imprivata®

Trusted digital identities: Healthcare's new security perimeter

Healthcare is in the midst of a digital transformation, creating information security, compliance, and workflow challenges. The proliferation of cloud-based applications, databases, and mobile devices, as well as an increasingly decentralized workforce, have eroded the once well-defined network perimeter. Going forward, healthcare organizations must focus on establishing and managing trusted digital identities for all users, applications, and devices throughout the entire extended digital healthcare enterprise – from the hospital, to the cloud, and beyond.

General-purpose security products designed to protect conventional infrastructure and applications aren't well suited for the digital era. Forward-looking organizations are turning to healthcare-centric, integrated identity and access management (IAM) solutions to address the unique security and workflow requirements of today's dynamic healthcare enterprises. By establishing, monitoring, and maintaining trusted digital identities across the diverse care delivery environment, healthcare-centric IAM solutions help organizations ensure the right people only have access to the data and applications they should, optimize processes, reduce security vulnerabilities, and improve compliance.

This paper reviews healthcare IT trends, explains some of the challenges digital transformation creates for healthcare IT and security leaders, and describes the capabilities and benefits of the Imprivata IAM solution portfolio. Imprivata delivers end-to-end provisioning, seamless multifactor authentication, role-based access controls, ubiquitous single sign-on, and integrated governance and compliance to establish, secure, and manage trusted digital identities across the entire healthcare ecosystem. The comprehensive solution forms trusted digital identities for clinicians, administrators, patients, endpoints, and connected medical devices, and ensures all users have access to the applications and information they need, anytime and anywhere they need it, using any device.

Digital transformation creates unique security challenges for healthcare IT

Digital transformation and the shift to value-based care are fundamentally reshaping healthcare IT. Today's care delivery ecosystem is no longer confined to the four walls of the hospital. In this constantly evolving digital era, healthcare professionals need access to applications and information anywhere, anytime, and from any device.

The modern healthcare enterprise includes an increasingly wider variety of:

- Users and roles – nurses, doctors (including those employed by the organization as well as affiliated and referring physicians), residents, students, contractors, vendors, business, and IT professionals
- Devices – traditional workstations and virtual desktops, shared mobile devices and workstations, personal devices, and connected medical devices
- Applications and service delivery models – on-premises, cloud, and hybrid

Yet many healthcare organizations still rely on general-purpose security solutions and point products designed to protect traditional applications and on-prem infrastructure. These disjointed security solutions and practices can introduce security gaps and disrupt the delivery of care. Healthcare professionals are forced to remember distinct user IDs and passwords, or carry multiple security tokens to access different applications, frustrating users and hampering technology adoption. And manually intensive and error-prone administrative processes impair IT agility and add risk.

To make the most of digital transformation investments, healthcare IT and security planners must find innovative ways to establish digital trust and protect today's diverse and dynamic IT environments, without impeding workflows or complicating operations. Organizations must create trusted digital identities across a complex network of people, technology, and information. By focusing on a trusted digital identity, healthcare enterprises can optimize processes and technologies to solve critical workflow, security, and compliance challenges.

To make the most of digital transformation investments, healthcare IT and security planners must find innovative ways to establish digital trust and protect today's diverse and dynamic IT environments, without impeding workflows or complicating operations.

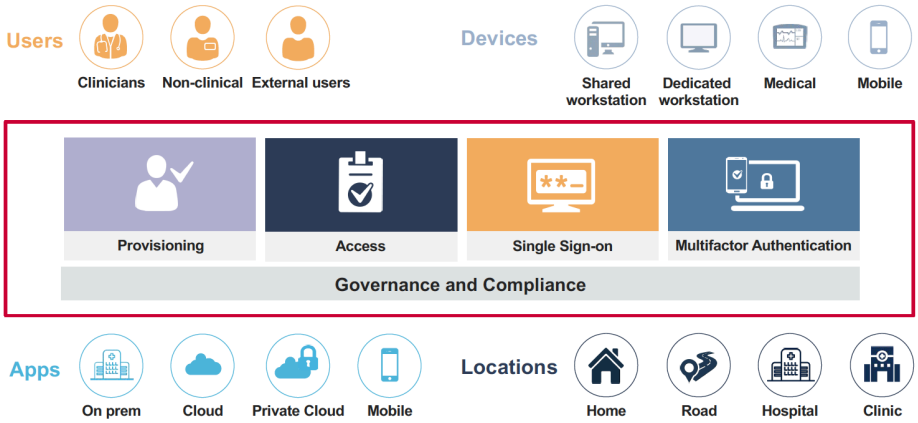
Imprivata solutions are tailor-made for healthcare

Imprivata IAM solutions are designed from the ground up to meet the unique security, compliance, and workflow challenges of the modern healthcare enterprise. Unlike general-purpose security solutions and point products, the Imprivata product family was specifically conceived and built for healthcare, with on-staff, practicing clinicians providing guidance and recommendations every step of the way. By establishing trusted digital identities, Imprivata solutions enable efficient, secure, and compliant access to the systems, applications, and data that providers need to deliver quality care.

Delivered and supported by a single technology partner, Imprivata solutions natively integrate with a wide range of healthcare devices and applications including shared mobile devices, interconnected medical devices, EHRs, and other clinical applications. The comprehensive solution provides unified security and consistent user experiences across devices and locations for ultimate efficiency and protection.

Imprivata IAM solutions give users fast and convenient access to a wide variety of healthcare endpoints including workstations, virtual desktops, mobile devices, and smart medical devices.

End-to-end provisioning, seamless multifactor authentication, role-based access controls, universal single sign-on, and integrated governance and compliance capabilities let IT and security professionals effectively establish, safeguard and manage trusted digital identities across the extended healthcare enterprise.



End-to-end provisioning

Imprivata IAM solutions automate all the administrative processes associated with on-boarding, tracking and removing users, and provisioning access privileges. Imprivata solutions eliminate manually intensive, error-prone, and time-consuming administrative processes ensuring that clinicians and hospital workers have secure access to critical healthcare applications and IT systems on day one. These solutions support role-based access controls to tightly align entitlements with job functions, eliminating privilege creep and orphaned accounts when users change roles or leave jobs. They integrate with major EHRs and other healthcare applications to accelerate time-to-value and streamline workflows, and support EPCS identity-proofing to enable compliance with DEA regulations.

Seamless multifactor authentication

Imprivata IAM solutions support seamless multifactor authentication, ensuring consistent and transparent user experiences across devices, applications, and locations. The product family supports a variety of authentication methods (push token, fingerprint biometrics, hands-free authentication, etc.) to accommodate various users, roles, and workflows.

Fast and convenient access
Imprivata IAM solutions give users fast and convenient access to a wide variety of healthcare endpoints including workstations, virtual desktops, mobile devices, and smart medical devices. The portfolio supports fast user-switching on shared mobile devices and shared workstations to streamline access, while protecting PHI.

It also supports an innovative proximity-based, secure walkaway capability that automatically logs off users and seamlessly re-authenticates them when they return, for ultimate convenience and ease-of-use.

Universal single sign-on
Imprivata IAM solutions support universal single sign-on (SSO) without the need to rely on complex usernames and passwords. Proximity badges and fingerprint biometrics can be leveraged to quickly and securely access private or shared workstations, cloud and on-premises applications, virtual desktops, and shared mobile devices. And because Imprivata provides SSO into cloud applications from any location and from any device, healthcare organizations can drive strong security across their entire enterprise, remotely or from inside the network. A strategic partnership with Microsoft enables cloud technology adoption by delivering seamless SSO into web apps on shared workstations, streamlining the login process into thousands of web apps from the Azure Marketplace.

Governance and compliance
Imprivata IAM solutions improve compliance with the DEA's regulations for electronic prescribing of controlled substances (EPCS), HIPAA, HITECH, and other healthcare regulations with comprehensive analysis, reporting, and auditing capabilities.

The solution set includes automated identity proofing and credential enrollment to satisfy the DEA requirements for EPCS. Imprivata also provides a centralized dashboard and pre-formatted reports designed by clinical experts that make it easy to audit user activity as well as assess and remediate threats. End-to-end provisioning capabilities and policy-based access controls make it easy to manage roles and entitlements over the entire lifecycle of a user.

Imprivata helps organizations strike the necessary, but often elusive, balance between security and clinical workflow efficiency.

Imprivata IAM solutions are purpose-built to meet the unique, demanding, and constantly changing security, compliance, and workflow challenges of the modern healthcare enterprise.

Imprivata identity and access management in action

Northern Light Health, a 1,176-bed integrated health delivery system serving the state of Maine, uses Imprivata to solve its identity and access management challenges.
Specifically, Northern Light leverages Imprivata Identity Governance to automate user provisioning and give care providers immediate, role-based access to clinical applications and IT systems. The solution helps Northern Light eliminate manually intensive, error-prone administrative processes, improve clinician productivity, and reduce operating expenses.

Imprivata Identity Governance also helps the IT team accelerate onboarding and avoid privilege creep by aligning access rights with roles. When new hires are added to the HR system, they are automatically assigned a unique set of access privileges mapped to their job code.

The Northern Light information security team is also able to efficiently track user activity, and easily delete or update user accounts when employees change jobs or leave the hospital.

Once provisioned, users are then given fast, secure No Click Access to their systems and applications via Imprivata OneSign. Providers who need the ability to prescribe controlled substances electronically are also enabled in Imprivata Confirm ID to meet the DEA's specific identity proofing, credential enrollment, and two-factor authentication requirements for electronic prescribing of controlled substances (EPCS). The integrated Imprivata identity and access management solution suite helps Northern Light strengthen security, improve auditing, meet specific compliance requirements, and reduce IT costs. It also allows clinicians to focus on patient care instead of technology.

"With Imprivata, 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," says Shawn McCrum, Manager of Identity and Access Management at Northern Light.

Imprivata enables secure, seamless access: Anywhere, anytime, any device

Imprivata IAM solutions are purpose-built to meet the unique, demanding, and constantly changing security, compliance, and workflow challenges of the modern healthcare enterprise. Imprivata helps organizations strike the necessary, but often elusive, balance between security and clinical workflow efficiency across the evolving healthcare technology landscape.

Imprivata IAM solutions help IT, security, and compliance organizations:

- Establish, manage, and secure trusted digital identities across the unique, complex, and decentralized healthcare ecosystem
- Enable secure, seamless access to a wide range of applications, from any location, using a wide variety of devices and authentication methods
- Improve security and audit response with a centralized platform for continuously managing digital identities and monitoring access to devices and applications across the enterprise
- Enable end-to-end compliance with EPCS, HIPAA, HITECH, and other complex regulatory requirements without disrupting clinician workflows or impairing patient care

Say goodbye to security solutions that impede workflows and frustrate users. Imprivata healthcare-centric IAM solutions ensure all users have secure access to the applications and information they need, anytime and anywhere they need it, from any device and location.

Imprivata healthcare-centric IAM solutions ensure all users have secure access to the applications and information they need, anytime and anywhere they need it, from any device and location.

imprivata®

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

IAM-WP-New-perimeter-0220