CASE STUDY

storageMAP

TURNING DATA RISK INTO DATA CONTROL IN HEALTHCARE

A large U.S. healthcare services organization manages millions of patient records across billing, claims, and clinical systems. Like many healthcare providers, the organization must retain certain records for compliance while also protecting highly sensitive PHI and PII.

A few years ago, unauthorized actors gained access to the organization's network, exposing sensitive information belonging to more than 3.5 million beneficiaries. The compromised data included names, Social Security numbers, insurance information, and medical treatment details.

The breach triggered multiple class action lawsuits, placing the organization at risk of tens of millions of dollars in potential legal settlements. Leadership quickly realized that retaining large volumes of unnecessary sensitive data significantly increased both security and legal risk.

THE CHALLENGE: TOO MUCH SENSITIVE DATA, TOO LITTLE VISIBILITY

Following the breach, senior leadership mandated a new policy to reduce risk by identifying and archiving ROT (redundant, obsolete, and trivial) data.

Managed care services organizations are challenged with balancing 10-year CMS retention requirements that drive data growth, with archiving aging beneficiary data that no longer needed to remain in active production systems.

The IT team faced major obstacles:

- Sensitive data scattered across hundreds of terabytes of unstructured storage.
- Limited visibility into which files contained PHI or PII.
- Manual identification and migration processes that could not scale.

Initial attempts to locate and move the data manually, supported by existing data governance tools, proved too slow and too complex.

Without an automated solution, the organization could not effectively put their data retention policy into practice.

THE SOLUTION: AUTOMATING SENSITIVE DATA DISCOVERY AND ARCHIVING

To address the challenge, the organization implemented Datadobi's unstructured data management platform, StorageMAP, specifically for archiving purposes.

StorageMAP enabled the IT team to automatically:

- Identify files older than 10 years containing sensitive beneficiary data to meet the CMS-governed retention threshold.
- Apply policies to locate ROT data across large storage environments.
- Move qualifying data to a secure archive target.

With automated discovery and policy-based data movement across billions of files, the organization was finally able to implement the data governance strategy required by senior leadership.

THE RESULTS: STRONGER DATA GOVERNANCE AND REDUCED LEGAL RISK

With StorageMAP in place, the organization was able to significantly reduce the amount of unnecessary sensitive data stored in production environments, ultimately minimizing future breach liability and removing millions of PHI records from exposure.

GREATER DATA VISIBILITY

The IT team could now quickly identify aging files and sensitive data across large storage environments.

POLICY-DRIVEN ARCHIVING

Automated workflows ensured that older sensitive data was securely archived according to organizational policies.

REDUCED SECURITY AND LEGAL EXPOSURE

By removing unnecessary PHI and PII from production systems, the organization reduced the risk of future breaches and legal liabilities.

THE TAKEAWAY: PROACTIVE DATA GOVERNANCE REDUCES RISK AND LIABILITY

Healthcare organizations face increasing cybersecurity threats and rising financial consequences from data breaches.

By proactively identifying and archiving unnecessary sensitive data, this healthcare provider transformed its data management strategy—from reactive breach response to proactive risk reduction.

With StorageMAP, the organization gained the visibility and automation needed to secure sensitive data, improve compliance, and dramatically reduce future liability.