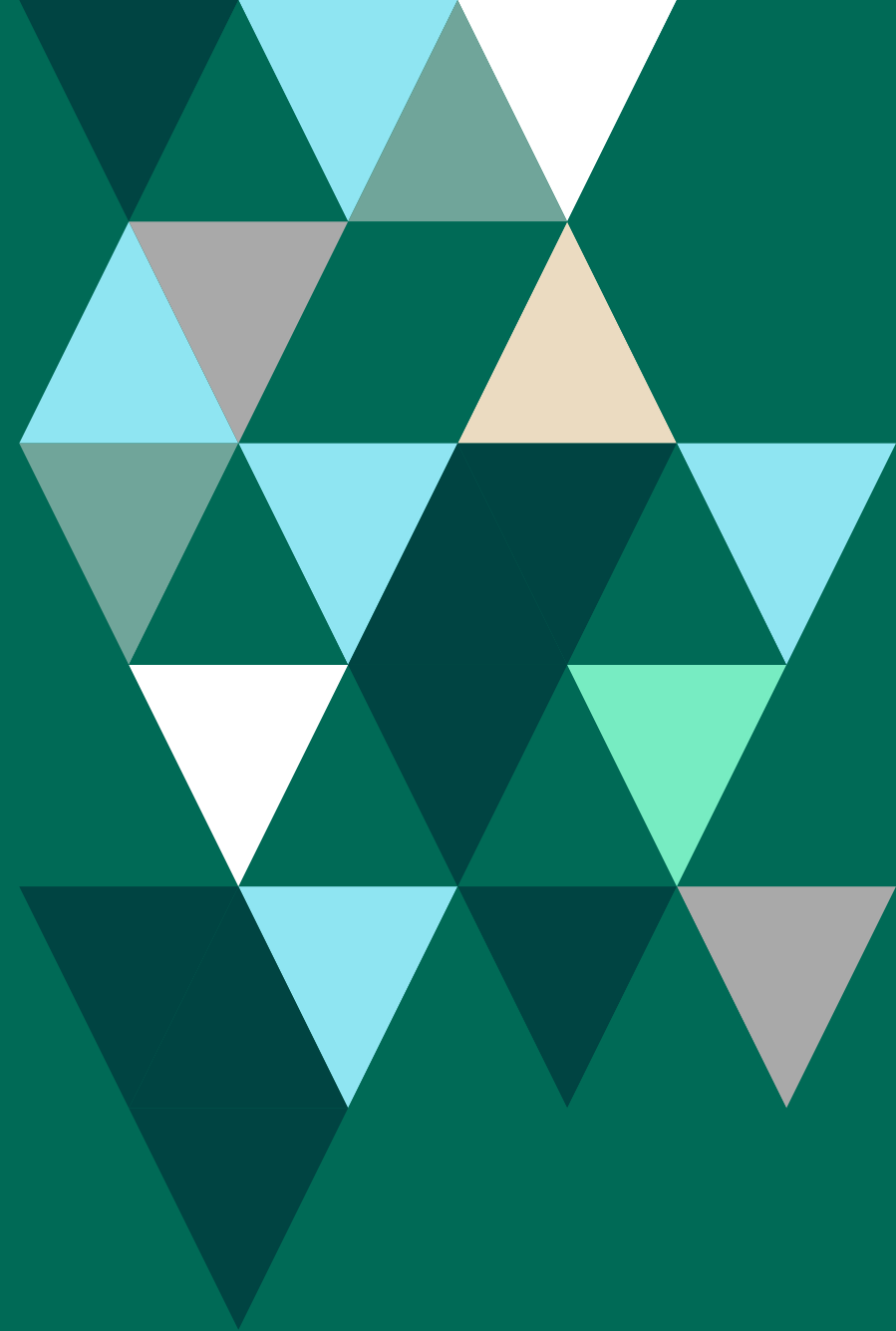


FORTRΔ

**Definitive Guide
To Protecting
Sensitive
Healthcare Data**





Your Data Is Leaking And It's At Risk

We live in an increasingly digitally collaborative world, a trend which has been accelerated in no small part by the COVID-19 pandemic. While all of this collaboration—both internally among employees and externally with outpatient clinics, suppliers, and patients—has enabled healthcare organizations to maintain higher levels of productivity, it has also increased the risk of sensitive data exposure and loss.

Removing sensitive, electronic information from an enterprise used to be difficult. The mainframe environment consisted of a single access point, one network, and a locked down ecosystem with a few logins. Keeping data secure and preventing unwanted viewers wasn't all that hard. In today's environment, however, the rate at which your clinicians, administrative staff, and other employees are sharing confidential data outpaces your IT team's ability to patch the perimeter, block or quarantine information, and stop confidential data from leaving your control.

With thousands of vectors for your patient data (PHI, EMRs, and PII – personally identifiable information), confidential research, and financial reports to leave your business—email, Dropbox/Box shared links, managed and unmanaged mobile devices, Slack, or even the traditional USB drive—you need a different security strategy to operate in an ever-porous enterprise environment.





We'll Cut To The Chase.

Data is a crucial and pervasive asset of any healthcare organization, but to safeguard your most valuable information—as well as that of your patients—there needs to be a shift in the data security strategy to protect what really matters: the data itself.





Your Sensitive Data Is At Risk Throughout The Organization

PATIENT RECORDS/DATA	RESEARCH
 <ul style="list-style-type: none">• ePHI• EHRs• PII• Third-party Lab Results• Imaging Results• Data from Connected Medical Devices	 <ul style="list-style-type: none">• Clinical Trials• Surveys & Research Findings• Unpublished Medical Papers
FINANCE	LEGAL
 <ul style="list-style-type: none">• Payer Filings & Records• Financial Reports• Compensation Plans	 <ul style="list-style-type: none">• Payer Agreements• Malpractice Filings & Settlements• HIPAA & GDPR Audits

A primary care physician sending health records to consult with an external specialist, billing departments sending diagnoses and plans of care to payer organizations, and labs sending test results to doctors and their patients. With so much sensitive data regularly being shared, both internally and externally, healthcare organizations are extremely attractive targets for today's cyber criminals. Hackers especially like to acquire medical records because they usually contain a complete, evergreen identity: name, date of birth, social security number, and medical information. The result: organizations in the healthcare industry suffered **2-3x more cyberattacks** in 2019 than the average amount for other industries.¹



Standard Tools Can't Be Your Only Line Of Defense Anymore

The most common question we hear is:

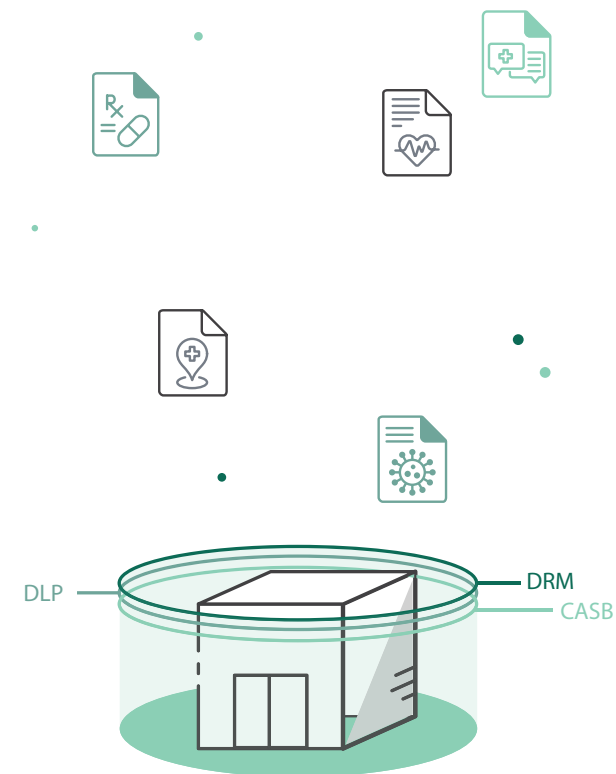
“DON'T I ALREADY HAVE A DATA SECURITY STRATEGY?”

Yes, and no. Data Loss Prevention, Cloud Access Security Brokers, Digital Rights Management and Classification tools offer their own valuable benefits, but they all share the same limitation: they're all about locking data down instead of protecting it when it's on the move.

A recent Ponemon Study found that **54% of healthcare associates** say their biggest problem is employee negligence in the handling of patient information.² Shared passwords, inadequate data security practices, and the mishandling of sensitive data are routinely exposing healthcare organizations and the sensitive data they are responsible for to hackers. And those errors can be costly! As stated in IBM's 2020 Cost of a Data Breach Report, the average total cost of a data breach was **\$3.86 million in 2019**.³ However, healthcare data breaches come with an even heftier price tag—cutting deep with an average cost of **\$7.13 million**. Cybersecurity experts maintain that a majority of data breaches can be avoided and millions of dollars saved if organizations simply focused more on controlling the flow and access of their sensitive internal data assets.

Additionally, in response to the COVID-19 pandemic, telehealth/telemedicine is on the rise, a practice that is introducing a new set of data security challenges for today's providers. More sensitive data is being shared via email and through cloud-based applications than ever before. Making sure it's secure, wherever it ends up, is critical to maintaining patient privacy and not running afoul of applicable regulations (e.g., HIPAA and GDPR).

In a nutshell, only having the standard cybersecurity tools in place will no longer suffice as a defensive security approach. Once confidential patient data, medical research, or payment/financial information is shared by an employee or otherwise leaves your network, your security strategy comes to an end. As your sensitive data travels to unknown endpoints, unknown companies, and unknown domains, all bets are off. You can't see it. You can't control it.





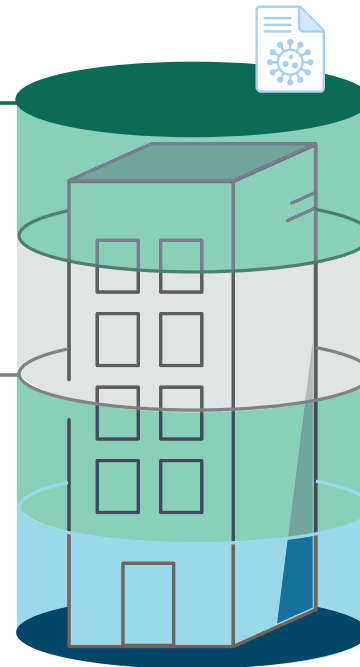
AN INCREASED FOCUS ON DATA SECURITY IS NOW A NECESSITY

Data Loss Prevention, Cloud Access Security Brokers, Digital Rights Management, and Classification rarely work at the most critical moment—when people are working with the information. Unfortunately, these tools can't prevent a payer or outpatient provider you're working with from saving and forwarding a copy of a patient's records to an unauthorized recipient. They're unable to secure information "in use" and track who it's going to. And once your sensitive data moves past the DLP fence and CASB proxy, it's in the wild and completely unprotected.



DIGITAL RIGHTS MANAGEMENT (DRM):
An attempt at data-centric security but a cumbersome user experience prevents enterprise-wide adoption and scalability.

DATA LOSS PREVENTION (DLP)
Scans and quarantines confidential information traversing the network but once it leaves, security teams can't see, audit or control what others are doing with mission-critical data.



CLOUD ACCESS SECURITY BROKER (CASB)
Enforces security policies and blocks information leaving cloud applications (e.g., Box, Salesforce) but once data is downloaded or moved offline, security teams lose all control of what happens.

CLASSIFICATION:
Tags and classifies sensitive information shared from your business but classifier won't be able to prevent an internal employee from downloading trade secrets and taking them to his/her next job.

You Need A New Strategy, A Data-Centric Approach, To Effectively Secure Your Sensitive Data, Everywhere It Goes.



Data-Centric Security: Protection For The Porous Organization

A truly effective data-centric security approach is one that can secure data through its **entire lifecycle**, everywhere it travels, no matter who has it or where it's stored. The goal is to protect confidential data at the point of its greatest vulnerability, when it's being used in other person's hands, and as it travels outside your perimeters into unmanaged domains, devices, and applications.

The ideal data-centric security solution is characterized by five capabilities with five key benefits.

Key capabilities of a data-centric security solution



Secures All Forms Of Data



360-Degree Visibility



Dynamic Data Protection



Integrates With Your Ecosystem



Invisible User Experience



Healthcare Organizations Need An Effective Treatment Plan For Data- Centric Security Success

HOW DOES THIS WORK IN THE HEALTHCARE INDUSTRY?

IT security teams at healthcare organizations struggle to balance between two competing demands: securing sensitive patient data while delivering quality care and meeting strict regulatory requirements (e.g., HIPAA). Without the right tools and strategy in place to help your IT staff overcome this obstacle, how can you ensure that your sensitive data is safe?

Another significant area of concern for healthcare organizations is the deployment of so many new systems heavily based in the cloud. While the cloud enables a variety of attractive options for using, sharing, and storing data, it also exposes new security vulnerabilities and avenues of attack. Not only are these attack surfaces emerging at a record pace, the amount of data in motion is exploding. As a result, the healthcare industry now needs to protect much more patient, provider, and payer data, often dispersed far beyond enterprise walls and accessible via an ever-widening array of end points. But how?

Deploying a data-centric security approach solves the balancing act: providing robust protection for sensitive data while still enabling it to be used wherever and however it's needed. Such an approach provides answers to the toughest questions keeping your team up at night.



How do I control how suppliers, distributors, and other partners consume or share our sensitive data?



How do I prevent leaks to unauthorized partners or competitors once an employee or third-party users have access to our sensitive files?



How do I track the flow of our sensitive documents throughout their lifecycle?



How do I confidently revoke access to proprietary information after employment or a partnership has ended?



Vera's solution to helping you implement data-centric security

At Vera, we've helped many technology companies bullet proof their data security by implementing the STAR solution as in below:

SECURE

Apply AES 256-bit encryption and granular access policies that travel with your data files regardless of how and where they're shared.

TRACK

Understand exactly who is accessing sensitive data inside and outside of your organization, to maintain visibility/control and thereby minimize the potential for leaks of pre-release content and other IP.

AUDIT

Withdraw access to sensitive files any time after they've been shared, regardless of where and with whom the files now reside.

REVOKE

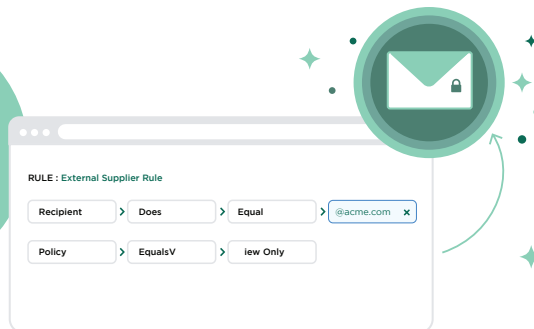
Secure Sensitive Data You Need To Distribute

Securing your data is the first step in the **STAR** approach, providing the confidentiality, control, and oversight you didn't have previously. With a single mouse click, you can protect documents, spreadsheets, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the associated files regardless of the methods by which they are shared.

Automatically Secure Sensitive Data Emailed Outside Your Organization

One of the most common workflows our healthcare customers leverage is automatically securing all sensitive files sent over email, for example, to/from an external lab/diagnostician, payor, or provider partner. Leveraging Vera's smart rules engine, all attachments sent to a specific company (example: @provider.com) are automatically secured without requiring your busy employees to take any manual steps. If the data is ever forwarded to a party that doesn't belong to the @provider.com domain, they won't be able to access it until they're specifically granted permission.

With VERA, your team's security policy sticks to the data, anywhere it goes.





Prevent Leaks, Even After Sensitive Data is Downloaded From File Sharing Systems

Many healthcare organizations, in an effort to embrace digital transformation, now leverage local file shares and cloud-based applications (e.g., Box, Dropbox, SharePoint, and OneDrive) to facilitate collaboration between clinicians, specialists, and medical research teams.

Vera has built out-of-the-box integrations to all of these systems to automatically secure any file uploaded or downloaded from them. That way, everyone involved can work exactly the way they normally would, while Vera works seamlessly behind the scenes to protect your sensitive data everywhere it moves.

If data ever leaks or is downloaded from your storage solution, Vera's security sticks to the file anywhere it goes, making sure only authorized parties are working with your information. Vera is the best type of companion—one that keeps data safe wherever it goes.



Secure ePHI Generated From Connected Devices and Home-Grown Apps

IT/Security teams in the healthcare industry can leverage the Vera SDK/API to extend robust data security to connected medical devices, telehealth portals, and other custom apps/systems where sensitive data is generated, shared, or stored. The result is fully automated data protection and a powerful data security fabric for your entire ecosystem and extended organization.



Track And Audit Sensitive Data You Have Distributed

Tracking and auditing your sensitive data to understand who's accessing it is the next step in the **STAR** approach. Knowing whose hands are on your sensitive data is always a luxury a healthcare organization wishes they had after the fact, but with Vera you can track the complete lifecycle of any file that's no longer inside your own company walls.

Follow the Path of All Your Sensitive Data

Healthcare organizations leverage Vera's tracking and auditing capabilities to understand exactly who is accessing sensitive company files inside and outside of the organization, track all access attempts (authorized or not), and receive granular metrics on usage and adoption, as well as to create required audit and compliance reports (for HIPAA/HITECH and other regulatory bodies as needed).

Vera's easy-to-use web-based portal allows you to easily track and audit file access, duration, location, actions taken, device type used, export types and counts, and general system events (both admin and connector activities).

Revoke Access To Sensitive Data You Have Distributed

Revoking access to sensitive files you've shared is the last step in the STAR approach. This level of control comes in handy for a variety of reasons, such as after a disgruntled employee leaves the organization, severing a partnership (e.g., with an outpatient clinic, payor, or other covered entity), or simply because you want to restrict file access after a certain amount of time.

Remove Access to Files to Maintain Your Data Security Integrity

Relationships come and go in any healthcare organization and sometimes people are tempted to take sensitive files with them—or simply forget that the files are still in their possession. That's not an option/concern with Vera integrated within your IT environment. Healthcare companies leverage Vera's dynamic data protection to revoke access to data a user or provider partner has accumulated throughout the course of their time engaging with your organization—even if it's been moved to a personal account. With one mouse click, all copies of electronic health records, medical research, and payment/financial reports are shut off, providing your organization with complete control over the data that matters most to it.

Vera data-centric security solution

PATIENT RECORDS/DATA

- ✓ ePHI
- ✓ EHRs
- ✓ PII
- ✓ Third-party Lab Results
- ✓ Imaging Results
- ✓ Data from Connected Medical
- ✓ Devices

RESEARCH

- ✓ Clinical Trials
- ✓ Surveys & Research Findings
- ✓ Unpublished Medical Papers

FINANCE

- ✓ Payer Filings & Records
- ✓ Financial Reports
- ✓ Compensation Plans

LEGAL

- ✓ Payer Agreements
- ✓ Malpractice Filings & Settlements
- ✓ HIPAA & GDPR Audits

... and many more!



Secure, track, audit, and revoke any file, on any device. With Vera, a single click, protects documents, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the file. And a simple, consistent interface on every platform promotes secure behavior and dissuades your employees, vendors, and customers from choosing risky, insecure workarounds when handling your data.

Ready To Bulletproof Your Data Security?

We'd love to help. Visit us at vera.com/data-security-healthcare

[Learn more](#)

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

