imprivata

CHECKLIST

Passwordless readiness checklist for healthcare CISOs

Assess your organization's ability to reduce credential risk, support zero trust, and secure access without disrupting care.

Healthcare CISOs are under pressure to reduce credential-based risk, strengthen zero-trust execution, and improve audit readiness without creating authentication friction that slows clinicians down. Passwordless authentication can help, but only when deployed as part of a broader identity security strategy.

Use this checklist to evaluate your organization's readiness to transition from password-dependent access to a more secure, adaptive, workflow-aware authentication model. The five focus areas below are designed to help identify gaps, assess readiness, and prioritize areas that may require additional planning before rollout.

1. Credential risk and attack surface reduction

Why this matters

Passwordless readiness starts with understanding where passwords still create organizational risk. For CISOs, the priority is not documenting every workflow in detail, but identifying where credential-based access creates the most exposure and defining a strategy to reduce reliance on passwords over time.

Readiness checklist

- [x] Identify workflows that still require passwords, including clinical, administrative, remote, privileged, EHR, EPCS, shared workstations, and third-party access.
- [ ] Rank workflows by risk of credential compromise, phishing, misuse, and patient care disruption.
- [ ] Identify authentication exceptions, shared credentials, password workarounds, and areas with inconsistent MFA coverage.
- [ ] Prioritize passwordless adoption based on risk exposure rather than technical feasibility alone.
- [ ] Define a phased plan to reduce password dependency, starting with the highest-risk access environments.

2. Zero trust and adaptive access maturity

Why this matters

Passwordless access should not be treated as a standalone authentication upgrade. It should help operationalize zero trust by continuously validating identity, context, device, location, behavior, and resource sensitivity before granting or maintaining access.

Readiness checklist

- [ ] Evaluate whether authentication decisions are static or risk-based.
- [ ] Confirm where phishing-resistant MFA is required today and where it should be expanded.
- [ ] Assess whether access policies account for healthcare-specific context, including shared workstations, roaming clinicians, rapid device changes, and remote access.
- [ ] Determine whether identity telemetry can support threat detection, investigation, and response.
- [ ] Validate that passwordless initiatives support broader zero trust, least privilege, and cyber insurance requirements.

3. Compliance, auditability, and identity assurance

Why this matters

For healthcare CISOs, passwordless authentication must be defensible. It needs to strengthen identity assurance, support healthcare access control requirements, and produce clear audit evidence, especially for high-risk workflows such as credential recovery, MFA enrollment, EPCS, remote access, and privileged actions.

Readiness checklist

- [ ] Confirm audit visibility across clinical, administrative, remote, and privileged access.
- [ ] Review whether credential recovery and MFA reset processes are resistant to social engineering.
- [ ] Validate alignment with HIPAA, EPCS, internal policy, and cyber insurance requirements.
- [ ] Assess whether identity verification is strong enough for high-risk actions such as password resets, authenticator enrollment, and service desk requests.
- [ ] Determine whether audit evidence is centralized, consistent, and easy to produce.

4. Clinical and operational resilience

Why this matters

A passwordless strategy will fail if it improves security but disrupts care delivery. CISOs need assurance that stronger authentication can support shared workstation environments, high-pressure clinical settings, mobile devices, remote access, and downtime events.

Readiness checklist

- [ ] Identify where authentication friction creates security workarounds or care delays.
- [ ] Prioritize shared workstations, remote access, privileged access, and high-risk clinical workflows.
- [ ] Confirm secure fallback and exception workflows for lost badges, unavailable phones, biometric failure, network downtime, and emergency access.
- [ ] Assess whether service desk teams are prepared for new authentication and recovery patterns.
- [ ] Define success metrics such as reduced password resets, fewer lockouts, improved MFA coverage, reduced credential exposure, and improved audit readiness.

5. Governance and execution readiness

Why this matters

Passwordless adoption requires governance across security, IT, clinical operations, compliance, and the service desk. CISOs do not need a tactical project plan. They need a clear, strategic operating model that defines prioritization, risk acceptance, exception management, rollout sequencing, and success metrics.

Readiness checklist

- [ ] Establish cross-functional ownership for passwordless and adaptive access.
- [ ] Define rollout priorities based on risk, clinical workflow impact, and operational complexity.
- [ ] Create an exception management process for legacy systems and special user populations.
- [ ] Set measurable outcomes for security, compliance, IT operations, and workflow impact.
- [ ] Build a phased roadmap that reduces risk while minimizing disruption.

Next steps

Areas with multiple unchecked items may indicate elevated credential risk, audit gaps, or barriers to zero trust that should be addressed before implementing or expanding passwordless access. Use those gaps to prioritize your roadmap, align stakeholders, and identify where additional planning is needed. Then, work with Imprivata to build a phased passwordless roadmap that reduces credential risk, strengthens identity assurance, supports zero trust, and minimizes disruption to clinical workflows.

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

7196-2026_DS-Passwordless