imprivata

CHECKLIST

Passwordless readiness checklist for CIOs

Assess your organization's ability to modernize access, reduce operational complexity, lower support burden, and scale passwordless authentication across the enterprise.

For CIOs, passwordless authentication is more than a security initiative. It is an opportunity to modernize access management, simplify infrastructure, reduce tool sprawl, improve workforce productivity, and support digital transformation with a more scalable authentication strategy.

Use this checklist to evaluate your organization's readiness to move beyond password-dependent access. The questions below can help identify gaps, assess operational and technical readiness, and prioritize the areas that may require additional planning before deployment.

1. Platform consolidation and access complexity

Why this matters

The question is not whether your organization can add passwordless authentication. It is whether you can simplify the access ecosystem while improving security and user experience. Many healthcare organizations rely on separate tools for SSO, MFA, password management, remote access, identity verification, and shared workstation workflows. Over time, these disconnected solutions increase costs, administrative overhead, integration complexity, and policy inconsistency.

Readiness checklist

- [ ] Assess whether authentication and access management capabilities are fragmented across teams, workflows, or vendors.
- [ ] Identify opportunities to consolidate SSO, MFA, remote access, self-service password reset, and shared workstation authentication.
- [ ] Determine whether existing identity and access investments can support broader passwordless workflows.
- [ ] Evaluate whether access policies are consistently applied across clinical, administrative, remote, and shared environments.
- [ ] Prioritize platform consolidation opportunities that reduce complexity, avoid multi-vendor inefficiencies, and accelerate outcomes.

2. Operational efficiency and service desk burden

Why this matters

Passwords create operational costs as well as security risks. Password resets, lockouts, enrollment issues, and authentication failures consume service desk resources and divert IT teams from higher-value initiatives.

Readiness checklist

- [ ] Establish a baseline for password resets, account lockouts, failed authentication attempts, and authentication-related service desk tickets.
- [ ] Identify which user populations, departments, locations, or applications generate the highest access support burden.
- [ ] Evaluate self-service password reset and high-assurance identity verification options.
- [ ] Assess where passwordless workflows could reduce recurring support requests.
- [ ] Define success metrics such as lower ticket volume, faster issue resolution, reduced downtime, and lower support costs.

3. Workforce productivity and digital transformation

Why this matters

Authentication capabilities directly impact digital transformation. EHR optimization, mobile workflows, virtual care, shared device programs, and application adoption all depend on fast, reliable access. When access creates friction, productivity suffers and technology adoption slows.

Readiness checklist

- [ ] Identify digital transformation initiatives affected by authentication friction, including EHR optimization, virtual care, mobile workflows, shared device programs, and cloud application adoption.
- [ ] Determine where faster access would improve clinician productivity, workflow efficiency, or application adoption.
- [ ] Prioritize high-impact workflows, including shared workstations, VDI, and EHR, mobile, and remote access.
- [ ] Assess whether passwordless access can scale across multiple user groups and device types.
- [ ] Define measures for tracking clinician satisfaction, time savings, application adoption, and support reduction.

4. Scalability, integration, and infrastructure readiness

Why this matters

A passwordless strategy must be scalable across the enterprise. CIOs need to know whether the organization can support passwordless access across clinical and non-clinical users, legacy applications, shared devices, mobile devices, cloud apps, and remote environments without introducing operational risk.

Readiness checklist

- [ ] Assess integration requirements across EHRs, VDI, IAM, directories, cloud applications, and legacy systems.
- [ ] Determine whether existing infrastructure can support reliable passwordless access at scale.
- [ ] Confirm readiness for shared device, mobile device, remote access, and offline scenarios.
- [ ] Identify legacy systems that may still require password masking or compensating workflows.
- [ ] Evaluate whether one access platform can support multiple user groups, authentication methods, device types, and access patterns.

5. Business case and executive alignment

Why this matters

Successful passwordless adoption requires a clear business case. CIOs need to show that access modernization supports organizational priorities by improving security, reducing costs, simplifying architecture, and enhancing productivity.

Readiness checklist

- [ ] Define the business case for passwordless access in terms of operational, financial, and strategic outcomes.
- [ ] Estimate the value of reduced password-related support activity, faster clinical access, improved productivity, and reduced tool sprawl.
- [ ] Align IT, security, clinical, operational, and financial stakeholders around shared objectives.
- [ ] Build a phased roadmap that balances speed, risk, workflow impact, and cost.
- [ ] Establish executive-level metrics for TCO reduction, productivity, adoption, user satisfaction, and operational resilience.

Next steps

Areas with multiple unchecked items may indicate operational, technical, or organizational gaps that could limit the enterprise value of a passwordless initiative. Use those findings to align stakeholders, prioritize investments, and identify where additional planning is needed. Then, work with Imprivata to build a phased passwordless roadmap that simplifies access management, reduces support burden, improves clinician productivity, and scales securely across users, devices, applications, and locations.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

7311-2026_APA Healthcare readiness checklist for CIOs