SHARDSECURE

DATA PROTECTION FOR HEALTHCARE ORGANIZATIONS

Healthcare organizations face a wide range of challenges in keeping patient and organizational data safe from cyberattacks. From breaches to supply chain attacks, complex threats threaten the daily operations of healthcare systems and the privacy rights of patients. To learn more about these threats, check out ShardSecure's prescriptions for strong data protection

Inoculate your organization against ransomware.

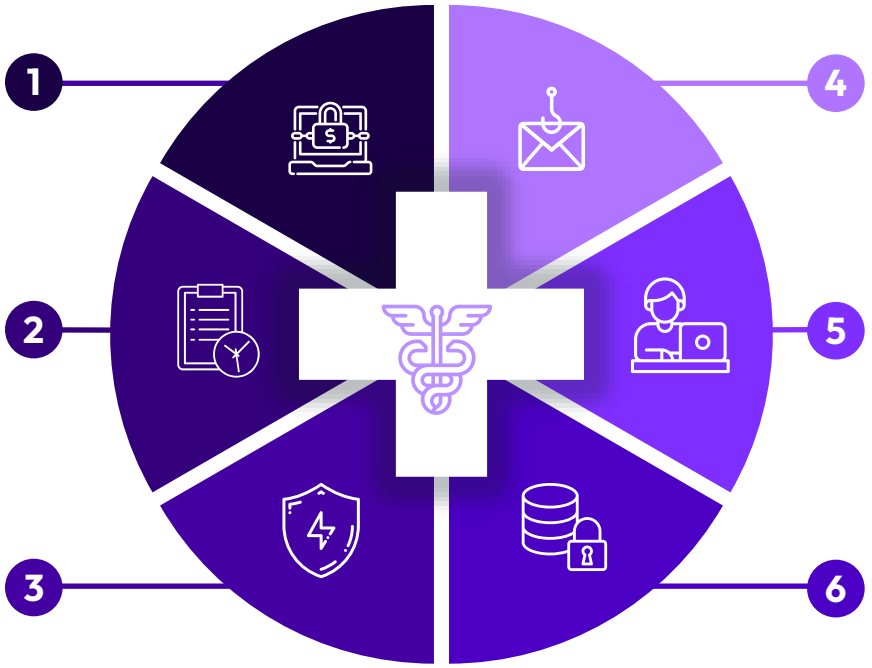
A shocking 60% of healthcare organizations reported being attacked by ransomware in 2022, nearly double the rate reported by the sector in 2020. In over a third of attacks, sensitive data was not only encrypted but also exfiltrated for double extortion. To mitigate ransomware, organizations should employ strong backup solutions, prepare response and recovery plans, and invest in threat detection tools.

Maintain compliance with data privacy regulations.

From the CCPA to the GDPR, data privacy regulations require that personal identifiable information (PII) be protected. At the same time, the Health Insurance Portability and Accountability Act (HIPAA) requires that healthcare organizations safeguard patient privacy. To avoid major fines, organizations must establish clear data handling procedures and implement robust data privacy measures.

Protect patient confidentiality beyond HIPAA.

Although it's seen as the gold standard for patient privacy, HIPAA leaves some major gaps. The law places most of the privacy burden on organizational awareness rather than technological safeguards, and it doesn't cover certain kinds of personal health data. To make sure patients are fully protected, organizations must invest in advanced data privacy tools.



Cyberattacks are contagious. Make sure your vendors are secure.

The healthcare industry is at the highest risk of third-party data breaches, comprising over a third of such incidents in 2023. By targeting vendors like insurance companies, debt collectors, software providers, and outpatient clinics, cyberattackers can exploit the sector's vulnerabilities. Robust access controls and security solutions can help combat supply chain attacks and restrict third-party access to sensitive data.

Update legacy systems and IoMT devices.

Cyberattackers often gain access to healthcare networks via outdated software and vulnerable Internet of Medical Things (IoMT) devices like glucose monitors and surgical robots. Although it's easier said than done, updating or replacing these unpatched devices and systems can help address weak points and prevent access to sensitive patient data.

Your patients are resilient. Your data should be, too.

Most hospitals have emergency generators for power outages but lack solutions for cloud outages. Unavailable data can complicate patient treatment and disrupt daily operations, so organizations should invest in a robust data resilience solution that keeps data accurate and available.

The ShardSecure platform enhances data privacy, security, and resilience, helping healthcare organizations protect their digital health against a number of top cyberthreats. To learn more, visit our healthcare page and take a look at our resources.