

HEALTHCARE'S PROBLEM WITH PASSWORDS

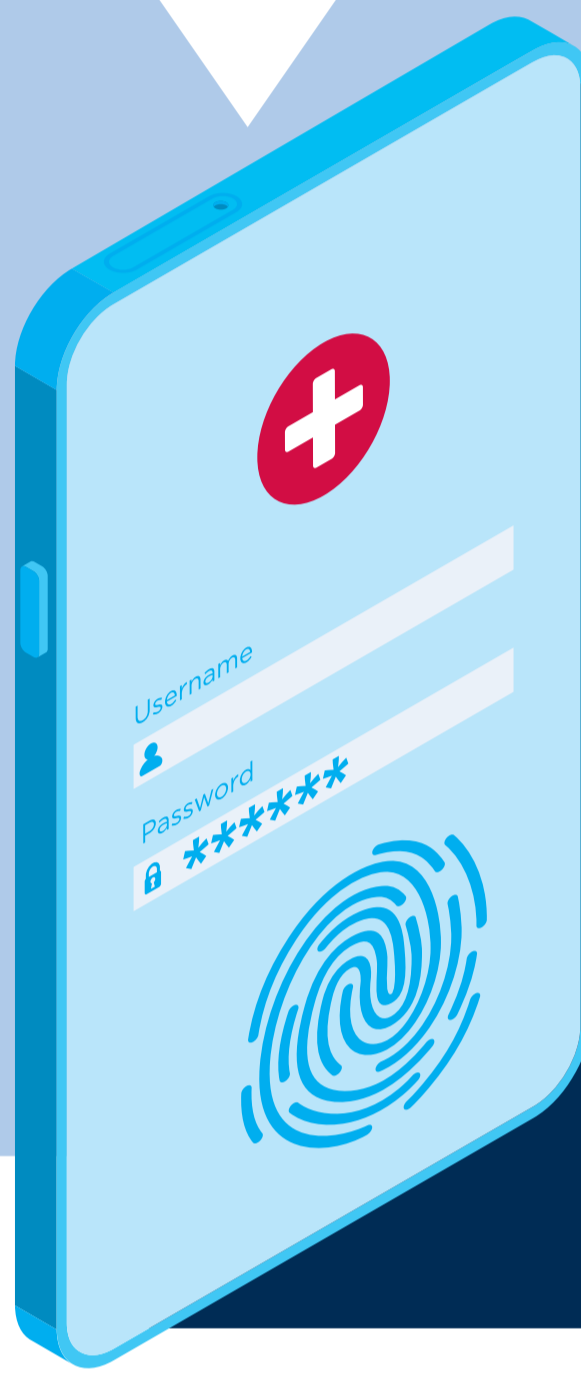


Healthcare workers are tasked with many things:

- Providing quality patient care
- Protecting patients' privacy
- Meeting regulatory requirements
- Keeping themselves safe

(All under extreme time constraints)

As part of their job, they are required to log in to multiple systems dozens of times per shift.



- Parking areas
- Building entrances
- Time and attendance clocks
- Personal workstations or floors
- Special access areas
- Sterile core areas
- Medication dispensaries
- Hospital information systems
- Electronic health record (EHR) applications
- Expensive treatment equipment
- Secure printers
- Laundry services

Logging into systems with passwords so many times each day is more than inconvenient — it poses a real security and **financial risk.**

- ▶ More than **85%** of healthcare organizations had data breaches in the past two years
- ▶ Data breaches cost healthcare **\$6.5M**
- ▶ Compromised, weak and reused passwords cause **81%** of data breaches¹
- ▶ **51%** of people reuse work passwords in their personal lives²
- ▶ **44%** of people know the risks of reusing passwords but do it anyway³

SINGLE SIGN-ON: A CURE FOR THE COMMON PASSWORD



Simple

Single sign-on (SSO) allows authorized personnel to log-in to systems with a swipe of the federally mandated picture ID badge they're already used to displaying.

- No passwords to remember
- No calls to IT for forgotten passwords
- No exposed and vulnerable areas or information



Cost Saving

A recent study of 19 facilities showed that SSO saved an average of 2,584 hours of mixed clinician time per facility per year.

That's a total dollar value of \$3,201,001 for the 19 facilities (\$168,474 per hospital).

SSO also eliminates 90% of lost/stolen password helpdesk calls.



Secure

SSO helps healthcare facilities maintain compliance and keep sensitive areas, equipment and patient data secure. For even stronger protection, facilities can add multi-factor authentication (MFA).

MFA prevents up to 99.9% of attacks.⁴

While 54% of people use MFA on their personal accounts, only 37% use MFA on work accounts.

For more on how using ID credentials with RFID contactless technology helps boost productivity, maintain compliance and save costs, read our executive brief, ***Spend More Time with Patients and Less Time with Passwords***. Discover HID Global's full portfolio of healthcare solutions at hidglobal.com/healthcare.

¹ <http://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report/#:~:text=80%25%20of%20hacking%2Drelated%20breaches,has%20been%20widely%20cited%20since.>

² <https://dataprot.net/statistics/password-statistics/>

³ <https://www.lastpass.com/resources/psychology-of-passwords-2020>

⁴ <https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>