CASE STUDY

storageMAP

STRENGTHENING DATA GOVERNANCE AFTER A MAJOR PRIVACY INCIDENT

A large financial services organization found itself under intense scrutiny following a combination of regulatory examinations and data exposure events in the industry.

While the incident originated outside the company, the event triggered a deeper internal review of how sensitive data was being stored, retained, and managed across the organization's infrastructure. That review uncovered a critical issue: the company was not meeting its own record retention policy.

For the executive responsible for distributed infrastructure, storage platforms, and data protection, the implications were significant. Retention policies, driven by SEC/FINRA recordkeeping rules, privacy regulations, and internal standards, coexist to limit legal exposure and protect customer information.

If the organization could not demonstrate compliance, it risked escalating legal costs, regulatory pressure, and long-term reputational damage.

THE ORGANIZATION NEEDED TO ACT QUICKLY.

THE CHALLENGE: MULTI-PETABYTE VISIBILITY

The day-to-day responsibility of addressing the issue fell to the storage operations team. The problem wasn't understanding what needed to happen — the company had a clear policy. The challenge was actually enforcing it.

The organization's storage environment had grown to multiple petabytes of data spread across several platforms and vendors. Over the years, massive volumes of data had accumulated, including:

- Aged data that should have been archived.
- Orphaned files with no clear owner.
- Potentially sensitive information stored in production systems.

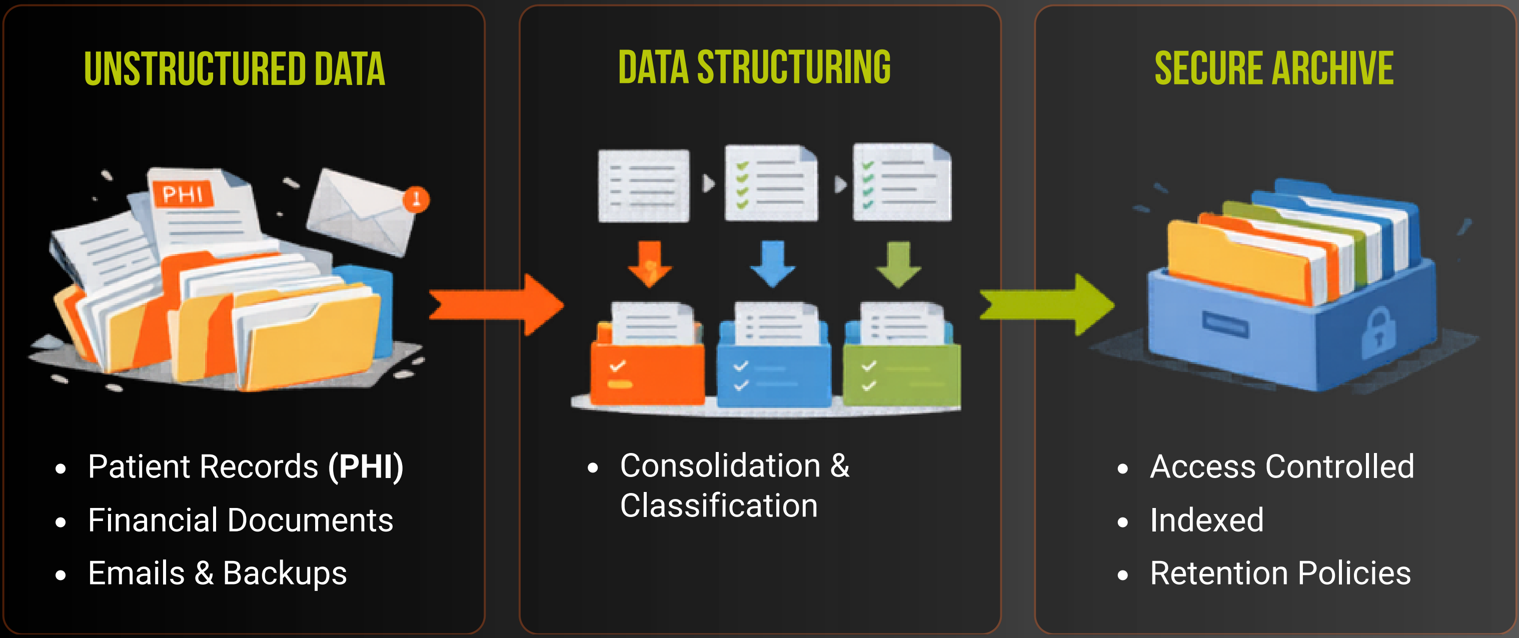
The team attempted to use existing reporting tools to analyze the environment, but the tools were not designed to scan datasets of this scale. Running full analysis across the environment simply wasn't feasible within the available time or resources.

Meanwhile, legal pressure was mounting. Leadership needed a path forward that would allow them to:

- Identify non-compliant data.
- Enforce retention policies.
- Reduce the organization's risk exposure.

THE TURNING POINT: GAINING VISIBILITY AND CONTROL

With StorageMAP, the team could finally map multi-petabyte unstructured datasets to their record retention obligations, identifying aged data that no longer needed to be kept, orphaned content with no business owner, and sensitive data that required tighter governance. Those insights became the basis for a defensible minimization program.



UNSTRUCTURED DATA

- Patient Records **(PHI)**
- Financial Documents
- Emails & Backups

DATA STRUCTURING

- Consolidation & Classification

SECURE ARCHIVE

- Access Controlled
- Indexed
- Retention Policies

Working alongside the organization’s cloud team, the infrastructure team used StorageMAP insights to begin systematically archiving eligible data from production storage to a lower-cost object storage tier.

For the first time, the privacy and compliance teams gained clear reporting on what data existed, where it was located, and how it was being managed.

Using StorageMAP, the team was able to perform large-scale analysis across their multi-petabyte data footprint and identify:

- Aged data that no longer needed to remain in primary storage.
- Orphaned files with no business owner.
- Sensitive data types that required additional governance.

THE OUTCOME: REDUCED RISK AND STRONGER GOVERNANCE

By implementing StorageMAP, the organization was able to begin enforcing its retention policies and significantly reduce its exposure to future risk. Aged and orphaned data was moved off production systems and archived to cloud object storage, lowering infrastructure costs while improving governance.

Most importantly, the firm could now demonstrate meaningful progress toward protecting customer data and managing it according to established policies. For leadership, this meant more than operational efficiency. It meant reducing legal exposure, strengthening compliance posture, and restoring confidence in the organization’s data governance practices.