EBOOK

The state of passwordless authentication in healthcare: Ending password pain

imprivata®

Executive Letter

Modern healthcare runs on fast, reliable, secure access to digital systems. Yet every day, clinicians and staff lose valuable time and significant cognitive bandwidth to passwords that weren't designed for the pace or complexity of clinical workflows. The consequences are familiar across the industry: delayed tasks, increased help desk burden, and user frustration that contributes to clinician burnout – not to mention all the ways that passwords amplify security risks.

Over the past several years, healthcare organizations have accelerated efforts to modernize their identity and access tools. As healthcare IT leaders contend with the pressure of safeguarding data while making workflows seamless and frictionless, we're seeing a natural, highly beneficial shift toward identity-centered approaches that reduce reliance on passwords across systems and devices.

This report reflects survey feedback from over 200 IT and IT security leaders at healthcare delivery organizations (HDOs) across the United States. We wanted to paint a picture of where HDOs are in their passwordless journeys, what barriers to advancement they face, and how they expect their cybersecurity strategies to evolve.

And the findings are clear. Leaders recognize that password-heavy environments are no longer sustainable. Clinicians need faster, more intuitive workflows. Security teams need stronger protection against increasingly sophisticated cybersecurity threats. Executives need a path to modernization that reduces risk without disrupting critical care and optimizes return on investment (ROI).

Ending password pain isn't just a convenience initiative; it's a strategic imperative. The data in this report offers a practical view into the state of healthcare cybersecurity, and what it will take to ensure efficient, secure, and clinician-friendly access in the future.

– **Chip Hughes, Chief Product Officer, Imprivata**

Introduction

Healthcare organizations have long struggled with the tension between implementing strong security controls and enabling the fast, seamless workflows that clinicians and patients need. Complex passwords and passphrases have become a source of friction and operational risk. They slow down care, frustrate users, and contribute to a growing threat landscape driven by credential theft, social engineering, and a new breed of AI-generated cyberattacks.

In November 2025, Imprivata conducted a survey of healthcare IT leaders to quantify the current state of the industry's passwordless and advanced access capabilities. The data reveals a decisive shift: HDOs consider passwordless access to be a vital evolution in healthcare's cybersecurity strategies, clinical efficiency initiatives, and modernization roadmaps.

However, password use remains pervasive, and few organizations have fully adopted passwordless access for their users. The top barriers to passwordless adoption are technical limitations and concerns about usability and regulatory compliance. Nevertheless, IT leaders agree that these barriers can and must be overcome to improve clinician experience, security, and operational efficiency.

85%

of respondents consider passwordless authentication to be very important (63%) or mission-critical (22%) to healthcare's future

7%

have fully adopted passwordless authentication for all clinical and other staff

57%

of organizations cite integration/technical challenges as the top barrier to adopting passwordless authentication

This report presents the survey findings and examines their implications for healthcare IT strategy, covering:

- **The benefits of passwordless and other advanced access capabilities**
- **The current state of passwordless adoption and impact**
- **The barriers to adoption that organizations face**
- **Our outlook for the future**

Passwordless: A strategic and foundational movement

Advancing beyond passwords is no longer optional; it is foundational to the security, reliability, and continuity of healthcare technology.

The majority of survey respondents agree that passwordless authentication is central to the future of healthcare cybersecurity and operations.

- 63% of respondents consider passwordless authentication "very important" to the future of healthcare IT security and efficiency
- An additional 22% describe it as "mission-critical"

85%

of healthcare IT and security leaders now see passwordless authentication as a vital component of their long-term identity security and access strategy.

In other words, 85% of healthcare IT and security leaders now see passwordless authentication as a vital component of their long-term identity security and access strategy.

Advanced access capabilities are gaining recognition and momentum

The recognition of passwordless as a strategic priority extends to broader advanced access capabilities, as organizations continue to strengthen their defenses against increasingly pervasive, sophisticated cyber threats. These access controls go beyond traditional username-and-password or static multifactor authentication (MFA) models to capabilities that continuously assess risk and protect high-value assets.

Respondents identified the following capabilities as most valuable to their organization's security strategy:

- **Continuous session monitoring – 81%**
- **Risk-based authentication – 74%**
- **Offline multifactor authentication – 73%**
- **Self-service password reset/unlock – 71%**

For healthcare organizations, interest in these capabilities indicates several themes:

- **Recognition that point-in-time login verification is not enough -** Continuous session monitoring and adaptive controls help detect anomalous behavior inside sessions, not just at sign-on

- **Awareness of connectivity and availability challenges -** Offline MFA reflects the reality of unreliable networks in some care settings and the need to maintain secure access during outages

- **Demand for scalable, self-service tools -** Self-service reset/unlock capabilities reduce help desk dependence while improving user experience

Overall, the survey shows that passwordless is not an isolated objective; it's part of an overall modernization of access controls needed to keep pace with evolving threats and distributed digital care models.

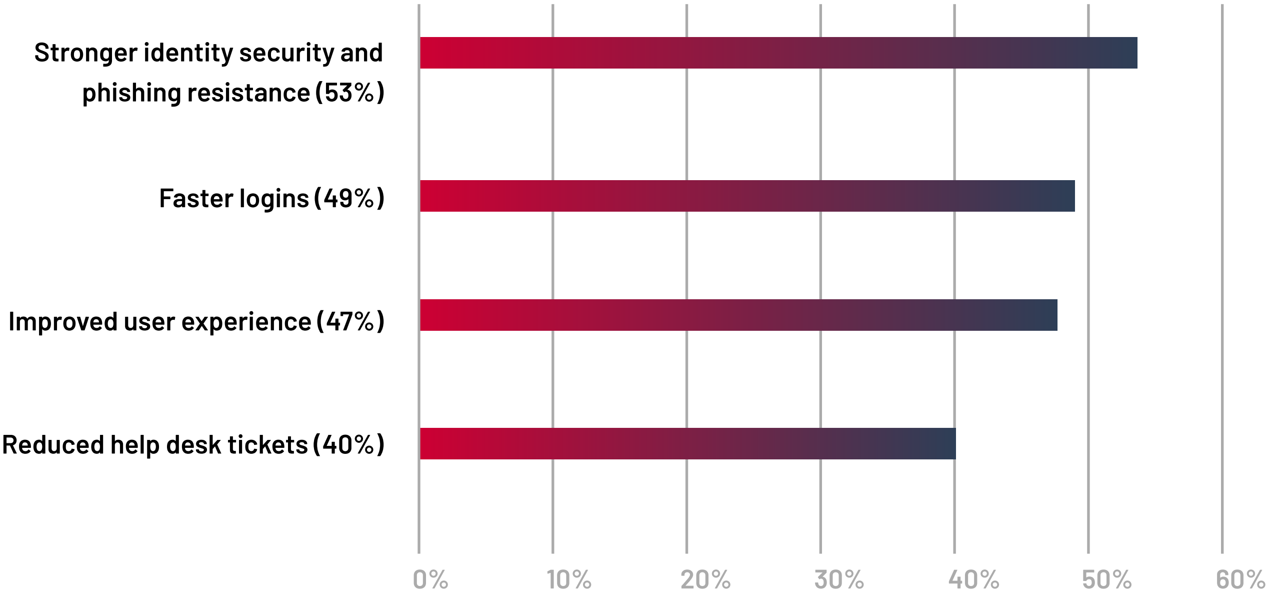
Start your passwordless journey here

Organizations expect meaningful gains in security, usability, and operations

Survey respondents see advanced access and passwordless authentication as a way to address long-standing friction and risk created by traditional passwords, while receiving significant workflow efficiency, security, and IT operational benefits.

When asked about the most important benefits they expect to receive, respondents prioritize stronger identity security and phishing resistance (53%), faster logins (49%), improved user experience (47%), and reduced help desk tickets (40%).

Most important benefits organizations expect from passwordless and advanced access capabilities



The survey findings suggest that healthcare organizations see passwordless and advanced access as a way to simultaneously:

- Reduce their exposure to credential-based attacks like phishing and brute-force attempts
- Remove authentication-related friction from clinical workflows
- Lower the operational burden and cost associated with password lifecycle management

Adoption lags behind intent

Despite broad recognition of the value of passwordless and advanced access, actual adoption is still in the early stages.

The survey highlights a significant implementation gap with the following findings:

- **Only 7% of organizations have fully adopted passwordless access for all clinical and non-clinical staff**
- **60% of organizations still use passwords extensively as a means of user authentication**
- **Only 27% use adaptive or risk-based authentication extensively**

- 54% of organizations use **at least three** authentication vendors
- 16% of organizations use **four or more** authentication vendors

At the same time, many respondents have introduced biometrics and other modern authenticators alongside passwords:

- **53% of organizations use fingerprint biometrics**
- **45% of organizations use facial recognition**
- **54% of organizations use at least three authentication vendors**
- **16% of organizations use four or more authentication vendors**

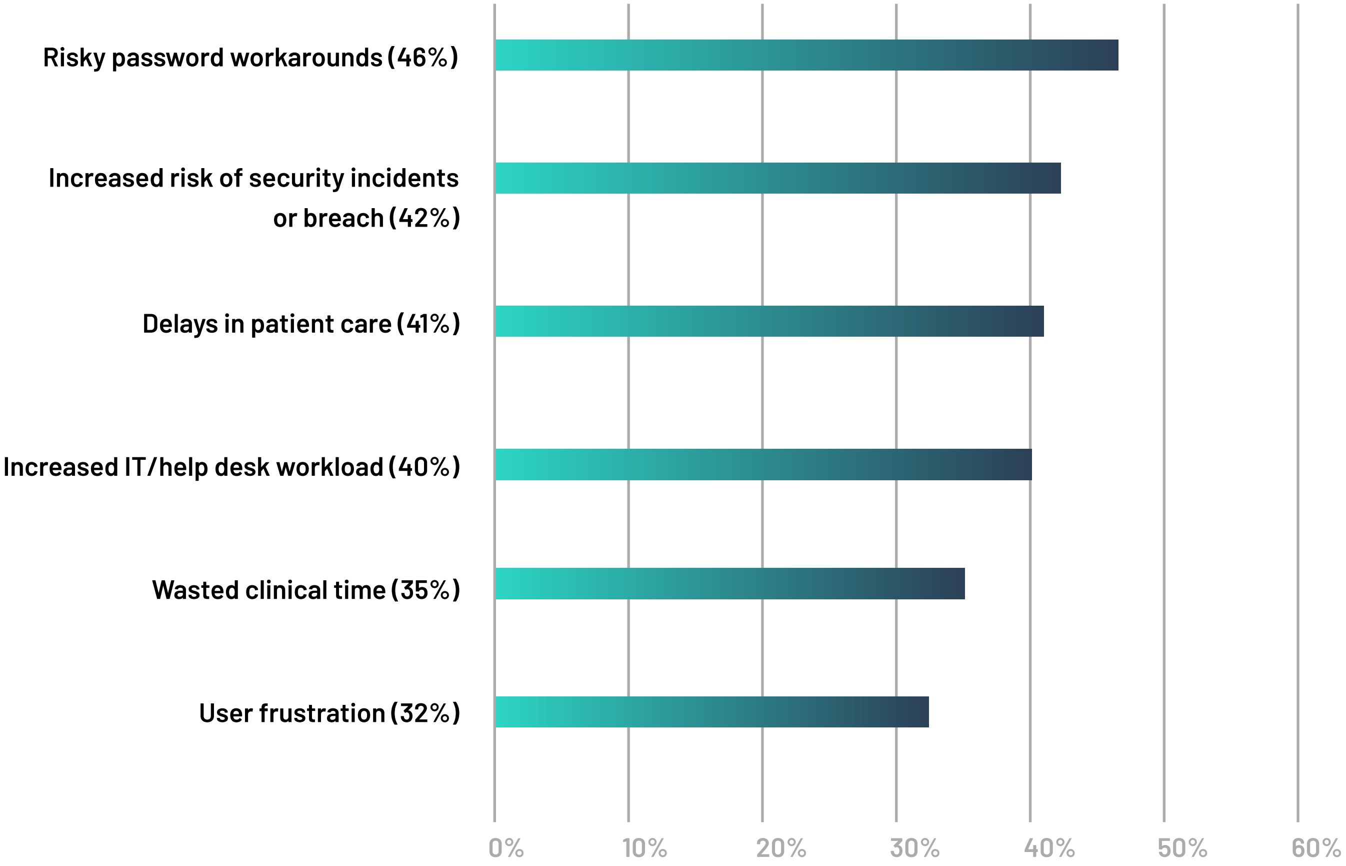
The data indicates that the market is in a transition phase. While organizations are experimenting with modern access methods (badges, biometrics, mobile authenticators, smart cards, passkeys), most have not yet unified these capabilities into a cohesive strategy for minimizing password use.

Instead, many HDOs find themselves with hybrid, fragmented environments where passwords remain deeply embedded in workflows and legacy applications, even as new authenticators are added around the periphery.

Healthcare still struggles with access management challenges

The continued reliance on usernames and passwords, coupled with the challenges of vendor sprawl, is not just a technical nuisance. Respondents report clear negative impacts on workflows, security, and IT operations, including risky password workarounds (46%), increased risk of security incidents or breaches (42%), delays in patient care (41%), and increased IT/help desk workload (40%).

Top negative impacts of passwords on workflows, security, and IT operations



For clinical workflows specifically, organizations cited the following as their biggest user authentication challenges:

- **Compliance and audit pressure (48%)**
- **High password reset volume (43%)**
- **Shared workstation access issues (42%)**
- **Workflow disruption (38%)**
- **Credential theft/phishing (34%)**

Taken altogether, the data suggest that status quo authentication has become a systemic risk.

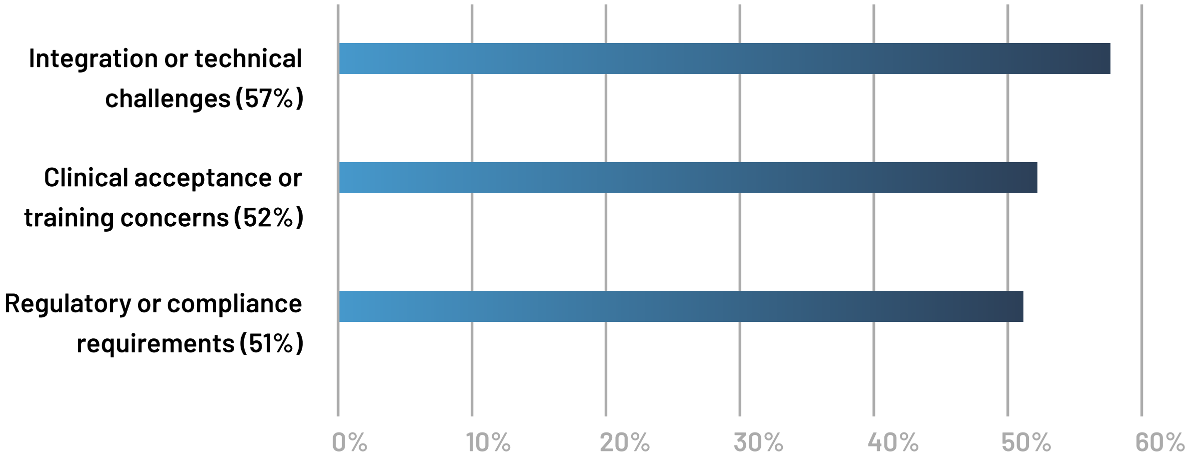
For clinicians, it introduces friction, time loss, and workarounds that can undermine safety and increase burnout. For IT and security teams, it inflates operational overhead while leaving key systems vulnerable to increasingly sophisticated attacks. For compliance and audit stakeholders, it complicates evidence gathering and policy enforcement across disparate authentication tools.

Barriers to adopting passwordless and advanced access technologies

If the strategic case for passwordless and advanced access technologies is clear, and the pain of the current state is well understood, why is adoption progress so limited?

Respondents cited a combination of obstacles at their organizations, reporting that the top barriers to passwordless and advanced access adoption are integration or technical challenges (57%), clinical acceptance or training concerns (52%), and regulatory or compliance requirements (51%).

Primary barriers to adopting passwordless and advanced access technology



The combination of these factors helps explain why organizations often need to begin their passwordless journeys by gradually adding new authentication methods on top of passwords rather than pursuing aggressive password minimization or fully passwordless workflows.

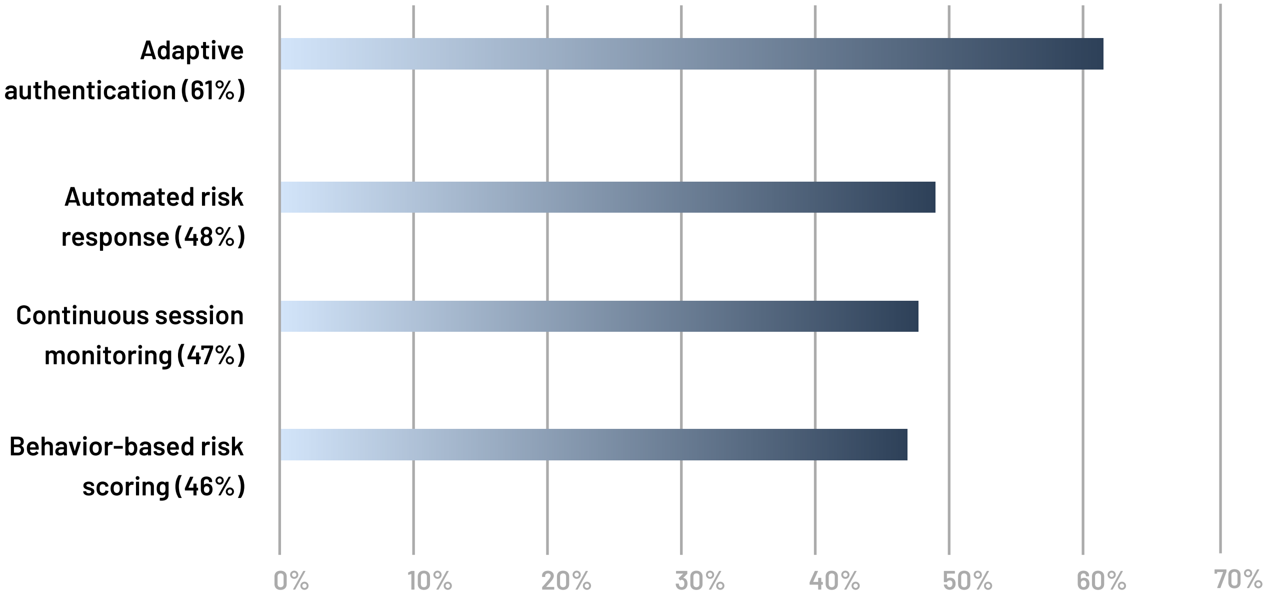
A cautiously optimistic outlook

Despite barriers to adoption, the survey reveals that organizations have a clear intent to make progress toward passwordless and advanced access over the next two years.

Key forward-looking findings include:

- 23% of organizations expect to fully adopt passwordless authentication for all clinical and other staff within the next two years — more than three times the current rate of full adoption (7%)
- Biometric authentication is cited as the top method for enabling password elimination, with
  - 57% of respondents including fingerprint authentication among the most essential capabilities needed to accomplish their goals, and
  - 54% including facial recognition among the most essential

Furthermore, organizations plan to invest in smarter security and threat detection capabilities over the next two years, including the following:



This planned investment in advanced access control suggests that many HDOs are moving beyond pilots and point solutions toward technologies that support an adaptive, passwordless future. This shift aligns with broader industry momentum toward phishing-resistant and context-aware authentication.

Although the gap between aspiration and current state remains substantial, the survey nevertheless indicates:

- **Strong and growing executive-level recognition of the need to reduce reliance on passwords**
- **Momentum toward capabilities that enable risk-based, continuous protection rather than static, one-time checks**
- **Increasing comfort with biometric and other non-password authenticators, particularly when they can be integrated into clinical workflows without sacrificing speed or usability**

As cyber threats grow more sophisticated and operational pressure intensifies, healthcare organizations need identity-centric strategies that advance both security and usability.

Intelligent, context-aware access controls offer a path beyond the limits of legacy authentication. By moving toward a passwordless future, leaders can reduce risk, streamline workflows, and build a resilient foundation for what comes next. Now is the time to chart that course.

METHODOLOGY

The survey was conducted in November 2025 and involved 206 respondents from healthcare delivery organizations across the United States. Respondents included CIOs, CISOs, IT directors, security architects, clinical informatics leaders, and other senior stakeholders.

Organizational profiles:

- Hospital systems: 46%
- Integrated delivery networks (IDNs): 20%
- Academic medical centers: 34%

Sizes:

- Small (<500 beds): 7%
- Mid-sized (500–2,000 beds): 64%
- Large (>2,000 beds): 29%

Start your passwordless journey here

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