WHITEPAPER

The journey to passwordless for healthcare

imprivata®

Table of contents

Safe harbor

Imprivata's strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by Imprivata at any time for any reason without notice. This information does not constitute a commitment, promise, or legal obligation to deliver any material, code, or functionality. This information is for informational purposes and may not be incorporated into a contract. In an industry such as ours, things can change very quickly and we have to react just as rapidly to new opportunities that may present themselves, and as a result this information should not be relied upon in making purchasing decisions.

NEW FUNCTIONALITY

New software features and functionality offered in new versions, if priced separately, are not included in Maintenance and Support. Additionally, any incremental hardware required to support new software features and functionality is also priced separately.

01

Introduction

While all industries contend with cybersecurity threats, healthcare is among the most-targeted industries, due in large part to the criticality of patient care, as well as the perceived value of PHI. Bad actors attempt to gain access to systems in many ways, but passwords are a common target – and the weakest link.

Healthcare CIOs and CISOs seek to eliminate or mask passwords from end user workflows and systems. However, they currently struggle with the absence of a viable solution that both keeps systems secure and enables end users.

Fully removing or masking passwords is challenging because:

- Clinicians depend on passwords to have anywhere, anytime access
- Alternative authentication methods used to replace passwords must meet or exceed the ease of use and efficiency clinicians depend on
- Generic authentication solutions are a poor fit for the complexities of healthcare infrastructure with its mobile workforce, many clinical workflows, shared endpoints, and legacy apps

The unsatisfying compromise is ever-longer and more burdensome Active Directory (AD) passwords, which negatively impact clinicians while still not meeting security needs.

Two decades ago, Imprivata enabled the adoption of EHRs in healthcare by introducing a solution that elevated both security and clinician convenience with Imprivata OneSign (now ***Imprivata Enterprise Access Management***), which has been known by our customers as tap-and-go[1]. Today, the healthcare sector is once again in need of a similar win-win, improving security and convenience at the same time.

WHO SHOULD READ THIS WHITEPAPER?

- Healthcare CIOs, CISOs, and anyone interested in healthcare security
- Topics covered include:
    - The definition and benefits of passwordless
    - Considerations for success with passwordless in healthcare
    - How to get to passwordless authentication and systems
    - A maturity model for passwordless authentication
    - The Imprivata vision for achieving passwordless in healthcare

[1] "Tap-and-go" is the ability to use a badge tap by itself after an initial MFA authentication, typically badge plus password during a configured period ("grace period")

02

What passwordless is and why is it needed

Passwordless can be looked at from different angles:

- From the perspective of the end user, passwordless means passwordless authentication: it's about not ever needing passwords for authentication.
- From an IT perspective, the focus is also on passwordless systems: how do we arrive at systems that no longer use passwords, internally or for any connections?

This whitepaper will focus on achieving "passwordless authentication" for end users, specifically for clinicians. When discussing removing passwords from systems, the term "passwordless systems" will be used.

The relationship between MFA and passwordless authentication

Multifactor authentication (MFA) and passwordless authentication are overlapping but distinct terms.

- **Passwordless authentication** | End user authentication without using passwords
- **MFA** | Using multiple authentication factors (something you know, something you have, something you are)

MFA can be passwordless (e.g., push token + facial biometrics), or password-based (e.g., push token + password). MFA helps to protect against the compromise of a single authenticator.

A passwordless authentication using only a single factor (e.g., facial biometrics by itself) is not MFA.

WHY GO PASSWORDLESS?

Removing passwords from end user authentication and systems has many benefits.

Cybersecurity benefits:

- Protection from phishing and password-spraying attacks
- Decreased ability for attackers to move laterally in your environment
- Improved cyber hygiene
- Improved protection against insider threats
- Reduced credential sharing

Operational benefits:

- Improved end user experience and satisfaction
- Fewer interruptions and increased time and focus on patient care
- Quicker adoption of mobile devices and connected medical devices that improve clinician productivity
- Cost reductions by eliminating password-related costs, such as help desk call reduction, and addressing password-related vulnerabilities

03

Considerations for success with passwordless authentication

Many different passwordless authentication methods exist in the market, but they're not all created equal. Here are some things that you need to consider when selecting methods.

- Healthcare workers interact with many devices, using different workflows. Look at each workflow individually.
- Ease of use is important for every user, but is especially crucial for clinicians.
- Simplicity prevails over complexity. Fewer methods are better. Methods that do not require new hardware or tokens to be issued and carried are preferred.
- Passwordless authentication for clinicians needs to be always available, or a fallback must be in place so that they can access medical records in urgent situations.
- Meeting cybersecurity needs is key: authentication needs to be resilient against the exploits used by attackers. Phishing-resistant authentication is highly recommended by many including the U.S. government's **Cybersecurity and Infrastructure Security Agency (CISA)**.

While the following list by no means covers all workflows you'll find, it offers a view into the complexity of the healthcare environment. Workflows are distinct, and the related authentication criteria are, too.

Workflow	Authentication criteria
Signing in to the EHR on shared clinical workstations	• Speed of access and usability are essential. Users log in up to 80 times a day. Users often authenticate in the presence of patients. • Clinicians may use many different endpoint devices throughout their day, including at shared workstations, the bedside, and other points of care. • Personal mobile phones may not be permitted because of policy or patient privacy issues. • Badge readers are typically already present on these workstations. Cameras may be available, although in some areas patient privacy concerns prevent them from being deployed. • Epic® recommends access to their systems within 10 seconds when possible.
E-prescribing of controlled substances (per the guidelines of the **U.S. Drug Enforcement Agency**)	• The US DEA requires two-factor authentication. • It is required that any token used is separate from the device used for e-prescribing. Tokens need to be compliant with **FIPS 140-2** or higher. • When using biometrics, specific **DEA requirements** need to be met. • All authenticators need to be strongly linked to the person authorized to e-prescribe, using the identity-proofing methods allowed by the DEA. • Electronic prescribing of controlled substances (EPCS) authentications are performed in various use cases. For general e-prescribing, a universal solution that works everywhere is important. For high-volume e-prescribing, in the Discharge department or for certain specialties, for example, a more efficient solution may make a higher footprint acceptable.
In-EHR re-authentication and witnessing	• Re-authentications can occur frequently. For clinicians, less friction is better. A minimal amount of friction is desirable to ensure clinicians read and consider what they are re-authenticating for. • In high-pressure situations, clinicians may share credentials to circumvent security protocols to gain efficiency. For example: a nurse may use a colleague's badge during rounding to avoid having to find a witness. Authentication methods that cannot be shared by users, such as biometrics, will provide higher accountability. • Re-authentication and sign-in should use the same authentication method for simplicity. • Some states have their own rules and regulations for re-authentication other than EPCS.
Signing in to shared mobile devices	• Device-level passcodes are needed to protect multiple apps on the device. These passcodes should be individual and never shared. • Not all mobile apps can use modern authentication such as OIDC and SAML. Password vaults can help ensure security even on legacy apps. • The small touchscreen keyboards on mobile devices make usernames and (long) passwords even more challenging to type. • Native mobile authentication methods such as Touch ID and Face ID are not a good fit for shared devices and witnessing in general, as they are designed for authentication of a single user to a personal device.

Workflow	Authentication criteria
Mobile EPCS	• On-device private keys and tokens stored on that same mobile device are prohibited by DEA regulations.
Signing in to connected medical devices	• Authentication options for connected medical devices are determined by the methods supported by the individual device manufacturer. Medical devices often lack a physical keyboard.
Access to managed single-user laptops and desktops	• External peripherals are not desired for cost and portability. • As laptops are used on the go, access should always be available, from any network, even when offline.
Access to cloud applications and remote gateways from bring your own device (BYOD) devices	• For access from BYOD devices, a solution requiring no new hardware or client software is required. Distributing and supporting software on unmanaged devices is especially costly and time-consuming. • Cloud apps and remote access gateways are an attractive target for phishing. Phishing-resistant authentication is highly recommended by **CISA** and other experts.
MFA-issuance (onboarding new MFA authenticators/ recovery from lost or forgotten authenticators)	• The assurance level of the authenticator used before issuing a new MFA authenticator transfers to the MFA issued[2]. In other words, if an attacker can enroll new MFA using a weaker method such as a password, it does not matter how strong that MFA is.[3] • MFA issuance should, as much as possible, allow the user to securely self-onboard new or replaced credentials, avoiding a help desk call. • Help desks need a secure way of verifying users who do call in for a new MFA authenticator.
Privileged access	• Privileged users such as administrators external vendors with access to the organization's systems and those in the C-suite are high-value targets for attackers and should use highly secure authentication methods. • Phishing-resistant authentication is recommended by **CISA**. Many experts also recommend using hardware security keys to provide the highest level of security.

04

Considerations for selecting passwordless authentication methods

Comparing the available authentication methods with the needs of all healthcare workflows can be overwhelming at first. That's because multifactor authentication makes use of different types of authenticators – something you have, something you are, and something you know – and not all authentication methods are acceptable for every workflow. Let's break it down.

*[2] **See NIST 800-63B 6.1.2***

*[3] See this **darkreading.com** article that shows how attackers exploit the availability of weaker authentication methods*

SOMETHING YOU HAVE AUTHENTICATORS

Phone-based authentication methods

Phone-based authentication can be easily deployed with no requirements for client-side hardware or software. Phones are not ideal for many clinical workflows, with the exception of EPCS.

Phones may not be allowed in certain clinical areas and clinicians may not have access to their phones during their shift. Push notifications and QR codes offer reasonable usability for occasional authentications but fall short for scenarios such as clinical workstations where clinicians need to authenticate up to 80 times a day.

If a phone is the sole source of authentication, securely recovering from lost or upgraded devices requires help desk support. Credentials synced to the phone's cloud backup solve the upgraded device problem but **may not meet all enterprise security requirements** and cannot be used for EPCS.

Phone-based authentication comes in many forms. SMS-based authentication is the least secure method and is discouraged by security experts. Push notifications with number entries are not resistant to the Attacker-in-the-Middle phishing attacks. FIDO[4] Passkeys are phishing-resistant and are considered the best option.

Platform Synced Passkeys can be synchronized to all users' devices via a cloud sync fabric chosen by the user. They are typically used to gain access to resources within a session but can also be leveraged to enable phone-based access to other endpoints. A key advantage is that they do not need to be re-enrolled when users upgrade their phones.

[4] *FIDO (Fast Identity Online) is a set of standards developed by the FIDO Alliance for strong authentication.*

Badge-based authentication methods

Badge-based access remains the best option for clinical access. Building access badges work well, but older badge types, especially, can be vulnerable to replay attacks. FIDO badges offer the best of both, combining the usability of badges and tap-and-go with phishing-resistant authentication. FIDO badges can also be used for EPCS and have the best potential for passwordless mobile EPCS[5].

Using a badge for clinical access and a phone for other workflows can cover almost all or all workflows. And since users have two methods, secure self-service recovery becomes feasible too. The phone can be used to recover from a lost badge, and vice versa.

Authentications using a secure enclave

For single-user devices with a secure enclave, the device itself can be used as a "something you have." This offers great ease-of-use as only the second factor is needed to access the device. For connections to any network or cloud resource, phishing-resistant MFA is available leveraging a key in the enclave. Another "something you have" is still needed to enroll the user to the device, so it does not replace the need for phone and badge authenticators. This method should only be used for devices that can be considered to be in the possession of the user and should not be used for single user devices in public areas.

Workflows used by clinicians

	Phone	FIDO USB token	Building access badge	FIDO badge	Secure enclave
Shared clinical workstation	🔴	🔴	🟢	🟢	🔴
Shared mobile device (check-out)	🟢	⚫	🟢	🟢	🔴
Shared mobile device (SSO, re-auth)	🔴	🔴	🟢	🟢	🔴
EPCS	🟢	⚫	🔴	🟢	🔴
EPCS on a mobile device	🔴	⚫	🔴	🟢	🔴
Connected medical devices	🔴	🔴	🟢	🟢	🔴

[5] *FIDO badges and security keys can be used for EPCS, if the vendor attests, they are compliant with FIPS-140-2 or higher.*

Workflows used by clinicians and non-clinicians

	Phone	FIDO USB token	Building access badge	FIDO badge	Secure enclave
Single-user device-managed	🟢	⚫	⚫	⚫	🟢
Access to cloud apps and remote gateways (BYOD)	🟢	⚫	🔴	⚫	🟢

🟢 Good fit | ⚫ Caveats (e.g. extra hardware, user experience, etc.) | 🔴 Bad or no fit

Table: Authentication method types scored by key workflows in healthcare. ***See Appendix A: "What you have" authenticators scoring notes*** *for more details*

"SOMETHING YOU ARE," USING BIOMETRICS

Biometrics are a great second factor that complement "something you have" factors because of the ease-of-use. Biometrics can also be used standalone for workflows where the set of potential users can be restricted to a small group or even a single user.

Facial biometrics have significantly evolved and are a popular choice of biometrics. The usability is attractive since the required user interaction is very minimal to none. Most endpoints have good quality cameras today. Facial biometrics work especially well on mobile phones and tablets given the high-caliber cameras built in on these devices.

Biometric enrollments can be centralized or stored on the local authenticator.

For clinicians, centralized biometrics are a commonly-selected option, as this modality allows users to enroll once and then use the enrollment across devices.

The security of facial biometrics cannot rely solely on the possession of a biometrics secret, since obtaining a picture of a user is easy for an attacker. Instead, Presentation Attack Detection (PAD), also called liveness detection, is needed to ensure that an authentic person is in front of the camera, and not a photo, video, or someone wearing a silicone mask.

It is important to be aware of the notice and consent requirements related to the collection and processing of biometric data. Some users may prefer not to use biometrics, and centralized biometrics are regulated in some areas, including in some US states such as Illinois, Texas, and Washington.

Products that implement Privacy by Design will offer alternate authentication methods when users opt out.

SOMETHING YOU KNOW

Memorized secrets are still required in a passwordless world as biometrics may not always be available. For example, some devices may not have cameras, and some users may not have consented to use biometrics.

The memorized secrets used in passwordless solutions are commonly referred to as PINs. PINs have a very different risk profile from passwords[6] because:

- They cannot be used by themselves (passwords can). They are always used in combination with another factor, most often a "something you have" factor.
- Hashes of PINs are typically better protected than password hashes. For example on Active Directory, well known attacks exist that allow exporting hashes and bruteforcing them.

Because of the lower risk, PINs can be significantly shorter than AD passwords (NIST recommends eight characters[7]).

Like biometrics, PIN enrollments can be stored locally, on the authenticator, or centrally. Centralized PINs allow for a single enrollment to be used everywhere and are a precondition to enable the tap-and-go workflow when using a badge with a PIN as the second factor.

Knowledge-based authentication (KBA, aka "security questions"), is another alternative "something you know" method. Answers to these questions can often be easily guessed or obtained through social engineering. Using this method is not recommended by experts; in fact, NIST no longer allows the use of KBA[8].

05

Understanding the approaches for passwordless systems

Removing passwords from backend systems requires the vendors of those systems to provide alternative mechanisms, typically by leveraging open standards, such as SAML or OpenID Connect (OIDC). In those cases, it is a matter of upgrading to a version that supports these new standards and configuring those systems for use.

In many cases, however, legacy applications and on-premises software, such as Microsoft Active Directory (AD), may not fully support passwordless mechanisms yet.

The security of these systems can still be increased, however. Once users no longer need to know their passwords, those passwords can be automatically, and regularly, rotated to a random and complex string. A single sign-on solution can enter those rotated passwords into apps on the users' behalf.

[6] See *Appendix B: password vs PIN.*

[7] See *NIST 800-63b* , *chapter 5.1.1.1*

[8] See *NIST 800-63b, chapter 5.1.1.2*

06

Achieving passwordless authentication is a journey

Passwords are used in many areas and processes, so replacing them with passwordless alternatives all at once is impractical. However, there are important benefits to be gained from deploying passwordless authentication to reduce password usage or eliminate passwords from select workflows – so knowing where to start is key. Passwords are deeply ingrained in how users work and are the universal fallback for clinicians during patient care. Change management while rolling out passwordless with frequent input from stakeholders – especially clinicians – is critical to success.

To help chart the path to passwordless, Imprivata has created a passwordless maturity model.

At the base level of this model, level 0, all access is password-based. We know this base level presents many challenges both for usability and security. The many password authentications demanded from clinicians at this level prompt them to bypass security by sharing credentials and open sessions.

It's no surprise, then, that most healthcare organizations are at level 1, where tap-and-go[9] is used to drastically cut down on the number of passwords clinicians need to enter throughout their day. For workflows that need higher security, such as access to gateways and cloud apps or privileged access, the password is typically used in combination with MFA.

To reach level 2, passwords are eliminated where their burdens or risks are most significant. Mobile workflows, re-authentication, witnessing, and cloud-facing authentication are all high-value workflows that are rewarding when addressed beyond tap-and-go. This will further improve the user experience and will increase user acceptance of the longer AD passwords that cybersecurity experts recommend. Given the prevalence of phishing attacks, moving to a phishing-resistant authentication method for high security workflows makes sense at this stage.

In level 3, passwords are completely masked from end users, enabling the randomization of backend passwords. This removes most security risks around passwords. Combined with ubiquitous use of phishing resistant authenticators, the organization's security posture significantly improves.

At the top, level 4, passwords are also removed from any systems, further reducing the attack surface. Given healthcare's complex ecosystem, it will take significant time for most organizations to reach this level. Reaching level 3 will already realize many of the security benefits of passwordless, making it less urgent to do so.

It's not necessary to reach a certain level in the model for all users at the same time. For groups of users with fewer or less complex workflows, it is likely possible to achieve higher maturity earlier than for other groups. For example, achieving level 3 for non-clinical users is easier than for clinical users and significantly reduces risk.

[10] The ability to use a badge tap by itself after an initial MFA authentication, typically badge + password during a configured period ("Grace period")

A framework for achieving passwordless maturity

	Key measures	Outcomes
Level 4: End-to-end passwordless	- Passwords no longer exist in any systems	- Reduced attack surface in systems
Level 3: Mask passwords for all end user workflows	- All passwords are removed or masked from end users - Move to phishing-resistant authentication everywhere	- Ability to randomize legacy passwords - Resistance to most password-based attacks - Reduced insider threat
Level 2: Mask passwords from the highest-impact workflows	- Go passwordless for workflows where it adds high clinical or security value - Move to phishing-resistant authentication for cloud apps, gateways, and privileged access	- Resistance to phishing attacks - Improved user experience for passwordless workflows - Ability to increase AD password length to 15+ characters with reduced impact on users
Level 1: Reduce password usage	- Reduce password entry for users with tap-and-go with SSO - Add additional factors for security for cloud apps and gateways	- Improved clinical user experience - Meet MFA requirements for cyber insurance - Reduced risk associated with unattended workstations and credential sharing
Level 0: Reduce password-based	- Passwords everywhere - Manual entry	- Baseline line access security

07

How Imprivata can help with passwordless authentication and systems

PASSWORDLESS CAPABILITIES AVAILABLE FROM IMPRIVATA TODAY

With **Imprivata Enterprise Access Management** (formerly Imprivata OneSign and Imprivata Confirm ID), password usage is significantly reduced. This saves precious time, reduces password fatigue, and improves security.

Clinicians interacting with **Imprivata Enterprise Access Management (EAM)** *dramatically reduce* the time spent typing long, complex passwords to enter workstations, applications, workflows, and medical devices.

A typical clinician who may have typed a password over

80x

in a shift[10] can reduce that to just ***once or twice*** per shift.

Passwordless tap-and-go is available by using the access badge as the first factor, and a centralized PIN, or fingerprint biometrics, as the second factor. From there, the security posture can be maintained with even less burden by setting a grace period, for example four hours, where only a badge tap is required. FIDO NFC badges are supported for tap-and-go to provide phishing resistant authentication.

Added security and convenience is achieved with our Secure Walk Away solution, where the continuous presence of a clinician can be detected using the Bluetooth Low Energy (BLE) chip embedded in their iPhone or Android device, enabling automatic locking when the user walks away and automatic login when they return.

[10] *Best Practices: Single Sign-On Drives Productivity, Security, and Adoption When Used with EHR at The Johns Hopkins Hospital*

Once in the session, further authentications are automated, using our APG-based SSO to legacy apps. EAM also supports standards-based SSO, such as SAML and OIDC for web apps, and WS-Federation for Entra ID.

Customers using a virtual desktop infrastructure (VDI) and/or Server Based Computing from vendors such as VMware, Citrix, and Microsoft automate that access through our virtual desktop automation product.

In the US, clinicians needing to frequently e-prescribe controlled substances can do so – in a frictionless and passwordless manner – by leveraging fingerprint biometrics and our Hands Free Authentication. To this end, Imprivata mobile EPCS supports passwordless using facial biometrics in combination with an OTP token.

The same badge-based and biometrics-based workflows can also extend passwordless access to many other areas, including access to connected medical devices, access to printers, checking out shared mobile devices, and access to Android shared mobile devices.

For end users no longer needing to know their password, password randomization is available. This is available for the AD password as well as legacy apps.

Imprivata ***PAM*** and ***VPAM*** are available for privileged IT and external vendor users allowing passwordless access to systems without sharing the privileged credential.

OUR VISION: ENABLE HEALTHCARE TO FULLY MASK PASSWORDS FROM END USERS

Let's revisit the challenges outlined earlier in the 'Considerations for success' section and see how our vision will help your organization to overcome these obstacles·

Healthcare workers interact with many devices, using different workflows

- Passwordless authentication is available everywhere;every workflow and every process, clinical or non-clinical, is covered either directly by Imprivata or through partner integrations.

Ease of use is important for every user, but crucial for clinicians

- Tap-and-go remains the preferred workflow for clinical authentication, but gets a big upgrade.
- FIDO badges deliver a phishing-resistant high assurance alternative and open up a broad ecosystem. They can be used for EPCS and for mobile workflows that require an out-of-band "something you have" factor.
- For the second factor, centralized facial biometrics are available across all workflows for frictionless access. Existing webcams can be used.
- Phone-based authentication covers all other workflows, leveraging facial biometrics and BLE to provide best-in-class usability as with Hands Free Authentication. Third-party, phone-based authentication will be supported so that users can have single mobile tokens.
- On single user systems, FIDO keys in the secure enclave are available to make the device itself the "something you have" factor, providing MFA without needing to use anything else.

Simplicity prevails over complexity; fewer methods are better

- By leveraging badges, phones, or the endpoints themselves, no new technology needs to be deployed or managed.
- With Imprivata authentication everywhere, users enjoy a single experience, and IT supports a single solution from a single vendor.

Passwordless authentication for clinicians needs to be always available or have a fallback

- Phones can be used to replace badges and badges can be used to register new phones. Together with the centralized facial biometric or PIN, this means users can easily and securely recover from lost or forgotten credentials without needing the help desk.
- For users, organizations, or locations where facial biometrics are not a good fit, a centralized PIN is available as a fallback.

Meeting cybersecurity needs is key: Authentication needs to be resilient against the exploits used by attackers

- With all workflows covered, users no longer need to know their passwords. Systems can become fully passwordless. For legacy systems such as AD, passwords can now be randomized on a nightly basis and become highly resistant to brute-force attacks. This significantly increases the security posture, without needing to replace or remove legacy systems.
- FIDO is leveraged to provide phishing-resistant MFA in the form of badges and security keys and on mobile phones.
- The grace period is now backed by continuous authentication, reducing risks around lost badges.

Conclusion

Embarking on the journey to achieving full passwordless authentication across all your applications and systems will bring significant security advantages by eliminating password-centric authentication that users find frustrating, and that attackers constantly exploit. However, it is important to focus on the journey, not just the destination. By implementing passwordless authentication for even just a few systems, applications, or departments, you will realize meaningful benefits by removing friction for clinicians, and better protecting your organization, employees, and patients from attacks.

By carefully selecting the appropriate passwordless authentication methods for given healthcare workflows, you can increase both security and convenience at the same time. Working with clinical leadership is essential to ensure clinical adoption and success, and to ensure that the workflows you put in place actually help – not impede – care delivery and productivity. It is best practice to deploy passwordless authentication in phases, focusing on those areas where the greatest benefit can be achieved with reasonable budget allocation and resources.

As a trusted partner, with proven healthcare insight and a commitment to innovation, Imprivata can help your organization to be successful and realize benefits at each stage along the way.

Schedule a product roadmap deep dive to see how you can advance towards passwordless, and how Imprivata can help get you there.

SCHEDULE NOW

Appendix A: “Something you have” authenticators scoring notes

Shared clinical workstation

	Score	Motivation
Phone	🔴	• Clinicians may not be willing or allowed to use personal phones in clinical settings • The usability is not sufficient for nurses logging in up to 80 times a day
FIDO USB token	🔴	• The usability is not sufficient for nurses logging in up to 80 times a day • There is a significant risk of the USB key being left in the reader when the user walks away • FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around
Building access badge	🟢	• Clinicians love the speed of access offered by building access badges • Badges commonly need to be worn while practicing medicine
FIDO badge	🟢	• FIDO badges can be just as fast as regular building access badges, provided they are combined with a centralized PIN
Secure enclave	🔴	• Secure enclave-based solutions are designed for single-user devices • Users need to enroll to each device they use

Shared mobile device (check-out)

	Score	Motivation
Phone	🟢	• Shared mobile devices are checked out once a shift, making phone-based authentication a good option
FIDO USB token	⚫	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around
Building access badge	🟢	• Badge access is the best option for device checkout, nurses are already familiar with it and use it for clinical workstation access
FIDO badge	🟢	• Same as building access badge, when used with a centralized PIN
Secure enclave	🔴	• Secure enclave-based solutions are designed for single-user devices • Users need to enroll to each device they use

Shared mobile device (SSO, re-auth)

	Score	Motivation
Phone	🔴	• Clinicians may not be willing or allowed to use personal phones in clinical settings
FIDO USB token	⚫	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around • Older phones may not support USB-C
Building access badge	🟢	• Badge access auth is quick, nurses are already familiar with it
FIDO badge	🟢	• Same as building access badge, when used with a centralized PIN
Secure enclave	🔴	• Secure enclave-based solutions are designed for single-user devices • Users need to enroll to each device they use

EPCS

	Score	Motivation
Phone	🟢	• Phones are the most used authentication method for EPCS • They provide a good option that works everywhere • The usability may be lacking for high-volume e-prescribing • The token cannot be exported to a backup, so when the user upgrades the phone, it will need to be re-enrolled
FIDO USB token	⚫	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around • Usability on shared devices is lacking
Building access badge	🔴	• Building access badges do not meet the DEA's guideline for something-you-have factors
FIDO badge	🟢	• FIDO badges can be used for EPCS as long as they are documented to be FIPS 140-2+ compliant • They are a great option for high-volume e-prescribing and enrolling new or upgraded phones for EPCS
Secure enclave	🔴	• Not compliant; the DEA requires the secret of the something-you-have factor to be stored on a device separate from the one that is used for e-prescribing

EPCS on a mobile device

	Score	Motivation
Phone	🔴	• Not compliant unless used with a different device; the DEA requires the secret of the something-you-have factor to be stored on a device separate from the one that is used for e-prescribing
FIDO USB token	🔵	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around • Older phones may not support USB-C
Building access badge	🔴	• Building access badges do not meet the DEA's guideline for something-you-have factors
FIDO badge	🟢	• FIDO badges can be used for EPCS as long as they are documented to be FIPS 140-2+ compliant • Most phones support NFC
Secure enclave	🔴	• Not compliant; the DEA requires the secret of the something-you-have factor to be stored on a device separate from the one that is used for e-prescribing

Connected medical devices

	Score	Motivation
Phone	🔴	• Phone methods are typically not available on medical devices • Clinicians may not be willing or allowed to use personal phones in clinical settings • The usability is not sufficient for nurses logging in up to 80 times a day
FIDO USB token	🔴	• The usability is not sufficient for nurses frequently logging in to these devices • There is a significant risk of the USB key being left in the reader when the user walks away
Building access badge	🟢	• Building access card authentication is the most practical alternative on medical devices given the limited user interface • It matches the authentication for shared workstations and provides fast authentications
FIDO badge	🟢	• FIDO badges combined with a centralized PIN offer similar advantages as regular building access badges
Secure enclave	🔴	• Secure enclave-based solutions are designed for single-user devices

Access to cloud apps and remote gateways (BYOD)

	Score	Motivation
Phone	🟢	• Phones are the most used authentication method for access on BYOD devices • They work across all devices, without needing client software
FIDO USB token	⚫	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around
Building access badge	🔴	• Building access badges require a badge reader on the endpoint as well as client software
FIDO badge	⚫	• FIDO badges require an NFC reader on the endpoint but can work without client software
Secure enclave	🟢	• The secure enclave, when present, can be used as a FIDO token, offering great usability as well as phishing-resistant authentication • Synced Passkeys, although strictly not necessarily stored in the secure enclave, offer another good solution for this workflow if the risks around backing up private keys to the users' cloud sync solution are acceptable

Single-user device – managed

	Score	Motivation
Phone	🟢	• Users of single-user devices, typically also have easy access to phones • User sessions are longer resulting in fewer authentications, so the lesser usability of phones is not as much of an issue
FIDO USB token	⚫	• FIDO USB tokens are a net new item to deploy and manage for IT and a new item for users to carry around
Building access badge	⚫	• Requires an extra reader to connect to the laptop
FIDO badge	⚫	• Requires an extra reader to connect to the laptop
Secure enclave	🟢	• Offers the best usability, with no other device to carry around or interact with • Another authenticator is still required to onboard the machine

Appendix B: Password vs. PIN

AD password	De-centralized PIN	Centralized PIN
Can be used by itself	Can be used as part of a multifactor authentication	Can be used as part of a multifactor authentication
Tools exist to extract and brute force password hashes from endpoints, Windows servers, and Kerberos tickets.	The PIN hash is stored on physical authenticators, potentially in a tamper-free container making access impractical	The PIN hash is stored on a centralized authentication server that is designed to resist attacks; PIN hashes can be further protected by a key management system preventing the export of the hashes
Recommend password length: at least 16 characters	Lower complexity is acceptable; NIST recommends eight (8) characters	Lower complexity is acceptable; NIST recommends eight (8) characters
Single enrollment	Separate enrollment for each authenticator or endpoint	Single enrollment
Can be used as a second factor with tap-and-go	Usability issues with tap-and-go	Can be used as a second factor with tap-and-go

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at

US +1 781 674 2700

London: +44 (0)208 744 6500

Germany: +49 (0)2173993850

Australia: +61 3 8844 5533

or visit us online at **www.imprivata.com**