How a West Coast Public Healthcare Organization Protects PII, PHI, PCI and Other Regulated Data

CASE STUDY

"Varonis always hits it out of the park. It does what it's supposed to: helps us find PHI and fulfill contract obligations from the state. Without it, we wouldn't be able to fulfill HIPAA regulations."

ABOUT THIS CASE STUDY:

Our client is an American public healthcare organization. We have happily accommodated their request for anonymity.

HIGHLIGHTS

CHALLENGES

- Discovering PII, PHI, and PCI hidden throughout their network
- Reporting on user activity and permissions on sensitive data for HIPAA compliance
- Reducing their blast radius and defending against ransomware

SOLUTION

Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **DatAlert** monitors and alerts on abnormal behavior on critical systems

RESULTS

- Sensitive data locked down and moved to encrypted servers
- Compliance reports and PRA requests fulfilled in seconds
- Risk mitigation thanks to automated alerts on file activity

Challenges

Achieving HIPAA compliance

In 2014, a West Coast Public Healthcare Organization (anonymous by request) was facing the same challenges that every healthcare organization will eventually need to contend with:

- Discovering what sensitive data they have and where it lives.
- Reporting on who has access to sensitive data and who's accessing it on a regular basis.
- Protecting sensitive data against threats like ransomware.

Sensitive data includes Personal Identifiable Information (PII), Protected Health Information (PHI) regulated under HIPAA and U.S. law, and Payment Card Information (PCI). It also includes critical company data, like financial data and internal-only files.

Gaining visibility into user activity surrounding PII, PHI, and PCI is essential for achieving HIPAA compliance. But before Varonis, the company had no way of pinpointing where this data lived in their environment. As a Security Admin explains:

> "Before Varonis, we tried to regulate PHI through policies, but we didn't have a tool that told us where PHI was stored on our network. With Varonis, we know exactly where all of our regulated data is."

A lack of visibility made proving regulatory compliance magnitudes harder. For example, if a patient submitted a Public Records Act (PRA) request, the organization had to manually collect every record they held for that patient. It might take days—or even weeks.

> "We basically had to do a search for file extensions and open up every single document and read it to see if it contained PHI. It was ridiculous and very time consuming."

"Before Varonis, we didn't have a tool that told us where PHI was stored on our network. With Varonis, we know exactly where all of our regulated data is."

Solution

The means to find sensitive data and manage risk

To get a handle on their data, the organization purchased:

- **DatAdvantage for Windows and SharePoint.** By highlighting permissions, DatAdvantage enables the Security Admin to discover when users have excessive access.
- **Data Classification Engine** analyzes enterprise data to identify sensitive data, including PII, PHI, and PCI.

> "Varonis scans all of our servers, all the file shares, and looks into documents for key medical phrases and terms. If it detects PHI, it tags it with the HIPAA classification."

With DatAdvantage and Data Classification Engine, the Security Admin has complete visibility into where the company's sensitive data lives and who has access to it.

If they need more context, they can right-click the file and see what keyword was considered sensitive. When they need to lock down data, DatAdvantage enables them to safely remediate permissions.

> "Varonis shows me where our PHI is located and I can drill in to see what type of PHI it is. When we get audited, we can generate reports to prove that we know exactly where our sensitive data is."

The organization used these two solutions for years to identify sensitive data, move it to encrypted servers, and enforce least privilege. But a lot has changed since 2014—including the risk of ransomware and the consequences of a data breach.

So in 2017, the organization added support for Active Directory with **DatAdvantage for Directory Services**. Then, in 2020, they adopted **DatAlert**.

> "DatAlert gives us alerts on changes on the network that could be malicious, like a bunch of files being deleted or encrypted. When it detects suspicious activity, it enables us to immediately launch an investigation. Every alert has a description of the problem and how to fix it."

DatAlert helps mitigate the risk of ransomware by monitoring file activity for unusual user behavior and permission changes. Having high-fidelity alerting and automated response to threats helps the Security Admin rest easy.

"Before Varonis, we used to spend a lot of time fighting fires. After Varonis, we have a solution that finds problems and tells us exactly how to fix them."

Results

Enterprise data blind spots eliminated

After partnering with Varonis for nearly a decade, the Security Admin is confident that their organization is top of the class when it comes to data security and HIPAA compliance.

> “Honestly, I don’t know how other agencies achieve compliance without a solution like Varonis. I think we’re doing a lot better than a lot of other organizations in the space and Varonis supports that.”

Varonis helped the organization achieve all of their goals:

1. They know exactly where PII, PHI, and PCI lives and who has access to it.
2. They can generate compliance reports and fulfill PRAs in seconds.
3. Alerts help them detect and defeat threats like ransomware.

Using the knowledge of their most at-risk areas, the Security Admin has been able to take steps to reduce risk company-wide, decrease the organization’s blast radius, and defend against ransomware.

> “Varonis always hits it out of the park. It does what it’s supposed to do: helps us find PHI and fulfill contract obligations from the state. Without it, we wouldn’t be able to fulfill HIPAA regulations.”

When something changes on their network, Varonis enables the Security Admin to understand and investigate the changes. If a Varonis alert ever indicates an attack, Varonis' Incident Response team is standing by to help the organization defend its data.

> "Out of all the products that I've used in my 30-year IT career, Varonis has been one of the most reliable."

DatAdvantage, Data Classification Engine, and DatAlert have provided tremendous value to this organization—so much value that they're now considering adding two more Varonis products to their security stack: **Automation Engine** and **Data Privilege**.

> "Before Varonis, we used to spend a lot of time fighting fires. After Varonis, we have a solution that finds problems and tells us exactly how to fix them. If I ran the same reports manually, it would take me hours or days. Varonis does all the labor in seconds."

"Out of all the products that I've used in my 30-year IT career, Varonis has been one of the most reliable."

See where you're at risk. Gain the insight you need to fix it.

Varonis helps you defend your sensitive data.

REQUEST A DEMO