imprivata

CHECKLIST

Passwordless readiness checklist for Clinical Informatics leaders

Assess your organization's ability to reduce authentication friction, protect clinical workflows, and give clinicians more time for patient care.

Clinicians move constantly across workstations, applications, mobile devices, and care settings. When authentication is slow, repetitive, or poorly aligned with workflows, it interrupts care delivery, increases cognitive burden, and encourages risky workarounds.

Passwordless readiness for Clinical Informatics leaders is about answering one central question: Can we make secure access feel invisible to clinicians while preserving the right safeguards at the right moments?

Use this checklist to assess your organization's readiness to move from password-dependent access to a more secure, intuitive authentication model. These sections can help identify gaps, evaluate current readiness, and prioritize areas that may require additional planning before rollout.

1. Clinician workflow friction and care impact

Why this matters

The starting point is not where passwords are used, but where authentication interrupts care. Clinical Informatics leaders are best positioned to identify the moments where login friction breaks clinical momentum, delays documentation, slows medication administration, or creates frustration across shifts.

Readiness checklist

- [ ] Identify the clinical workflows most disrupted by repeated authentication.
- [ ] Determine where login delays affect time-to-care, documentation, medication workflows, or patient throughput.
- [ ] Capture clinician feedback on access pain points by role, unit, and care setting.
- [ ] Assess whether current authentication workflows increase cognitive burden, create repeated interruptions, or increase frustration during the shift.
- [ ] Identify workarounds that indicate access is not facilitating the clinical workflow environments.

2. Shared workstation and fast user switching readiness

Why this matters

Shared workstations are one of the defining access challenges in healthcare. Clinicians need to move quickly from room to room and patient to patient without losing session context, repeating unnecessary logins, or leaving systems exposed.

Readiness checklist

- [ ] Evaluate whether shared workstation access supports fast clinician movement across care settings.
- [ ] Determine whether current login and logout workflows create delays or security gaps.
- [ ] Assess whether session switching is fast, reliable, and attributable to the correct user.
- [ ] Identify high-volume care areas where badge-tap, biometric, or other low-friction access methods would have the greatest impact.
- [ ] Assess whether walk-away security and session locking support both patient safety and usability.

3. Clinical adoption and user experience

Why this matters

A passwordless strategy only succeeds if clinicians use it. The best authentication method is not necessarily the most advanced. It is the one that fits naturally into the clinical environment, role, and moment of care.

Readiness checklist

- [ ] Validate proposed passwordless workflows with frontline clinicians before rollout.
- [ ] Identify which authentication methods are appropriate by role, location, and workflow.
- [ ] Account for practical constraints such as gloved workflows, infection control, personal phone restrictions, shared devices, and high-acuity settings.
- [ ] Confirm fallback options for lost badges, biometric failure, unavailable phones, or downtime scenarios.
- [ ] Ensure training explains what changes in the clinician's shift, not just how to log in.

4. Patient care continuity and downtime resilience

Why this matters

Authentication cannot become a bottleneck during network issues, downtime events, emergency care, or high-acuity workflows. Clinical Informatics leaders need confidence that stronger authentication will not delay urgent access to patient information.

Readiness checklist

- [ ] Determine where authentication failures could delay urgent clinical access.
- [ ] Confirm downtime and offline access requirements for high-acuity and high-traffic care settings.
- [ ] Validate emergency access procedures with clinical, compliance, security, and operations stakeholders.
- [ ] Assess whether fallback workflows preserve appropriate user attribution without slowing urgent access to patient information.
- [ ] Review whether authentication resilience is included in downtime planning.

5. Measurable clinical impact

Why this matters

Passwordless readiness should be tied to measurable clinical outcomes. Clinical Informatics leaders should help define success from the clinician's perspective: fewer interruptions, faster access, less frustration, better workflow continuity, and more time for patient care.

Readiness checklist

- [ ] Define clinical success metrics that will be used to evaluate the impact of passwordless access.
- [ ] Establish baseline measurements for authentication time, password resets, lockouts, repeated prompts, and failed login attempts.
- [ ] Determine how clinician satisfaction and qualitative feedback will be collected and evaluated after rollout.
- [ ] Identify the clinical workflow outcomes that will be measured, such as reductions in delays, interruptions, or access-related workarounds.
- [ ] Define how adoption and usage data will be used to optimize workflows by unit, role, location, and device type.

Next steps

Areas with multiple unchecked items may indicate workflows where authentication friction could continue to disrupt care delivery, clinician satisfaction, or adoption. Use those gaps to prioritize workflow validation, align stakeholders, and identify where additional planning is needed. Then, work with Imprivata to design passwordless workflows that support faster, more intuitive access across shared workstations, mobile devices, EHR workflows, and high-assurance clinical tasks, without compromising security.

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

7229-2026_Passwordless readiness checklist for Clinical Informatics leaders