LastPass for healthcare

The healthcare industry includes hospital systems, medical services, pharmaceuticals, medical device manufacturers, health insurers, public health providers, and research and development institutions, all aimed at maintaining and improving health. It involves a complex network of professionals, facilities, and technologies.

Preventing unauthorized access is vital for healthcare providers

Healthcare providers have a critical responsibility to protect sensitive patient and customer data, including Personal Health Information (PHI), healthcare records, and financial details related to patients, providers, and vendors. Cybercriminals increasingly target the healthcare sector, where poor password management and inadequate access controls create significant vulnerabilities. Granting unnecessary access or delaying access revocation for part-time staff, contractors, and temporary employees increases the risk of unauthorized access as security gaps widen.

Healthcare organizations adopting cloud-first strategies face growing challenges in securely managing passwords and access across various digital tools and platforms. Misconfigured cloud infostructure, outdated workstations, and unsecured shared devices create security gaps while rapid SaaS adoption often leads to “SaaS sprawl,” with unauthorized apps compromising security further. Without a centralized password management system, maintaining control over access and ensuring secure, consistent password practices becomes even more difficult.

Healthcare providers must comply with stringent regulations like HIPAA, HITECH, and ACA, requiring ongoing audits to prove compliance. Proper password management is crucial to avoid penalties and reputational damage. Failure to secure credentials and access rights increases risks around data privacy, compliance, and cyber insurance, leading to significant financial consequences.

The US Department of Health and Human Services (DHHS) found that large data breaches increased 93% between 2018 and 2022, with large ransomware breaches increasing 278% during that same period.

Treat passwords like you do your patients: with the utmost care

As a trusted global leader in password and identity management, LastPass is uniquely positioned to solve the cybersecurity, efficiency, and compliance challenges that healthcare providers face. Designed specifically to meet the complex demands of a credential-driven industry, LastPass creates, stores, manages, and shares credentials across teams and departments, without compromising on security, privacy, or accessibility. Providers can reduce the risks associated with weak or mismanaged passwords, enabling them to focus on delivering quality care while staying secure.

Healthcare organizations must balance strict security with a user-friendly experience for IT admins, end users, and third-party collaborators like contractors, vendors, and temporary staff. LastPass delivers a cloud-native solution that simplifies credential management while meeting these requirements. It safeguards sensitive credentials and ensures secure access and sharing across internal and external teams. With LastPass, healthcare providers can implement granular, security-driven access policies that help prevent unauthorized access, mitigate insider threats, and reduce human error.

Additionally, robust reporting capabilities provide visibility into user activities, ensuring compliance with regulations like HIPAA, HITECH, and others. LastPass empowers organizations to stay ahead of the growing cybersecurity challenges in the healthcare industry, ensuring both operational efficiency and regulatory adherence.

LastPass

LEARN MORE

LastPass benefits for healthcare

The easiest, most affordable, and most reliable way for healthcare organizations to slash cyber and operational risk is to standardize password management with LastPass company wide.

Secure	**Prevent unauthorized access**	Help prevent threat actors and unauthorized users from gaining access to applications, online accounts, sensitive information, and systems.
	Stop account takeover and data breaches	Ensure the reliability and accessibility of online accounts and applications, and the privacy of credentials.
	Control shadow IT	Give organizations visibility into and management over unapproved and over-provisioned SaaS apps, allowing administrators to track credential sharing, manage access privileges, and spot vulnerabilities.
	Extend secure access management	Integrate seamlessly with major identity providers (IdPs) like Microsoft Entra, enhancing user management throughout the employee lifecycle.
Comply	**Meet cyber insurance requirement**	Make it easy for organizations to meet password and access management requirements for cyber insurance.
	Support compliance	Aids organizations in meeting compliance standards set by regulations like GDPR, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA, and SOX, as well as cybersecurity frameworks such as NIST, CISA, Zero Trust, and NERC-CIP.
	Meet partner security requirements	Helps organizations comply with strict partner security standards through robust access controls, password sharing rules, strong authentication mechanisms, and actionable reporting.
Streamline	**Deliver intuitive experiences to every user**	Offers hundreds of customizable policies, flexible privileges, detailed reporting, and various authentication options, making it an indispensable tool in a tech stack.
	Standardize password protection	Simplify credential management for employees across the entire organization.
	Alleviate help desk friction	Reduce the burden on IT helpdesks caused by frequent credential issues, such as lost passwords and account lockouts.
Collaborate	**Maximize teamwork through sharing**	Streamline password and information sharing both inside and outside the company, helping to boost productivity and efficiency for partners, freelancers, and remote workers.
	Maximize adoption + usage	Boost adoption and usage among employees by offering an intuitive and user-friendly interface that simplifies password management tasks.
	Promote a security culture	Help administrators ensure all employees actively contribute to a security-focused culture, protecting against common threats like leaked or stolen credentials to uphold fiduciary responsibility.

LastPass

LEARN MORE