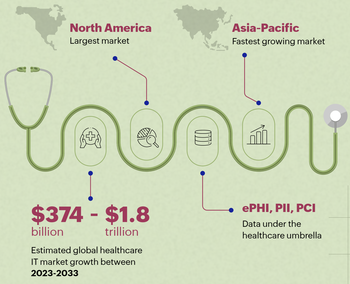
ManageEngine
DataSecurity Plus

Healthcare data security: Challenges, costs, and safeguards



Why does data security matter in healthcare?

Protect patient privacy and confidentiality

People will disclose health information only if they trust their data will be secure.

Data theft

Stolen medical records can be used to create fraudulent insurance claims.

Disruption of medical services

Disruptions lead to delayed treatments, and that puts lives at risk.

387 breaches

7 breaches of **1 million** or more records

45,555,982 stolen records in total

77% of breaches were due to a hacking or IT incident. Hacking and IT incidents cover a broad range of security incidents, including hacks, ransomware, malware, and phishing attacks.

278% increase in ransomware attacks from **2018 to 2023**

93% increase in large data breaches from **2018 to 2023**

These are all just from the **first half of 2024 - just in the United States.**

Cost of a data breach

Healthcare **$10.93 million** | Other industries **$4.45 million**

is the average cost of a data breach in U.S. in 2023.

The reason is two-fold:

1 Expensive breach recovery

a. High volume and complexity of data

b. Multiple parties involved in data handling (healthcare providers, business associates, insurance providers, clearinghouses, etc.)

2 Highly regulated industry

a. High penalties levied by HIPAA

b. Additional penalties based on relevant state laws

What makes securing healthcare data hard?

- Outdated software, obsolete devices, and unpatched vulnerabilities
- Increased digital environments, like telehealth and remote patient monitoring
- Human error, like mishandling data or falling for phishing scams
- Limited budgets to enforce security measures

Top 5 threats to the healthcare industry

Ransomware attacks could literally hold lives hostage in exchange for monetary benefit, and the institutions would have to pay.

A supply chain attack on any one of the hundreds of SaaS applications that healthcare organizations use could spread across systems and bring operations to a halt.

Exploiting the vulnerabilities in increasingly interconnected medical equipment could directly disrupt the timely delivery of critical healthcare services.

Insider threats, like employees or third-party contractors mishandling information, sharing credentials, or even deliberately leaking data.

A DDoS attack could prevent hospital administration from accessing patients' records, appointments, test results, and insurance information.

Simply put, invest in a solution that can help you simplify data security and let you focus on providing healthcare.

Let that solution be DataSecurity Plus.

ManageEngine DataSecurity Plus is a unified data security posture management platform that helps you locate all sensitive data in your storage environment; monitor it; and protect it from unauthorized access, modification, and exfiltration.

ManageEngine
DataSecurity Plus

Download a free trial | Get Quote

Sources: Mordor Intelligence | HIPAA Journal | HHS | Security Intelligence