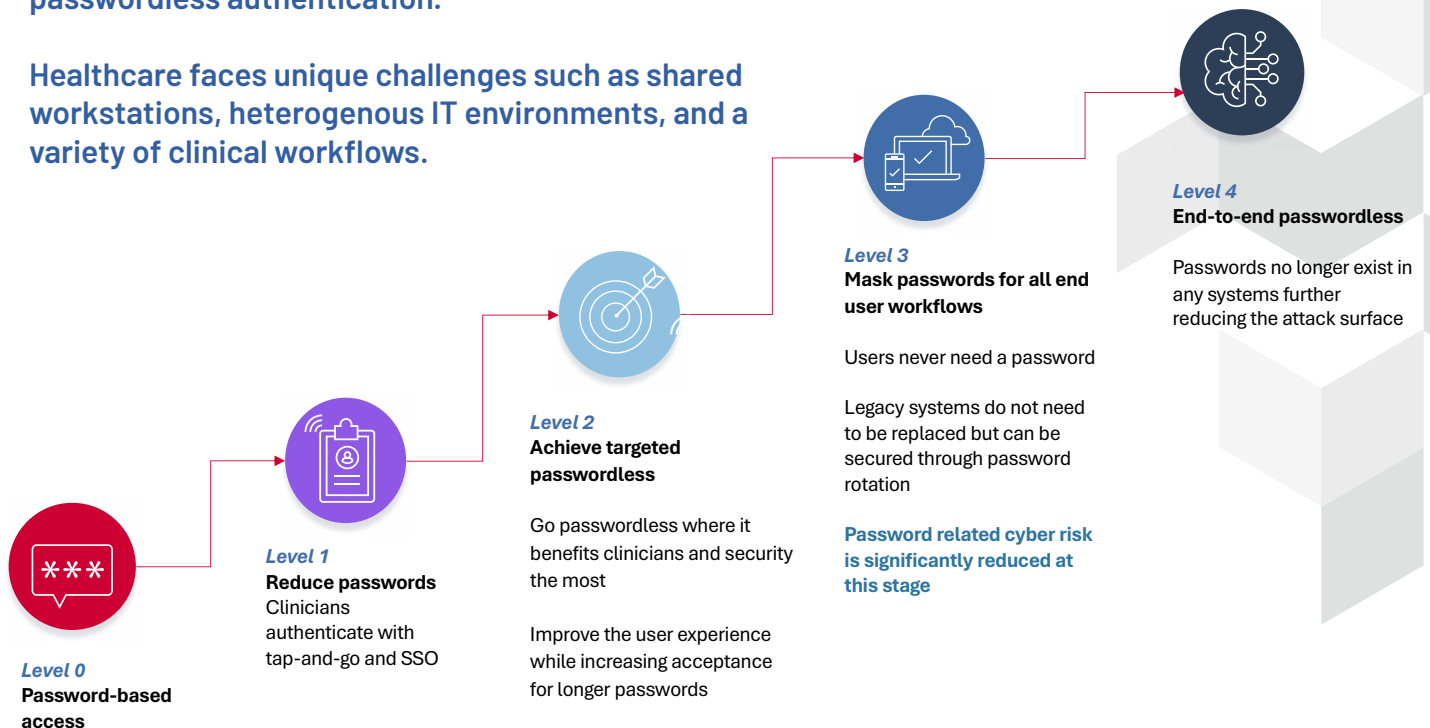# Chart a path to passwordless for healthcare

Eliminating passwords from end user authentication and systems offers security benefits, such as protection against phishing and password-based attacks. Passwordless authentication also leads to a better user experience for clinicians, giving them more time to focus on patient care and increasing their adoption of new mobile and medical devices.

The reality is that 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 – 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. Therefore, change management while rolling out passwordless with frequent input from stakeholders – especially clinicians – is critical to success.

Imprivata's passwordless maturity model

Healthcare organizations can benefit from using this maturity model for a stepwise approach on the journey to passwordless authentication.

Healthcare faces unique challenges such as shared workstations, heterogenous IT environments, and a variety of clinical workflows.

Level 0
Password-based access

Level 1
Reduce passwords
Clinicians authenticate with tap-and-go and SSO

Level 2
Achieve targeted passwordless

Go passwordless where it benefits clinicians and security the most

Improve the user experience while increasing acceptance for longer passwords

Level 3
Mask passwords for all end user workflows

Users never need a password

Legacy systems do not need to be replaced but can be secured through password rotation

Password related cyber risk is significantly reduced at this stage

Level 4
End-to-end passwordless

Passwords no longer exist in any systems further reducing the attack surface

Learn more by downloading the comprehensive whitepaper The journey to passwordless for healthcare