How Varonis Helped a Regional Healthcare Network Lock Down At-Risk PII and PHI Across Their Hybrid Cloud

> If you work within a regional healthcare network, and your organization is poised for growth like we were, you need a way to prove that you have visibility and control over your unstructured data. If you don't have a solution like Varonis, you open yourself up to a lot of risk.

About this case study:

Our client is a mid-sized hospital and regional healthcare provider network in the US. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

- Protecting PII, PHI, and other sensitive information during a time of rapid business growth
- Minimizing the data blast radius with increasing use of shared drives and remote connectivity
- Ensuring data privacy protection measures continue to meet HIPAA standards

Solution

The Varonis Data Security Platform:

- Provides continuous and automatic visibility
- Identifies at-risk sensitive PII & PHI data in hard-to-find places
- Automatically classifies HIPAA-regulated data
- Monitors and alerts on anomalous activity that could lead to a data breach
- Automatically moves, archives, or deletes stale and sensitive data
- Simplifies compliance and e-discovery

Results

- Enhanced data privacy and security for over 2,500 employees
- Visibility into data and clear audit trails that show which users are accessing data
- Simplified DSARs, internal audits, and reporting for HIPAA compliance

CHALLENGES

Ensuring data privacy during rapid business growth

Hospitals and regional healthcare networks in the U.S. are responsible for securing the sensitive data for thousands of individuals.

This data includes information about employees, patients, projects, and operations. But as organizations continue to grow, it becames increasingly difficult to keep track of where data lives, who can access it, and whether that access is for legitimate purposes.

And as data grows, so does the blast radius — all the damage a bad actor could do if just one identity is compromised.

These were the challenge faced by the Network Admin of a mid-sized hospital and regional healthcare provider network (anonymous by request):

> **“When I started at the hospital, we had 4 servers and 50 desktops. Now, we have over 300 servers and 2,500 desktops.”**

For this organization, rapid growth mandated the use of shared drives to facilitate collaboration across multiple locations. But remote connectivity posed risks. Improper file sharing was creating security vulnerabilities and increasing this hospital’s attack surface.

> **“Having all of our locations remotely connected forced us to think about security concerns that didn’t exist 20 years ago.”**

As a healthcare organization with thousands of patients under their care, keeping track of sensitive data was especially important. It was their responsibility to ensure data privacy for all PII and PHI, both of which are protected under HIPAA.

But it wouldn't be easy. The healthcare organization had data spread out across a massive hybrid environment — in the cloud, in on-premises servers, archived in email folders, and even saved on employees' computers.

The organization's lacked visibility and control when it came to their patient and employee data. An attacker using stolen credentials for just one account could put critical information at risk, potentially jeopardizing their HIPAA compliance.

According to the Network Admin:

> **"Employees knew they shouldn't do things like save PHI to personal computers or create folders with Global Group Access, but not everyone was adhering to those standards."**

The organization decided to look at Varonis.

"When I started at the hospital, we had 4 servers and 50 desktops. Now, we have over 300 servers and 2,500 desktops."

SOLUTION

Data classification, auditing, and remediation under one roof

The regional healthcare network purchased the Varonis Data Security Platform. Having classification, auditing, remediation, and entitlement capabilities all in one dashboard enabled them to get in control of their data.

Varonis identifies classifies all the data — including PHI, PII, financial records, and other HIPAA-regulated data — in the organization's environment. The platform maps out permissions, and identifies and remediates overexposed information.

And best of all, all of this is done automatically. The Network Admin can see exactly where sensitive information is located and take swift action.

> **"Gaining visibility into PHI improperly stored in shared drives or users accessing data that they probably don't need is eye-opening. No other solution we tried gave us all of that information behind a single pane of glass."**

Varonis provides continuous monitoring and alerting for their data. According to the Network Admin, having a behavior-based threat detection system gives them tremendous peace of mind.

> **"We have alerts set up that warn us when a user is added to a security group, if a folder is shared incorrectly, or if a large amount of files are modified within a small time frame. Basically, Varonis warns us about anything that doesn't look like typical user activity."**

Varonis helps ensure that sensitive data stays secure and that it is properly moved, archived, quarantined, or deleted based on predetermined parameters.

> **"Varonis has helped us automatically organize data and it allows us to say definitively that we know where data lives. Cleaning up stale data used to be a very long and manual and process, but not anymore."**

Varonis also makes compliance and e-discovery a breeze by helping the Network Admin fulfill data subject access requests (DSAR). Varonis makes it easy to pinpoint files containing PII, PHI, and other HIPAA data.

RESULTS

Enhanced privacy and protection for 2,500 end users

The organization’s Network Admin sees other healthcare organizations fined millions of dollars after failing to protect user privacy and meet HIPAA compliance standards.

They’re thankful that they have Varonis keeping a watchful eye on their unstructured data environments.

> **“To be honest, I don’t know how we would meet regulatory requirements without Varonis. Native tools aren’t enough—system and application event logs don’t get into the weeds of who is doing what in your file shares the way Varonis does.”**

For an organization in the healthcare industry, having visibility and control capable of scaling with their business growth has been essential. Despite a massive increase in the data they manage, the Network Admin feels more in control over that data than ever before.

> **“If you work within a regional healthcare network, and your organization is poised for growth like we were, you need a way to prove that you have visibility and control over your unstructured data. If you don’t have a solution like Varonis, you open yourself up to a lot of risk.”**

According to the Network Admin, having Varonis in their corner, and knowing that Varonis’ team is always proactively working to improve their products, gives them confidence.

> **“Varonis performs a ‘health check’ every quarter. The constant contact—them asking how we’re doing, what we need, and how they can help—that’s huge. I really appreciate that Varonis is always willing to help and find ways to serve us better.”**

Protect sensitive data. Automate compliance.

Varonis takes the complexity out of file auditing, securing sensitive information, and maintaining retention policies.

Request a demo