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.

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

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.

CONTINUE READING >