VARONIS

How Varonis Helped a Large Regional Healthcare System Lock Down Over 500,000 HIPAA Hits

> Varonis has, in magnitudes of a hundred times or more, simplified how fast we can get through folder clean-up and remediation. It's hard to quantify exactly how much time it has saved us because, in a matter of months, it completed remediation tasks that would take us over three years to do manually.

About this case study:

Our client is a large regional healthcare system. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

Challenges

- Locking down regulated data, including 318,357 folders with Global Group Access
- Restricting user access to 504,162 HIPAA hits to protect patient data and meet compliance regulations
- Expediting remediation that would otherwise take 3 years to do manually

Solution

The Varonis cloud-native Data Security Platform:

- Continuously discovers and classifies critical data across cloud and hybrid environments
- Locks down permissions and prevents exposures
- Proactively detects and helps prevent threats
- Migrates data where it belongs
- Makes remediation faster, safer, and more efficient

Results

- Dramatic reduction in open access completed within months, not years
- Data security and privacy for over 1,500 end users
- Reporting capabilities that make it easy to monitor and prove HIPAA compliance

CHALLENGES

Locking down PHI information

Knowing the importance of data protection and privacy, one large regional healthcare system (anonymous by request) started working with Varonis in 2015.

In the years since, they have continued to expand their reliance on Varonis to meet their evolving needs.

According to their Security Engineer:

> **"We're a hospital organization with a lot of PHI, HIPAA, and financial data that we do not want to be released to the public. Before Varonis, we didn't have a way to ensure or measure data privacy."**

The organization suffered from "permission creep." Years of new employees coming and going and staff members changing positions had resulted in out-of-control file share permissions.

> **"Over the years, different people fell into system admin roles. Many of those people had just enough knowledge to be dangerous — they knew how to give out file server access or file share permissions, but they didn't know how to do it correctly. This led to a lot of sensitive folders with wide-open access."**

The Security Engineer was concerned. Healthcare systems have a burden to safeguard PHI and strictly adhere to HIPAA Privacy and Security Rules.

Failure to comply can have serious consequences: In 2023, the HHS OCR settled cases with eight covered entities and four business associates for potential HIPAA violations, with fines totaling more than $4 million. This organization didn't want to face similar fines or betray the trust of their patients.

A Varonis Data Risk Assessment revealed over 11 TB of overexposed data — **318,357 folders, 504,162 HIPAA hits, and 16,292 Social Security Numbers were open to everyone.**

Globally exposed data creates a massive attack surface — **a single compromised endpoint could result in a headline-making data breach.**

> **"Seeing those numbers was gut-wrenching. We knew some areas were in bad shape, but I had a few sleepless nights after I saw exactly how bad it was."**

The organization predicted it would take their small security team over three years to fix their extensive blast radius manually — an impossible goal.

"We're a hospital organization with a lot of PHI, HIPAA, and financial data that we do not want to be released to the public. Before Varonis, we didn't have a way to ensure or measure data privacy."

SOLUTION

Varonis products to find and fix folders with global group access

Over the years, the org continued to expand their use of Varonis to help them solve problems, including:

+ Monitoring and protecting their on-premises data stores and email. Varonis maps who can and who does access PHI and other sensitive data.
+ Scanning for and classifying PHI and other data in their servers. Varonis helped them isolate HIPAA concerns.
+ Automatically migrating data cross-domain or cross-platform after it has been earmarked for archival, quarantine, or deletion. Varonis ensures that data is stored properly, based on content type, age, access activity, etc.

Varonis automatically finds and fixes folders with Global Group Access, helping the healthcare organization rein in their out-of-control data and protect their users and patients.

> **"Varonis is helping us go through years' worth of data and limit access to the users who need it. It's moving all of our folders away from Global Group Access."**

Varonis performs dependency checks, gives you a preview of results before running the job, and allows you to quickly roll back if needed.

Manual remediation is time-consuming and vulnerable to human error — if it can be done at all. Broken ACLs and other mistakes often creep into shared drives as a result.

> **"Trying to remediate permissions manually left us feeling defeated from the get-go. We were spending all of our time on it, and we had no clear way to tell who had access to certain data."**
>
> **"Worse, when we started manually locking down access, sometimes applications or systems would go down as a result of our changes. That would stop us in our tracks and force us to fix the broken systems before trying again. I don't think we could have finished fixing permissions without Varonis. It would have taken years."**

Varonis provides continuous monitoring and alerting on data and systems.

> **"Varonis alerts us to anomalous activity. If I see the signs of ransomware or a crypto attack, I can use the alert dashboard to quickly understand what's going on."**

Varonis helped them stop a potential security threat that started when an administrative user opened a phishing email. The affected user's account sent out an official-looking employee survey, which contained a URL to a webpage asking for credentials.

Varonis flagged the volume of emails as suspicious, and the Varonis Incident Response team helped investigate the issue.

> **"Pre-Varonis, we would have run around, scouring our servers, and spent tons of wasted hours looking through event logs to try and get a handle on what was happening. With Varonis, we have alerts that allow us to quickly understand and resolve situations."**

The Incident Response team guided the client on how to create queries, add users to watch lists, and create a variety of different user audit logs. This helped them identify "patient zero" and confirm which accounts had been compromised.

Varonis helped them quickly reset passwords, lock down Outlook Web Access (OWA), and determine that the attack did not pivot from OWA to their on-prem network.

> **"I'm very pleased with the Varonis Incident Response team. They helped us narrow down the points of entry, lock down outside access, and quickly get things under control."**

"I don't think we could have finished fixing permissions without Varonis. It would have taken years."

RESULTS

Data protection for over 1,500 end users

The regional healthcare system used to suffer from rampant overexposure. Over half a million HIPAA hits, 318,357 folders and 16,292 Social Security Numbers were open to everyone. A data breach would have compromised the confidential information of thousands of staff and patients.

With Varonis, they've been able to dramatically reduce open access and limit permissions to critical folders. According to the Security Engineer, the value of that extra security cannot be overstated.

> **"It's priceless. Protecting our patients is my number-one priority. Knowing that their data is secure gives me tremendous peace of mind."**

They also have more clarity and control over their environments. Varonis has played a pivotal role in facilitating permission remediation and locking down personal data.

> **"Varonis has, in magnitudes of a hundred times or more, simplified how fast we can get through folder clean-up and remediation. It's hard to quantify exactly how much time it has saved us because, in a matter of months, it completed remediation tasks that would take us over three years to do manually."**

Now Varonis gives them all the insight and reporting capabilities they need to prove HIPAA compliance.

> **"When a C-level executive walks into my office, I can demonstrate within minutes that we're in better shape. I can show them 'Here's where our data lives,' and I can click on a user and say, 'Here's what they have access to.' Having that level of insight and security means the world to me."**
>
> **"I couldn't function in my role without Varonis. I think of every solution in my security stack as a tool in my tool belt. If I was forced to get rid of some tools, Varonis is the last one that would go."**

Reduce your attack surface and simplify compliance with Varonis.

Put remediation on autopilot with Varonis.

Request a demo