WHITEPAPER

A CISO’s worst fear and greatest hope: C0mp1ex_P@55w0rdz

imprivata®

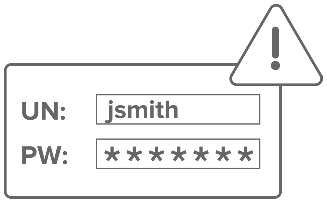
Exhaustion abounds for the CISO and other security warriors trying to unfailingly secure technology in a human world.

Humans – both the good-minded who want to comply and keep your HDO secure, as well as not-so-good-minded – pose internal threats based on behavioral interactions with technology. Sadly, healthcare records, which contain information about our most human vulnerabilities, are also the most valuable records on the dark web.

An increase in cyberattacks and a broader attack surface due to a mobile workforce only further complicate protection.

And this all comes at a time when the healthcare industry was already tackling increasingly tighter margins and the challenges of navigating value-based care – before the compounded complications of the COVID-19 virus hit.

According to IBM's annual "Cost of a Data Breach 2021"[1] report – and despite the industry's increased focus on security and compliance – 20% of breaches were initially caused by compromised credentials. Further, for the eleventh consecutive year, healthcare experienced the highest cost of a data breach.



20%

of breaches were initially caused by compromised credentials

Striking a balance between security and ease of access

A common approach to mitigating the threat and potential impact of a data breach is to implement complex 16+ character passwords that make user access to clinical systems and applications harder. While these complex passwords go a much longer way in offering security protections, clinicians often equate the idea of security with barriers and frustration. Frequently referred to as "security friction," the concept suggests that most people will default to convenience when an extra effort is required. Unfortunately, security friction can lead to workarounds that compromise protections adopted for security in the first place.

Think about this: clinicians who typically have only 12 to 15 minutes to spend with their patients have very little time to focus on complex security barriers. It's even tougher for surgeons and other clinicians who may be doing an emergency laparotomy, inserting a heart stent in the operating room, or who are focused on other medical procedures. At the point of care, clinicians at your facility want to focus their precious time on what matters most: patient care.

It's a key challenge in healthcare – trying to balance the protection of huge amounts of personal and medical data with clinicians' need for fast access to that data to successfully treat patients.

When IT and security teams design systems that force clinicians to enter complex usernames and passwords multiple times during their shifts, workarounds are inevitable – clinicians will share usernames and passwords or leave workstations unlocked. If IT and security teams do nothing to head off these threats, both the organization's risk and impact of a breach can increase.

Clinician adoption is essential to a strong security infrastructure

What is most important to healthcare CISOs and other security professionals? Ensuring that their organization is as secure as possible without slowing down clinicians who want to provide often rapid care for patients.

Leading healthcare facilities are using strong, multifactor authentication and single sign-on (SSO) to make it easier for clinicians to adopt new technologies. With this type of secure access in place, clinicians can simply tap their badges or scan their fingerprints to authenticate into their clinical systems and applications. This capability enhances their experience with technology, bolsters security, and allows clinicians to focus on patients.

Many healthcare organizations globally have already taken this step and invested in a single sign-on and authentication management platform to:

- Enable organizations to implement 16+ character strong passwords to avoid credential breaches without introducing security friction
- Stop waste of clinical time with manual password entry an average of 70+ times per day
- Drive clinician satisfaction and productivity with the EHR
- Empower clinicians with self-management of their passwords to reduce calls to your help desk

CONTINUE READING ›