RESOURCE CENTER

Why healthcare data security is a business priority

Get the full interactive view at https://bitwarden.com/sv-se/resources/why-healthcare-data-security-is-a-business-priority/

bitwarden

Table of Contents

Why the healthcare industry is a top target for cyberattacks

The healthcare industry has emerged as a prime target for cyberattacks, particularly due to the value of electronic health records (EHR). Healthcare providers are prime targets for malicious attackers for many reasons. They have access to immense amounts of valuable digital patient information on the black market, as well as a very complex IT environment comprising various connected devices, outdated operating systems and software, and a sprawling third-party software supply chain network. These issues are compounded by a lack of funding for trained security teams and technology and insufficient government guidance, leaving the sector vulnerable to persistent cyberthreats.

This article will dive deeper into why the healthcare industry is a top target for cyberattacks, backed by statistics from trusted sources and research-driven reports. Read on to learn why every healthcare organization needs a strong password manager to protect its bottom line and achieve stronger healthcare data security.

The importance of healthcare data security

Healthcare data security is paramount in today’s digital age, where sensitive patient information is increasingly stored and transmitted electronically. Protecting this data from unauthorized access, use, or disclosure is not just a regulatory requirement but a fundamental aspect of maintaining patient trust and the reputation of healthcare organizations. Effective data security measures ensure the confidentiality, integrity, compliance, and availability of sensitive healthcare information. Each of these is crucial for delivering quality care and safeguarding patient privacy. By prioritizing healthcare data security, organizations can mitigate risks, prevent data breaches, and foster a secure environment for both patients and healthcare providers.

The vulnerability of healthcare data

The data security challenges facing the healthcare industry are multifactorial. Healthcare records are a treasure trove of sensitive information, including personal identifiers, medical history, insurance details, and even financial data. Cybercriminals aim to monetize this type of information on the dark web, making healthcare organizations an attractive target.

Historically, the healthcare industry has lagged behind when it comes to digital transformation and updating systems. This leads to a corresponding lag in updating legacy software and patching existing operating systems and connected devices, creating a weakened organizational security posture. The increasing use of electronic health records (EHR) and patient portals has created a bigger attack surface.

Similar to other highly regulated industries, the healthcare space is underfunded and understaffed to properly tackle security threats, resulting in vulnerability blind spots. A complex IT environment comprising connected devices and disparate third-party vendors requires careful monitoring to ensure security resilience. When IT teams are ill-equipped, healthcare institutions find themselves increasingly vulnerable to incidents that can cause widespread outages that risk patients’ lives and their data.

Government agencies have recently released more guidance aligning with the National Institute of Standards and Technology (NIST) cybersecurity framework to harden healthcare security posture and prioritize healthcare data security. High-profile attacks like the Change Healthcare ransomware attack disrupted insurance claims and electronic pharmacy refills, indicating there’s more work to be done. Deterrent measures such as public-private sector information sharing, general security education and awareness, and greater investment in security teams must be priorities, rather than afterthoughts.

Recent data highlights the healthcare industry's vulnerability to cyberattacks and data breaches. IBM's report on the average cost of a data breach revealed that the healthcare industry experiences the most costly data breaches. And to make matters worse, public reports of hacking incidents targeting healthcare data are increasing rapidly.

The annual data breach report published by the Identity Theft Resource Center (ITRC) revealed the healthcare sector has led all industries in the number of reported breach incidents every year for the past five years.

Challenges facing healthcare data managers

Healthcare data managers are on the front lines of protecting sensitive healthcare data, facing a myriad of challenges in an ever-evolving digital landscape. The sheer volume and complexity of healthcare data, driven by the widespread adoption of electronic health records (EHRs) and the proliferation of connected devices, make data management and security increasingly difficult. These advancements, while beneficial, introduce new vulnerabilities, such as data breaches and unauthorized access. Additionally, compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) adds another layer of complexity, requiring significant time and resources to ensure adherence. Protecting sensitive healthcare data in this environment demands robust security strategies and continued vigilance.

Common healthcare data threats

Healthcare data is susceptible to a variety of threats, each posing significant risks to patient privacy and organizational integrity. Data breaches, often resulting from unauthorized access, theft, or loss of sensitive patient data, are a primary concern. Ransomware attacks, where threat actors demand a ransom to restore access to compromised systems, can severely disrupt healthcare operations. Phishing scams, which trick individuals into revealing sensitive information like login credentials or financial details, are also prevalent. Healthcare organizations must remain proactive, implementing comprehensive security measures and awareness training to protect against these threats and ensure the safety of patient data.

Data shows ransomware attacks on healthcare data are on the rise

The vulnerabilities discussed above have led to a rise in healthcare industry ransomware attacks. Attackers encrypt critical patient data and demand hefty ransoms for decryption keys, causing downtime and compromising patient care. In November 2023, Nashville-based Ardent Health Services was targeted by a ransomware attack that forced it to divert ambulances and reschedule elective procedures. In November 2023, a US Department of Health and Human Services (HHS) hearing revealed that the vulnerabilities plaguing larger health systems are even worse in rural areas lacking the infrastructure of major metro area counterparts.

In 2023, reports revealed that ransomware attacks cost healthcare facilities $77.5 billion in downtime. Organizations like Tenet Healthcare reported a $100 million loss attributed to a ransomware attack, and Scripps Health estimated losses of nearly $113 million primarily due to lost revenue and recovery costs.

Healthcare facilities can mitigate ransomware-related damage by minimizing their attack surfaces. Simple tactical ways include patching vulnerabilities and updating software, training and educating employees who handle the most critical data, and engaging in strategic pentesting to assess areas of weakness. Organizations should also ensure they leverage one of the most effective security tools: an enterprise-wide password manager to protect patient data.

Read more:
How to choose the best enterprise password manager for your business

How password managers mitigate threats targeting healthcare data

Another recent report revealed that 42% of healthcare organizations experienced a cyberattack due to insecure system entry points. To combat these threats effectively, every healthcare organization needs to prioritize cybersecurity measures, and password managers are a cost-efficient solution that can be implemented quickly for immediate impact.

42% of healthcare organizations experienced a cyberattack due to insecure system entry points.

2023 Ponemon Institute Report

Implementing a HIPAA-compliant password manager like Bitwarden enables healthcare organizations to generate and manage strong and unique passwords for various systems and accounts, reducing the vulnerability to password-related breaches. Other key benefits include:

- Strengthening authentication with seamless single-sign-on (SSO) and directory integration options.
- Enforcing strong password policies such as minimum password length and two-factor authentication adds an extra layer of security.
- Protecting against credential stuffing and brute force attacks by eliminating the need to memorize or reuse weak passwords for multiple accounts and ensuring employees can share credentials securely.
- Simplifying compliance with data protection regulations like HIPAA.

Additionally, password managers allow for the enforcement of robust password policies, like two-factor authentication (2FA), adding an extra layer of security. By centralizing and encrypting login credentials, healthcare organizations can mitigate the risk of unauthorized access and credential-stuffing attacks.

Other best practices for protecting healthcare data

Protecting healthcare data requires a comprehensive approach that encompasses robust security measures, employee training, and regulatory compliance. Along with implementing an enterprise-wide password manager, key best practices include:

- **Implementing data encryption**: Protect sensitive data both in transit and at rest to prevent unauthorized access.
- **Using antivirus software**: Detect and prevent malware that could compromise healthcare systems.
- **Providing employee training**: Educate staff on security best practices and raise awareness about potential threats.
- **Conducting regular security audits**: Perform risk assessments to identify and address vulnerabilities.
- **Ensuring regulatory compliance**: Adhere to regulations such as HIPAA and the Health Information Trust Alliance (HITRUST) to maintain data protection standards.

By following these best practices, healthcare organizations can effectively protect sensitive patient data, maintain compliance, and uphold the trust of their patients.

Why Bitwarden is the trusted cybersecurity solution for healthcare organizations

Bitwarden is an open source, enterprise-grade password manager that simplifies the process of generating, storing, and securely sharing unique passwords on any device. For larger healthcare entities that require centralized control over password security, Bitwarden supports advanced features like flexible Single Sign-On (SSO) integration options, LDAP directory service connectors, API access, custom management roles, and activity monitoring through detailed event and audit logs.

HIPAA regulations stipulate that systems used for storing personal health information (PHI) must adhere to HIPAA compliance even when data is encrypted. That’s why Bitwarden has committed to achieving HIPAA compliance, certified by a third-party auditor, to serve as a trusted Business Associate for healthcare organizations subject to HIPAA regulations.

Get started with Bitwarden

To explore Bitwarden business features and capabilities, get started with a free trial today.

You may also like:

Why use a HIPAA-compliant password manager

HIPAA Password Requirements Explained