

# Data Security Platform for Healthcare

Ensure compliance while protecting patient data from ransomware & insider threats

BrickStor SP eliminates the complexity of healthcare's top three data management challenges: data protection, compliance, and integrity. This unified approach to data security reduces the cost and complexity associated with bolt-on security offerings.

## Meet Electronic Health Records Requirements

**Archive and Records Disposition** – Maintain immutable copies and demonstrate when data has been purged or deleted.

**Regulatory Compliance and Reporting** – Generate automated reports to demonstrate compliance for audits, investigations, legal holds, and regulations.

**Data Protection** – End-to-end data integrity checks with automated snapshot and replication policies ensure your primary and secondary data copies are intact and protected.

## Ransomware Protection

BrickStor SP actively evaluates trust for each file operation in real time based on client IP, user account, file activity and other behavioral identifiers to provide the security and visibility necessary to defend against modern attacks. When BrickStor SP detects irregular or malicious behavior, it can alert your organization's security or infrastructure team and stop the user and host from being able to steal, manipulate and access files until the behavior is investigated and mitigated.

## Zero Trust Data Security

BrickStor's data-centric zero trust architecture protects your data at the source. User behavior analytics identify and stop insider threats and other breaches in real time.

“ In **2023**, the healthcare industry reported the most expensive data breaches, at an average cost of **10.93M.** ”

- Cost of a Data Breach Report, 2023  
IBM Security and Ponemon Institute



According to the Office of Civil Rights, breaches between 2009 and 2023 resulted in the exposure of **519,935,970 healthcare records.** That equates to more than 1.5x the population of the United States.

- HIPAA Journal