VARONIS

How a U.S. Community Hospital Saves Hundreds of Hours Every Week Managing Permissions with DataPrivilege

CASE STUDY

“Varonis takes the onus off of IT support staff—who shouldn’t be managing departmental permissions anyway—and gives control back to stakeholders. We can finally lock down our data with confidence.”

ABOUT THIS CASE STUDY:

Our client is a U.S. Community Hospital. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Saving time and money by decreasing the burden on IT to provision permissions
- Improving efficiency by transferring access controls to department heads
- Gaining visibility into where HIPAA, PII, and PHI lives and who has access to it

SOLUTION

DatAdvantage:

- Maps who can access and who does access data, including PII, PHI, and HIPAA-protected data
- Shows where users have too much access and where sensitive data is at risk
- Automates changes to access control lists and security groups

DataPrivilege:

- Empowers data owners to manage permissions
- Reduces the burden on IT and speeds up file access
- Automatically enforces security policies and least privilege

RESULTS

- 75% reduction in permission requests
- IT work hours and resources freed up to focus on cybersecurity

Challenges

Time and resources lost due to permission gatekeeping

Before a U.S. Community Hospital (anonymous by request) adopted Varonis, it often felt like their various departments were at war with each other. As their Chief Technology Officer explains:

> “IT was the ‘bad guy.’ We managed permissions, so we were perceived as gatekeepers who prevented other departments from accessing the information they needed.”

Even with more than a dozen IT members dedicated to provisioning permissions, the task was time-consuming and tedious. **Their team was spending an estimated *400+ hours every week* resolving access requests.**

The process was frustrating for all parties. IT spent all of their time chasing people down and asking questions, because they weren’t in a position to know which employees needed access to specific files, folders, and groups. Meanwhile, the lack of expedient access bogged down efficiency and productivity for other departments.

Worse—the organization was starting to make mistakes when it came to data handling. The CTO was concerned. They lacked a clear way to identify where sensitive data (HIPAA, PII, PHI) lived in their servers or trace who had accessed it.

> “There were a lot of questions being asked about the data integrity for HIPAA, PII, and PHI—and we couldn’t answer them. We needed a way to protect that information and see where it was going.”

In a worst-case scenario—a data breach—they wouldn’t be able to identify which data had been stolen or the parties responsible.

> “Hackers exploit exposed personal information. If we don’t lock down that data, it opens us up to a lot of risk—especially within the healthcare network.”

> “We managed permissions, so we were perceived as gatekeepers who prevented other departments from accessing the information they needed.”

Solution

Giving permissions control back to department heads

Varonis DataPrivilege eliminates the bottlenecking that occurs when every access request needs to go through IT. By empowering data owners to view and manage team permissions, Varonis has helped the hospital streamline data access governance (DAG) for all files, folders, and security groups.

> “We used to have a dozen people focused on nothing but permission management. Now, stakeholders have direct control over their data. Each department has its own drive with separate share permissions and security controls,” explains the CTO.

The intuitive self-service portal makes it easy for department heads to change permissions, monitor data usage, and enforce “least privilege” without enlisting IT’s help—so only the people who need to view sensitive data are able to access it.

According to the CTO, this has freed up the IT team to focus on mission-critical tasks like locking down sensitive data.

> “There’s so much information within a hospital. If it all has to flow through IT, you’re wasting time and resources. Varonis frees me up to utilize my team more fully and help it grow,” explains the CTO.

DatAdvantage for Windows helps the hospital enforce least privilege by mapping active permissions and providing a clear audit trail that tracks when users access data and which data they touched.

This visibility is crucial in ensuring that data stays secure, even though it's now being managed by individual departments. Before Varonis, the CTO says, this level of control was impossible.

> "We can run reports on all of our drives and SharePoint to locate HIPAA, PHI, and PII in our server and identify who has access to it. Without Varonis, we wouldn't have the ability or the resources to drill down into that info and examine the details."

DatAdvantage also warns IT whenever it detects users with too much access. This enabled the CTO and the IT team to quickly lock down exposed data by finding and remediating a number of files and folders that were open to everyone in the company.

> "It's very important—especially for hospitals—to lock down sensitive information. If hackers manage to spill sensitive patient information, it would be disastrous."

> "We used to have a dozen people focused on nothing but permission management. Now, stakeholders have direct control over their data. Each department has its own drive with separate share permissions and security controls."

Results

Permissions requests reduced by over 75%

As soon as the hospital gave each department control over their own permissions, **access requests fell by a stunning 75%**. This frees up valuable time and resources for the IT department.

Where managing permissions used to be a full-time job for more than a dozen IT members, now it only takes **one person** to monitor DataPrivilege—and it's no longer a full time job.

The end result? Hundreds of work hours saved every week and increased efficiency across the board.

> “Varonis takes the onus off of IT support staff—who shouldn't be managing departmental permissions anyway—and gives control back to stakeholders. We can finally lock down our data with confidence.”

When it comes to data security, the CTO says that Varonis gives senior leaders a “30,000-foot view” that helps them consider all of their sensitive data as a whole and assess current risk levels.

This heightened visibility has helped his team take proactive steps to defend HIPAA, PII, and PHI against data breaches.

> “Varonis has helped us go from passive and reactionary to proactively protecting our sensitive data. We finally have the confidence and capability to secure our data stores.”

This hospital endeavors to always be on the cutting-edge of cybersecurity, and they're glad to have found a partner like Varonis that continues to innovate, evolve, and support them.

> "There isn't another product out there that does what Varonis does—or even comes close to it; and the customer support is amazing. Varonis checks every box."

> "Varonis helped us go from passive and reactionary to proactively protecting our sensitive data. We finally have the confidence and capability to secure our data stores."

VARONIS

Put access controls back into the hands of data owners without sacrificing cybersecurity.

DataPrivilege frees up your IT team to focus on what matters—defending your business against data breaches

REQUEST A DEMO