# Data Security in Healthcare Needs a Checkup

A visual guide to the data security challenges and essential solution requirements for today's healthcare organizations.

## SENSITIVE HEALTHCARE DATA IS ON THE MOVE

### 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- Unpublished Medical Papers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

Widespread collaboration—both **internally** among clinicians and administrators and **externally** with patients, payors, and outpatient facilities—is essential to delivering top-notch care in a timely manner.

## The 3 C's Driving Data Sharing Today

New **collaboration technologies** emerge daily – many of which are outside IT's control.

Rapid adoption of **cloud services** results in more data beyond the corporate perimeter.

The work-from-home trend—accelerated by **COVID-19 pandemic**—pushes data sharing to unprecedented levels.

## GREATER SHARING = GREATER EXPOSURE = GREATER RISK

**$3.9 million**

average cost of a data breach in 2019.[1]

**$7.13 million**

average cost of a healthcare data breach in 2019.[1]

**54%**

of healthcare IT staff say employee negligence when handling patient data is a big problem.[2]

**34%**

of healthcare data breaches come from unauthorized access or disclosure.[3]

**25%**

of healthcare organizations using cloud-based solutions do not encrypt their files during data transfer to the cloud.[4]

**85%**

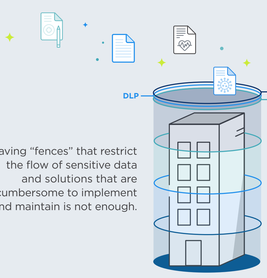
of all business assets are in digital form, which is why data-centric security is critical.[5]

**100%**

of web and cloud-based applications that store critical health information are vulnerable to cyberattacks.[6]

## WHY TRADITIONAL DATA PROTECTION SOLUTIONS FALL SHORT

Having "fences" that restrict the flow of sensitive data and solutions that are cumbersome to implement and maintain is not enough.




Visibility, control, and protection also need to extend **"beyond the fence"** to account for the myriad business-driven use cases that require sensitive data to be shared, both internally and externally.

## WHAT MAKES VERA DIFFERENT

**Complete data protection** that extends beyond the perimeter of your organization and the time of initial sharing/distribution.

**Ease of use** that includes the option of viewing and editing via a VERA HTML wrapper, or inline for native applications with the VERA client.

**Comprehensive coverage** with no limitations on devices, file types, data stores, collaboration tools, or applications.

**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 AUDIT** Understand exactly who is accessing sensitive data inside and outside of your organization, to maintain visibility/control and achieve compliance with applicable regulations (such as HIPAA/HITECH).

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

## READY TO BULLET PROOF YOUR DATA SECURITY? CONTACT VERA TODAY!

Learn more | Request demo

Call Us: 844-GET-VERA

**Sources:**

1. 2020 Cost of a Data Breach Report, IBM, 2020.
2. Ponemon Institute Research Report, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, 2019.
3. Main Causes of Security Breaches in the Healthcare Industry, RSI Security, 2019.
4. HyTrust Cloud Survey, HyTrust, 2017.
5. 2019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics, Cisco & Cybersecurity Venture, 2019.
6. 2018 Horizon Report: The State of Cybersecurity in Healthcare, Fortified Health Security, 2018.