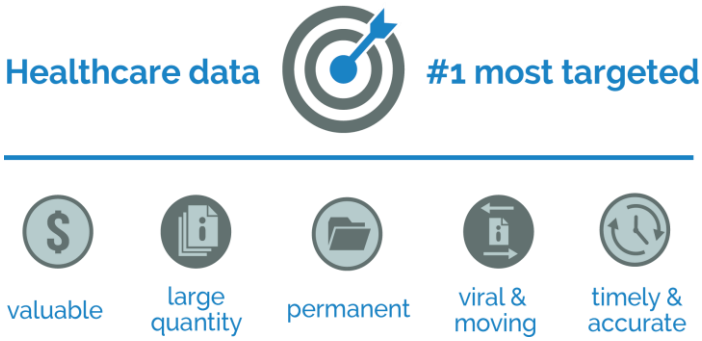
Discover. Classify. Protect. *SIMPLIFIED*

Healthcare is now the most targeted industry for cybercriminals, insider threats, and accidental disclosures. *CloudVault® Health* safeguards sensitive healthcare data, saving hospitals, physicians, insurance companies, and their business associates from costly breaches, HIPAA and Meaningful Use violations, and unintended disclosures. Unlike legacy solutions that focus on network or application perimeter security, CloudVault® Health's patented solutions protect the actual healthcare data itself, even when it moves outside the healthcare organization into multiple business associate domains across the chain of trust.

More Data = More Risk

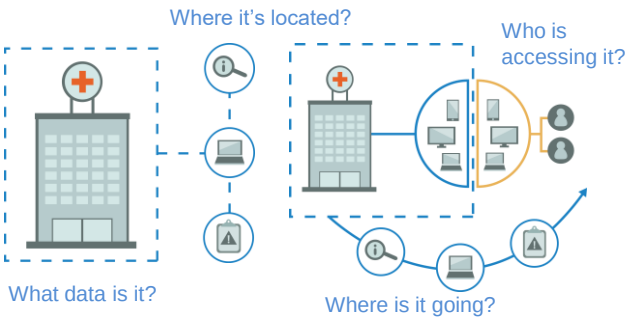
Every time a patient engages the healthcare system, gigabytes of data are created, and shared across the healthcare ecosystem. As this information propagates across stakeholders, healthcare organizations simply lose track of it, to the point where many healthcare organizations don't know where all their sensitive data exists out across their networks. So, it's not surprising that over 40% of all data breaches last year across all industries were in healthcare. What is surprising to some, is that the information shared with a physician is 10 times more valuable than the information shared with a bank, making healthcare data an appealing target.

With more data access endpoints, increasing government regulations like HIPAA Omnibus, and massive amounts of electronic patient data, the obvious question is: *"How does the industry keep all this healthcare data safe?"*



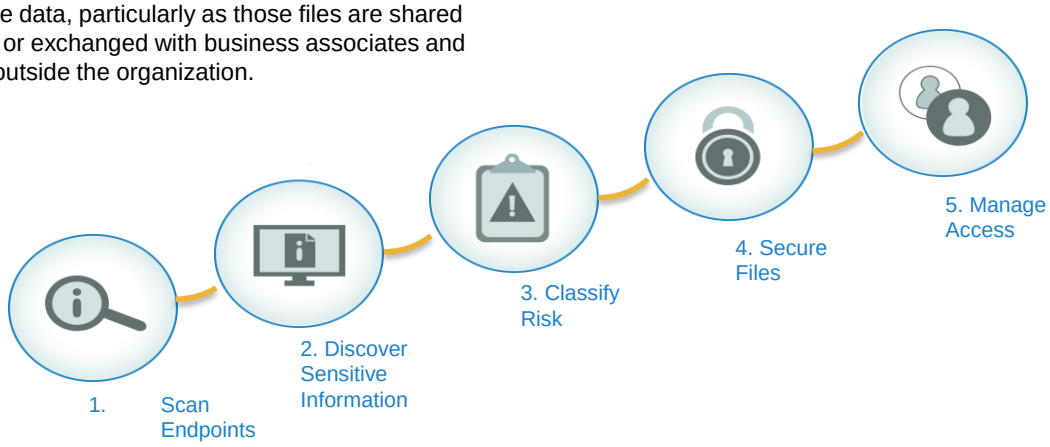
Start by knowing your data

The healthcare industry is being forced to address this situation thru legislation, litigation, and financial penalties. But before much of the risk can be mitigated, you have to know where all that sensitive information is, where it's going and who's accessing it. You simply can't protect something if you don't know where it is.



Five Pillars of Protection

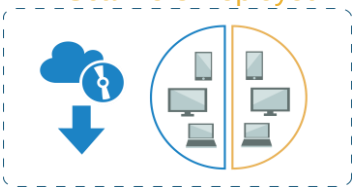
CloudVault Health's patented solutions protect healthcare information by ***Discovering, Classifying, Securing and Managing Access*** to the files that contain sensitive healthcare data, particularly as those files are shared internally or exchanged with business associates and vendors outside the organization.



Discover. Classify. Protect. *SIMPLIFIED*

How CloudVault Works – It's Simple

1. Scanners Deployed



Scanning agents are deployed to endpoints inside the network or outside the organization.

2. Endpoints Scanned

Endpoints are continuously scanned. Metadata collected about file activity on each endpoint

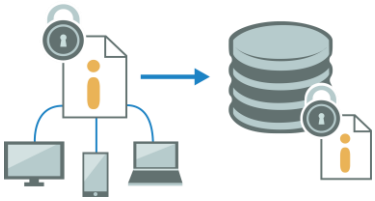
3. Metadata Collected & Analyzed

Metadata is analyzed and classified to discover PHI, PII, and other sensitive information or inappropriate activity

4. PHI Discovered and Classified by Risk Level

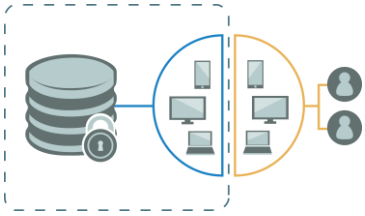
PHI and other sensitive information is discovered, risk classified and reported

5. Files Automatically Secured



Based on classification, files can be automatically encrypted, and moved securely to the Cloud

6. Manage Access

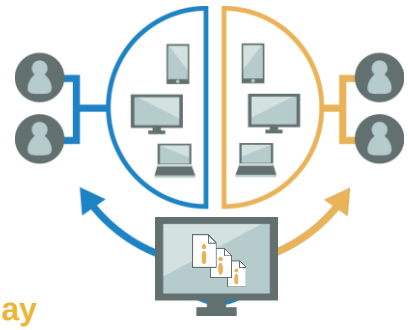


Internal and External users, with appropriate entitlements may securely access sensitive files.

Business Associate Agreement Compliance

Increased healthcare cyber risks have introduced new obligations into Business Associate Agreements. Once a document that merely acknowledged the exchange and general protection of healthcare information, Business Associate Agreements (BAAs) have become advanced, legally binding contracts, that place significant obligations, with meaningful penalties, on both Covered Entities and their Business Associates. The BAA process is increasingly complex, time consuming, and costly for all parties, and has become a significant barrier to sales for vendors that service healthcare organizations.

CloudVault Health aligns the policies and provisions within each BAA with the actual data governance practices in operation, and provides visibility of those practices transparently, to internal staff or outside parties, enabling the organization to meet or exceed its contractual and regulatory obligations



New Regulations = More Risk

HIPAA Omnibus 2013 requires covered entities such as hospitals and insurance companies to now be ***operationally*** and ***financially*** responsible for tracking and protecting all patient information throughout their service provider networks, including partners and vendors where up to 70% of all breaches occur.

Penalties Include

- Federal and state fines
- Balance sheet reserves
- Breech response & audit costs
- Civil and Criminal litigation
- Higher insurance premiums
- Serious brand damage

Start today

CloudVault Health's simple, automated deployment enables healthcare organizations to quickly improve their data protection posture, without dependencies on IT staff or planning another large scale IT project.

In a matter of hours, healthcare organizations can dramatically reduce their data risk, improve data protection policy adherence, and know with certainty, where their highly sensitive, highly regulated data actually is, not just where it is supposed to be!