imprivata®

Imprivata Identity Governance

Fast, secure role-based access to systems and applications

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

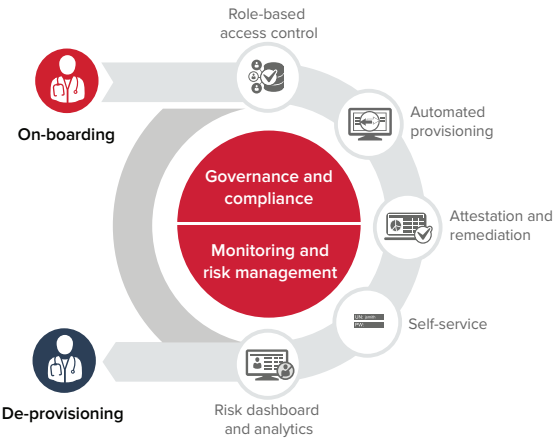
Designed and built exclusively for healthcare, Imprivata Identity Governance® is an end-to-end solution with precise role-based access controls, automated provisioning and de-provisioning, streamlined auditing processes, and analytics that enable faster threat evaluation and remediation.

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:

- Reduces IT costs by replacing burdensome, slow, and error-prone manual administering of user accounts while ensuring a high standard of security through efficient identity creation and termination
- Strengthens data security by streamlining auditing processes and providing compliance teams with rights and usage data in a single comprehensive report
- Empowers care providers to deliver high-quality care while increasing their productivity by ensuring correct, timely access



About Imprivata

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 further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

Key features of Imprivata Identity Governance

Deployment options for hybrid healthcare environments

Implement on-premises or in your Azure tenant, leverage the security and scalability of your Azure platform, and reduce on-premises administration and overhead costs.

Same-day access rights to clinical systems

Care providers can access key clinical systems – from their first day at the organization to their last.

Self-service portal

Users can update their passwords and request additional application access quickly, without IT involvement.

Access and entitlement enforcement

IT and department heads can manage identity roles and entitlements over the lifecycle of a user, with workflow capabilities that allow for certification and remediation of access and entitlement rights.

Easy to use role management and configuration

Users can easily select, copy and make bulk edits to roles, streamlining the role management process. Application configuration is as simple as point and click.

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

Governance, risk management, and compliance dashboard

Compliance teams and security analysts can view complete user behavior and entitlements in reports that combine rights and usage data. The table below shows select examples of out-of-the-box reports.