

Imprivata Identity Governance

Increase operational efficiency while strengthening your security posture

Designed and built exclusively for healthcare, Imprivata Identity Governance® is an end-to-end solution with precise role-based access controls, automated provisioning and de-provisioning, streamlined auditing processes, and analytics that enable faster threat evaluation and remediation.

Automate identity management, increase security

Securing and controlling access to protected health information is one of the most critical issues facing healthcare organizations today. Security incidents can disrupt patient care, while failure to comply with HIPAA privacy and security regulations can result in financial and criminal penalties.

In response, healthcare organizations are implementing corporate governance, risk management, and compliance solutions that contain more secure and auditable controls as well as improvements to the monitoring and remediation of threats.

Imprivata Identity Governance automates the identity management process and empowers care providers to deliver high-quality care in a secure and compliant manner. Imprivata Identity Governance helps drive faster time to value through:

- Strategic integrations with leading EHR systems including Epic, Cerner, MEDITECH, and others to seamlessly automate the provisioning, management, and deprovisioning of provider identities
- API-level integration with healthcare applications and support for non-API-level integration using Imprivata Bridge Studio, a drag and drop interface, to easily add automation
- Integrations with Imprivata OneSign®, Imprivata Confirm ID®, and Imprivata Privileged Access Management to accelerate role development, monitor digital identities, and reduce risk.
- Healthcare-specific governance, risk, and compliance modules with prebuilt reporting, allowing an organization to easily bring its user attestation/periodic access review program to 100% compliance

With solutions and services from a single, trusted, and responsive vendor, you can automate identity management in months, not years.

Benefits

- Reduce IT costs by automating the identity management process
- Strengthen data security across the entire organization
- Empower care providers to deliver high-quality care with role-based, timely access to the right systems
- Deploy on-premises or host in an Azure environment for greater flexibility and scalability

Handle privileged accounts with confidence

Cybersecurity threats are becoming increasingly sophisticated, leading to a shift in the identity management industry and to the convergence of three pillars: identity management, access governance, and privileged access management. Imprivata offers a comprehensive platform that incorporates these three pillars.

With Imprivata Identity Governance, users are assigned roles and provisioned access to Active Directory, email, and applications. Some roles – such as a system admin or domain admin – require privileged access. Combining Imprivata Identity Governance with Imprivata Privileged Access Management means that these admin users can be provisioned directly into that privileged Active Directory group and other systems. So, from “day one,” users will have their privileged access, and have that access monitored through a privileged access management (PAM) solution. This is a critical combination for keeping controls and visibility over users who have broad access to sensitive information.

With an integrated identity governance, single sign-on, multifactor authentication, and PAM solution, organizations can take a unified approach to identity access — securely managing all user identities while easily meeting regulatory requirements.

Imprivata Identity Governance integrations

Imprivata Identity Governance integrates with the applications integral to healthcare delivery organizations.

INTEGRATION WITH LEADING EHRS

For healthcare organizations, the electronic health record system is one of the most critical applications for clinicians to be able to access on day one. Imprivata Identity Governance has been successfully automating provisioning processes for leading EHR solutions including Epic, Cerner, MEDITECH, and others, for decades. With that experience, Imprivata has standardized the integration approach so that health systems are able to seamlessly automate the provisioning, management, and deprovisioning of provider identities and achieve faster ROI. Where possible, Imprivata leverages available APIs to integrate with EHRs, allowing for faster implementation and tight security protocols.

“ The amount of time that we’re saving creating accounts is priceless. ”

Ana Agostini, Administrative Director of IT Services, Memorial Healthcare System

“ We have issued periodic access reviews every quarter. It’s very easy to use and we get 100% compliance every time — and we’re talking about sending it to over 700 plus leaders throughout the organization. For them to validate the access that their employees have, for the right applications and in very short time, it’s sound governance. ”

VP of IT, large healthcare delivery organization

INTEGRATION WITH IMPRIVATA ONESIGN, IMPRIVATA CONFIRM ID, AND IMPRIVATA PRIVILEGED ACCESS MANAGEMENT

Using Imprivata Identity Governance with Imprivata OneSign, Imprivata Confirm ID, and Imprivata Privileged Access Management will provide an integrated solution suite that – more than any other identity governance solution – will further reduce IT costs, improve data security, and shift the focus to quality patient care: exactly where it should be. Specifically, the benefits of Imprivata Identity Governance integration with Imprivata OneSign, Imprivata Confirm ID, and Imprivata Privileged Access Management include the following:

- **An improved security and a near-passwordless end user experience:** Imprivata Identity Governance automatically stores application credentials into Imprivata OneSign, eliminating the need for users to ever enter new credentials. Application credentials do not need to be delivered to users via email or on printed slips of paper and will never be seen by another individual in the organization.
- **Role reconciliation** for role discovery, optimization, and risk assessment: Imprivata Identity Governance can analyze report information from Imprivata OneSign to automatically determine which users have access to particular applications. This information allows administrators to assess the proper scope of application entitlements, establishing new roles and reconciling existing ones.
- **License optimization** and management: By identifying users' existing access to applications from Imprivata OneSign reports, Imprivata Identity Governance can determine appropriate application license needs and usage.
- **Automation of the electronic prescribing for controlled substances (EPCS) onboarding process:** As providers are approved for EPCS privileges, Imprivata Identity Governance will automatically assign the user to an appropriate user policy enabling enrollment within EPCS as well as provide notification to the provider.
- **Manage privileged and non-human identities** without increasing the risk of privileged access abuse. Privileged access to backend systems and servers is easily and securely granted to IT admin and external vendor/contractor users through Imprivata Privileged Access Management. This is a critical combination for keeping controls and visibility over users, who have broad access to sensitive information, and eliminating redundant processes for privileged and non-privileged accounts.
- **Extend current homegrown or legacy identity management solutions** for clinical provisioning. Imprivata Identity Governance can be deployed side-by-side with an existing identity solution, such as Microsoft Identity Manager, to address the gaps in managing clinical and legacy applications.

“ With Imprivata Identity Governance in place, we’ve seen huge time savings due to the reduction of manual processes, and we’ve ensured that clinicians receive fast and secure access to applications and systems. ”

Shawn McCrum, Manager of Identity and Access Management, Northern Light Health

“ The role of the CIO is to remove the hassle, burden and overhead of security so that clinicians, for example, can be in the moment. We need to give them the right tools to make doing the right thing from a security standpoint easier than not doing the right thing. Once we do that, the whole organization will be just as security conscious as we are. ”

Chris Paravate, CIO, Northeast Georgia Health System

See and remediate risk in seconds

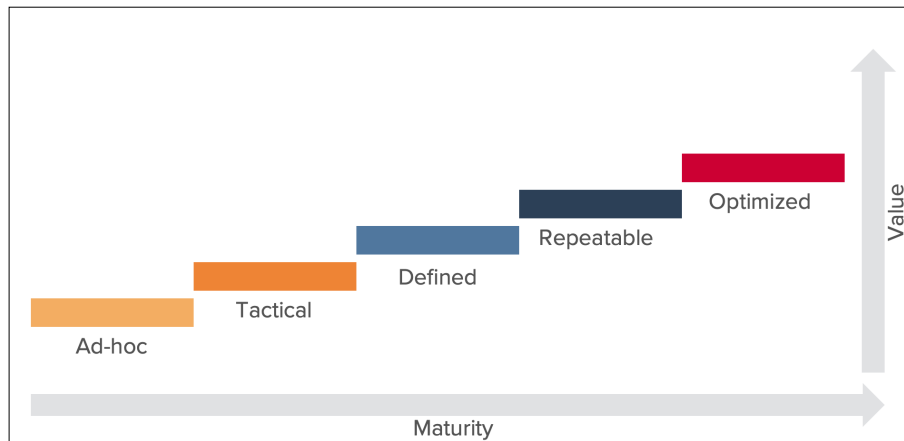
Digital identities can be compromised in the blink of an eye, so health IT security leaders need to be faster than that. The Identity Governance risk dashboard provides access to a customized view of reports and graphs that enables an administrator to spot a risk and immediately take action to remediate it.

Below is a sample of out-of-the-box reports that can be generated in Imprivata Identity Governance:

| Report name | Description |
|---|---|
| Role based application access statistics | Compare default applications in an identity governance role with corresponding users' Imprivata OneSign access data to refine default role assignments and eliminate over-assignment during on-boarding |
| Unauthorized application accounts | Compare user's Imprivata OneSign application access with their identity governance-assigned applications to determine any unauthorized access granted outside of Imprivata Identity Governance |
| AD reconciliation report | Lists all changes synced from Active Directory that did not originate from Imprivata Identity Governance |
| Out of role report | Identify users who have additional access beyond their role or are not in a defined role |
| User entitlement report | User application and entitlements, primarily used for periodic access reviews |
| Orphaned accounts | Lists users whose AD accounts have been disabled but certain application accounts are still enabled |
| Active accounts by application | Identity governance-managed application accounts that are active for licensing purpose for respective applications |
| Expiring users | Finds users who are about to expire or are expired |

A partnership for the journey

Sustaining and increasing benefits from healthcare organizations' investment in identity governance and administration solutions can be challenging; projects can stall, champions can change, and ecosystems are constantly evolving. Imprivata has developed a phased [maturity model](#) with criteria and metrics to assess operational and governance status and keep projects on track. Our team will continue to work with you to ensure you are getting value out of your Imprivata investments.



Imprivata identity governance maturity model

Imprivata solution portfolio

Imprivata solutions are purpose-built to meet healthcare's unique security and workflow challenges. Imprivata Identity Governance delivers end-to-end provisioning, role-based access and integrated governance and compliance. Combined with the benefits of other Imprivata solutions, such as ubiquitous single sign-on, seamless multifactor authentication, and privileged access management, healthcare organizations can confidently secure and manage digital identities across their ecosystems.



Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

Copyright © 2021 Imprivata, Inc. All rights reserved. Imprivata, OneSign, Identity Governance, and Confirm ID are registered trademarks of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.