practice dashboards for application monitoring with a single click.

Imprivata Cloud Portal (ICP) Integration (December 2024)

Streamline user experience by providing a holistic Imprivata Cloud Platform.

Internationalization of Machine Learning Closing Model (August 2024)

Availability of our full-feature set of machine learning to our international customers for optimized internal access auditing.

First Access Reporting (July 2024)

Allows customers to build custom reports on First Access data with scores and explanations for enhanced auditing functionality.

Auto-Disabled End User Accounts (May 2024)

Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)

Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

COMING INNOVATION

Unified Patient Privacy Intelligence Model

Optimize risk identification, advancing anomalous workflow model and establishing a foundation for UEBA model expansion.

SailPoint Integration

Leverage an API integration with SailPoint to launch a workflow upon the creation of an alert in PPI.

User Notifier/First Time Offender workflows

Expand upon the current "Delegated Incident Review" workflow to include auto-provisioning of users (managers, end users, etc.), use of updated memo templates, identification of first-time and repeat offenders, and enhanced governance reporting.

Report Results – Details & Access Reports

Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

Redesigned Report Builder

All new user interface for the application's report builder, improving performance and enhancing ease of use.

VIP / Watchlist

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

Drug Diversion Intelligence

(formerly FairWarning)

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

RECENTLY RELEASED

Investigation List (March 2025)

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

Dashboard Library (December 2024)

Enhance user and analyst workflows with the ability to install best practice dashboards for application monitoring with a single click.

Imprivata Cloud Portal (ICP) Integration (December 2024)

Streamline user experience by providing a holistic Imprivata Cloud Platform.

User-Based Risk Model & AI Configuration (August 2024)

Streamline users and analyst workflows with the power of AI, providing the ability to rank users with peer clustering to determine which users present the most risk.

Device Cluster Management (June 2024)

Discover trends within users and potential anomalies for diversion mitigation through the ability to set defined peer groups.

Auto-Disabled End User Accounts (May 2024)

Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)

Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

COMING INNOVATION

High Risk User Monitoring

Leveraging One ID technology and our UEBA anomaly detection, monitor your high-risk users on your dashboard and immediately investigate.

SailPoint Integration

Leverage an API integration with SailPoint to launch a workflow upon the creation of an alert in DII.

User Notifier/First Time Offender workflows

Expand upon the current "Delegated Incident Review" workflow to include auto-provisioning of users (managers, end users, etc.), use of updated memo templates, identification of first-time and repeat offenders, and enhanced governance reporting.

Report Results – Details & Access Reports

Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

Redesigned Report Builder

All new user interface for the application's report builder, improving performance and enhancing ease of use.

VIP / Watchlist

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

User Risk Dashboard Workflow

Monitor high risk users, drill into access details, and open an investigation from a configurable dashboard widget.

Privileged Access Security

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

Overview

Imprivata's Privileged Access Security 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

New VPAM User Interface (January 2025)

Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available within [Vendor Privileged Access Management](#) (VPAM).

Next-Gen Connection Manager (September 2024)

The next generation of the Connection Manager provides a more reliable and faster connection experience for users.

Containerized Network (September 2024)

Enable easy and streamlined access to users connecting to devices and thick clients with strict port requirements, such as PLCs, common in OT environments.

Improved Upgrade Process (September 2024)

Experience a faster and streamlined upgrade process that minimizes downtime and provides quicker access to new functionality and features.

Pre-Connection Notifications (May 2024)

Provide timely notifications during the connection process with application-specific information that vendor users need to know before connecting to an application.

Custom Application Access Request Forms (April 2024)

Capture custom information about access that your administrators need to make an informed decision when granting or denying access; common examples include case number or who approved access.

Access Request Reminder Notifications for Gatekeeper Admins (May 2024)

Automatically remind Gatekeeper Admins of pending requests on a configurable basis to reduce the need to reach out to remind customers and to facilitate quicker access approvals.

COMING INNOVATION

Credential Rotation & Job Engine

Improve the security around privileged credentials by automating password rotation based on certain events or time-based triggers, powered by a new job engine.

Access Request Workflows for Internal Users

Improve control over access to privileged assets by internal users by requiring users to request approval before access is granted.

Secret Unlock

Provide users with the permission to check-out and unlock credentials to view passwords for use cases where necessary – and ensure they are rotated after use to maintain credential security and peace of mind.

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).

HTML5 Client

Provide seamless and faster connectivity for users for RDP and SSH sessions directly in the browser, without the need to launch the Connection Manager.

Self-Managed Nexus Connections & Directory

Independently find, set up, enable and manage Nexus connections for vendors using Imprivata CPAM for even faster connectivity.

Additional MFA Options

Provide locally authenticated users with expanded MFA options for added flexibility.

Device Posture Check Configuration

Enforce device posture checking and user requirements such as anti-virus, enabled updates, and enabled UAC, with new administrative controls.

 **imprivata**[®]

