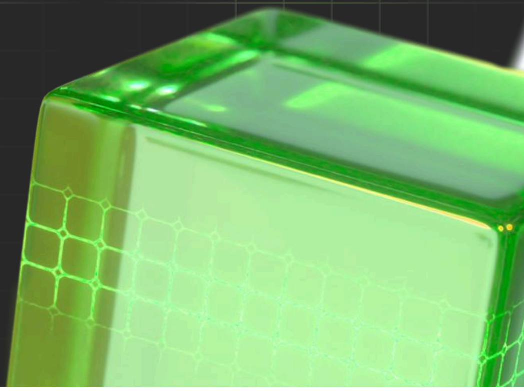
QOHASH

Healthcare: Use case

Managing Personal Health Information (PHI) in healthcare workflows to protect patient data and reduce risk



Problem statement

Data transformation efforts have had the unintended consequence of escalating the risks of sensitive data retention, particularly in highly regulated industries like healthcare.
In a whitepaper, CGI states:

> "As businesses, governments, and individuals become more reliant on these connections, valued data assets are increasingly vulnerable, and cybersecurity threats multiply. The rapid accumulation of sensitive data, coupled with the complexity of modern IT environments, creates an expanding attack surface that requires proactive risk management and resilience."
>
> CGI, Data to Diamonds - White Paper

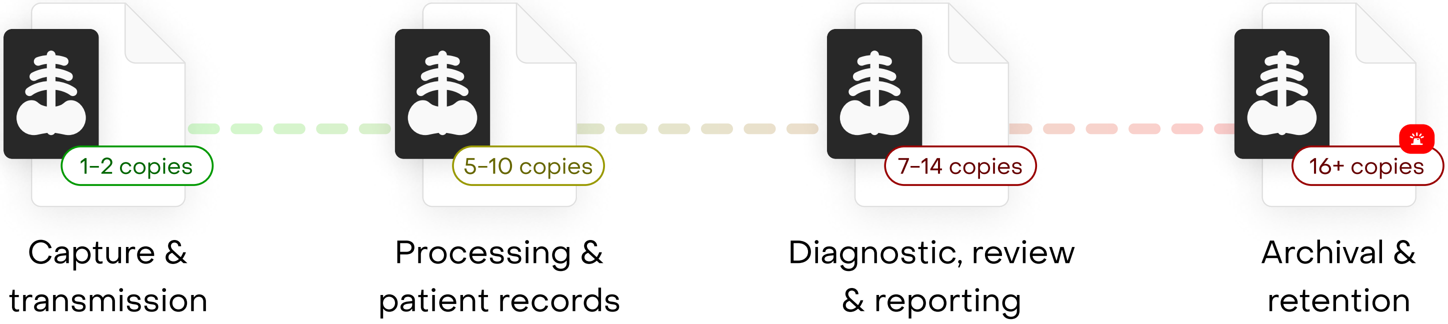
The increasing volume of Personal Health Information (PHI) in the healthcare sector further heightens the potential for data breaches, unauthorized visibility, and compliance violations.

The flow of PHI such as X-rays are essential to patient care, but can also present significant data security and compliance risks. A single X-ray file can traverse multiple departments, from radiology to referring physicians, administrative staff, and insurance providers. This proliferation results in numerous copies of the file stored across various systems, including:

- Electronic Health Record platforms
- Email and messaging systems
- Workstations and file servers
- Cloud and Network storage services

Patient workflows

Using the example of an x-ray, lets examine the issue of data retention across organizational workflows.



1–2 copies
Capture & transmission

5–10 copies
Processing & patient records

7–14 copies
Diagnostic, review & reporting

16+ copies
Archival & retention

Current state vs. desired future state

	Current state	Future state (with Qohash)
Visibility	Files with PHI are copied and stored in multiple locations without visibility.	Inventory sensitive data across repositories and real-time tracking of files containing SI.
Control	IT teams struggle to control data across systems due to file sprawl.	Tracks specific data elements, across files with precision. Effectively investigate and remediate incidents.
Compliance	Audits and compliance checks are reactive, consuming time and resources.	Proactive compliance management with automated classification and risk scoring.
Risk mitigation	There is a high risk of data exposure due to uncontrolled PHI copies.	Risk-based alerts notify security teams, users, or trigger automated risk-reduction workflows.
Operational efficiency	Time-consuming manual processes for tracking sensitive data.	Automated workflows reduce administrative overhead and enhance security.

How Qohash reduces PHI risk and enables compliance

Sensitive data tagging is a core feature of Qostodian, ensuring that all files with PHI, including X-rays, are appropriately tagged and controlled throughout their lifecycle. Key benefits include:

- **Automated tagging:** Qostodian applies predefined tags to files containing PHI within the platform through file properties and organizational policies.
- **Granular visibility:** Tagged files can be traced at employee, data element and data source levels, preventing unintended or unathorized accumulation.
- **Audit & compliance readiness:** Track when, how, and who has access to files containing PHI, streamlining HIPAA compliance audits.
- **Integration with security policies:** Tagged files within the platform can trigger security policies such as alerts, quarantine, retention enforcement, and deletion scheduling.

In addition to tagging capabilities, Qohash further strengthens PHI security through high probability information classification frameworks. Qohash's Qostodian platform provides a strong solution for tracking, classifying, and managing PHI in healthcare environments. Key capabilities include:

- **Purview labeling:** Apply labels in the Qostodian platform to files supported by Microsoft Purview for DLP policy creation.
- **Granular visibility:** Get high-fidelity results of sensitive data to enable rapid discovery and address the data risk attack surface.
- **File tracking:** Track the propagation of PHI in real time, enabling IT teams to substantiate data workflows against organizational policies and best practices.

As healthcare workflows are increasingly digitized, PHI proliferation demands robust data governance and monitoring to avoid penalties and reputational harm. Qohash's Qostodian platform provides visibility, control, and risk reduction workflows to safeguard PHI.

Qohash offers data security solutions focusing on unstructured data risk management. Our platform, Qostodian, enables organizations to automatically monitor, identify, and address high-risk data efficiently. Our expertise lies in managing everyday data accessible by employees in regulated and high-stakes environments, including financial services, healthcare, public sector, and high technology.

Visit our website www.qohash.com | visit our trust center trust.qohash.com

AICPA SOC 2 TYPE 2

AICPA SOC 3

ISO 27701

ISO 27001