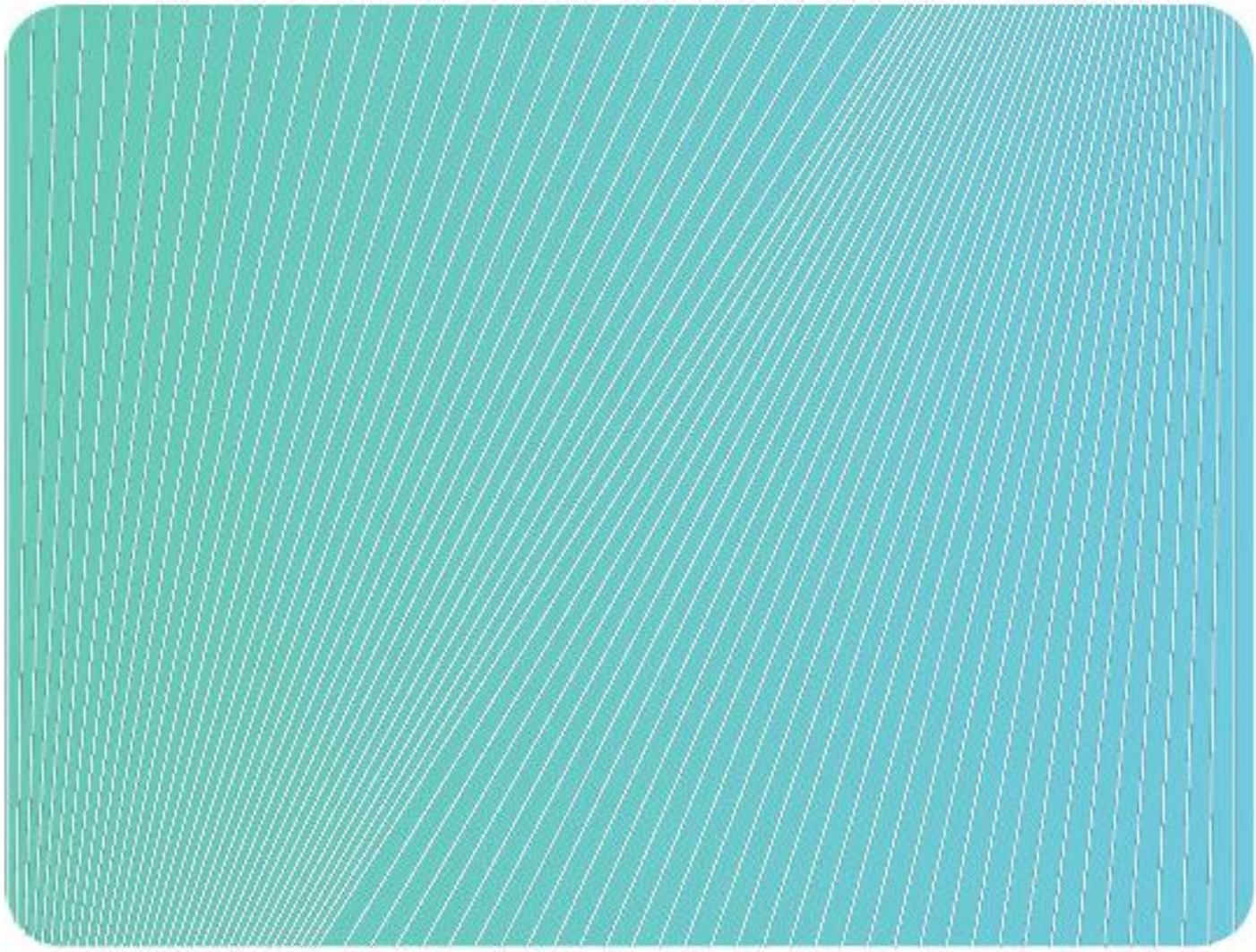
auth0

7 Things Healthcare Organizations Need to Know About Passwordless Authentication

How passwordless authentication enables a secure and seamless CX



WHITEPAPER

auth0.com

Increase Digital Health Uptake by Going Passwordless

Healthcare organizations are shifting towards digital, patient-centric care models at an accelerated rate driven by Covid 19 pushing the rollout of virtual care systems and the enforcement of Smart on FHIR mandated by the 21st Century Cures Act final rules. The latter opens up an application economy, increasing competition from outside players. And healthcare consumers are ready to adopt services from new players - 27% are willing to receive virtual care from technology companies such as Google and Microsoft.

Digital impressions matter now more than ever—28% of consumers have switched or stopped going to a healthcare provider because of a poor digital experience. Additionally, patients will not adopt digital health services if they are perceived as insecure. This, in addition to the fact that the healthcare industry is a top breach target, means that the user experience has to be balanced with security — one cannot be at the behest of the other.

With login being the first point of entry into your virtual care or digital health service — the experience needs to be as frictionless as possible — enter passwordless.

Passwordless Authentication

Going passwordless removes login friction while increasing security by removing passwords. Passwords are insecure and often recycled due to the sheer number of passwords users have. As its name suggests, passwordless authentication involves verifying a user's identity with something other than a password. This might be a push notification sent to a secondary device or a unique biometric like the user's face or fingerprint.

Passwordless takes the guesswork out of secure, frictionless authentication — an increasingly urgent priority as healthcare goes digital. Seamless authentication cultivates customer trust and can improve conversion rates since a user frustrated by a clunky login into your patient portal, mobile application, or website can result in poor user adoption or uptake.

Eliminating passwords also makes your data more secure by frustrating malicious attacks on the login box. Customers can be confident that you'll protect their information and you can be confident that you've taken proactive steps to avoid data breaches.

Here are seven things you need to understand about passwordless for healthcare to make an educated decision about how to roll it out to your customers.

1. Healthcare organizations have good reasons for investing in passwordless.

Digital transformation focuses on modernization to unlock operational efficiencies and optimize security, while enhancing the customer experience. In line with these core outcomes, there are many advantages to going passwordless. Among the most compelling:

- **An effortless login experience:** Passwordless authentication delivers a seamless digital experience: Users aren't stymied by forgotten passwords, and they can access your platform securely in seconds.
- **Reduce security risk:** As more patients begin to leverage technology to access and transfer electronic health information (EHI), the threat of experiencing a data breach is amplified. Verizon's 2021 Data Breach Investigations Report (DBIR found that 61% of all data breaches involved credentials.

- **Reduce long-term costs:** Password management is expensive, largely because people forget their passwords and need help resetting them. Industry experts generally agree that each password reset costs a company $70.
- **Higher conversion rates:** A superior customer experience yields loyalty, higher conversion rates, and ultimately more revenue. For some companies, eliminating passwords has improved conversion rates by more than 50%.

2. Implementing passwordless reduces login friction.

The biggest benefit of going passwordless is that it reduces login friction.

Keep in mind that the average person has to keep track of about 100 passwords and spends almost 13 minutes every week resetting those passwords — often through a call to a help desk, which not only takes up their time but also costs your company money. Passwordless authentication alleviates this login friction without weakening your security posture.

A frictionless user experience can be a powerful competitive advantage for healthcare organizations at every level. With the consumerization of healthcare, people have more options. They will switch providers as a result of a negative digital experience. Given that login is the first point of entry to your digital service, login friction has a direct correlation with conversion/retention rates and revenue. Customers aren't a captive audience like employees, who are more or less stuck with whatever workforce identity solution you give them. By enabling a frictionless customer experience, your investment in passwordless supports customer retention and revenue growth.

3. There are different types of passwordless authentication for different users/use cases.

With traditional username-password authentication, users must input something they know (a password) to verify their identity. Passwordless authentication, in contrast, requires users to demonstrate that they have something (sometimes called a **possession factor**) or that they are something (referred to as an **inherence factor**). These factors are much harder for bad actors to circumvent than knowledge-based factors.

Biometrics

Instead of a password, biometric authentication uses unique physical traits to verify a user's identity. You've probably used facial recognition to unlock your smartphone without entering your passcode or your fingerprint to access your laptop without typing in a password.

Biometric authentication is more secure than a password because no one has your exact fingerprint (even if you are an identical twin) or your exact face (the chances of two faces being similar enough to bypass facial recognition is extremely unlikely, even in the case of identical twins).

Biometrics rely on inherence factors: something that is inherent to the user, like their facial features, fingerprint, or voice.

Magic links

Magic links are another method of passwordless authentication in which users are prompted to enter their email address instead of a username-password combination. The user then receives an email containing a "magic link" they can click to be instantly logged in. This process is repeated every time the user needs access to the platform.

One-time passwords

One-time passwords (OTP, sometimes called one-time codes (OTC)), work similarly to magic links. Customers receive a password or code via email or SMS text message that they use to log in. As their name suggests, one-time passwords are good for one use only; every time a user logs in, the process is repeated with a different single-use password.

One-time passwords and magic links sent through email are **knowledge factors:** you need to know the password for the email account to access the magic links.

One-time passwords and magic links sent via SMS are **possession factors:** they rely on something the user has, like a secondary device, to validate identity.

Push notifications

Push notifications are a mobile-centric form of passwordless authentication. To access an app on a mobile device, users receive a push notification that allows them to open the app and verify their identity. This is how Auth0 Guardian works.

All of the types of passwordless authentication we've discussed here, from biometrics to push notifications, can be deployed as part of multi-factor authentication (MFA; we'll talk more about MFA in the next few pages).

4. Eliminating passwords makes your data — and your users — more secure.

Here's the bad news: Passwords are relatively easy for bad actors to guess, steal, or buy and are a primary breach source. And because so many people reuse passwords across platforms, a single compromised password can endanger patient health data. Password managers like LastPass are effective against brute force attacks, credential stuffing, phishing, and other threats that target the login box. But adoption rates for password managers remain low: You can't count on your customers availing themselves of these resources.

While you can't control customer behavior, you can lower your risk of a data breach by going passwordless.

Multi-factor authentication and passwordless

You might be wondering where multi-factor authentication MFA comes in. With the healthcare industry incurring the highest breach cost across any industry, approximately $9.23 million annually, removing points of vulnerability like passwords is essential. Passwordless authentication can remove passwords from the equation. It can be used as the first factor in MFA, then combined with secondary authentication factors for enhanced security. This approach helps you balance security and convenience for your customers.

In actuality, passwordless authentication methods like WebAuthn are two factors in one. If you use device biometrics, you're actually using both a possession factor (the device) and an

inherence factor (the biometric factor). In this case, you don't necessarily need to demand another authentication method.

It's a good idea to ask for multiple authentication factors when the context suggests a higher-risk interaction. People expect and appreciate MFA at moments that call for increased security: when they enter payment information for medical billing or access EHI data or try to access your service from an unfamiliar device, time, or location. Using passwordless as part of the process speeds and streamlines the experience for users without compromising a high-security standard.

5. Going passwordless conserves resources in the long term.

As we've established, password management is expensive (in terms of time and resources) for IT teams. When users have to call customer support to reset their passwords, they're unhappy, and you're spending money you could be directing at value-add projects. Industry consensus puts the cost of a password reset at $70 per password, but at Auth0, we've seen costs as high as $120 per password. Some enterprise companies spend as much as $1 million a year just on staffing and infrastructure costs around password management.

Going passwordless requires an upfront infrastructure investment, but over time it can reduce costs associated with password management. And when your IT and customer support teams aren't distracted by password resets, they can focus on adding more value for your customers.

Even more expensive than constant password resets is a data breach. As referenced earlier the healthcare industry has the highest breach cost, which is due to the fact that customer personally identifiable information (PII) was the most common type of record lost. Data breaches result not only in actual fines but also in reputation erosion and lost revenue as patients and customers decide they feel safer with your competitors.

6. Passwordless authentication helps drive more conversions.

Reducing login friction is key to customer satisfaction, but it also boosts conversion rates. If the login process is too cumbersome, time-consuming, or is perceived to be insecure, customers are likely to go elsewhere. Going passwordless can boost conversions by as much as 54% by removing friction. Imagine the impact on your bottom line over time.

Not even industry pros are immune to password headaches. A recent survey conducted by Yubico and the Ponemon Institute found that almost half of more than 1,700 IT professionals could not complete a personal transaction because they had forgotten their password. Make it as easy as possible for customers to access and use your services seamlessly. Passwordless helps check that box.

7. A third-party provider is the best pick for passwordless.

As you probably know, implementing passwordless can be a bit more involved than simply swapping out the login box. How complex it will largely depend on the identity and access management (IAM) framework you currently use to verify users' identities and control their access to information. Going passwordless can require dedicated development resources over a sustained period of time, along with scaling, updates, and maintenance after the initial implementation.

That's why organizations often choose an expert identity provider like Auth0 to reduce the time-to-value of their passwordless implementation. Entrusting passwordless to a third-party provider isn't just faster; it also allows you to offload future maintenance costs. Perhaps most importantly, it gives you peace of mind: You don't have to keep track of emerging threats, software updates, and new legislation, because you'll know your identity provider is on it.

Where do I go from here?

Ready to learn more about implementing passwordless authentication with Auth0? Start here. You can also reach out directly to our experts to understand how going passwordless can help you provide the secure, friction-free experience your customers want.

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit **https://auth0.com** or follow **@auth0** on Twitter.