

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- Unpublished Medical Papers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.

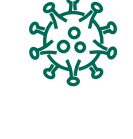
The 3 C's Driving Data Sharing Today



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

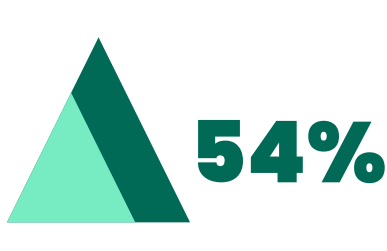
\$3.9 million

average cost of a data breach in 2019.

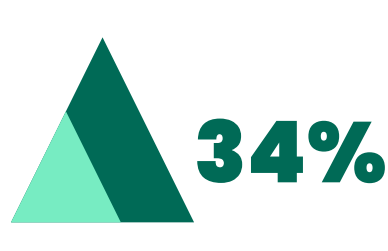


\$7.13 million

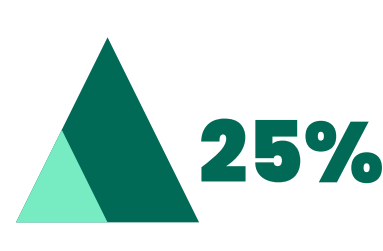
average cost of a healthcare data breach in 2019.¹



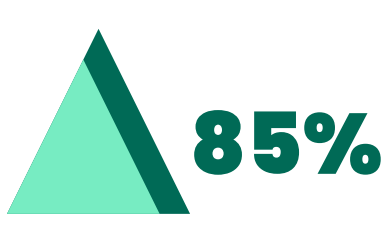
of healthcare IT staff say employee negligence when handling patient data is a big problem.²



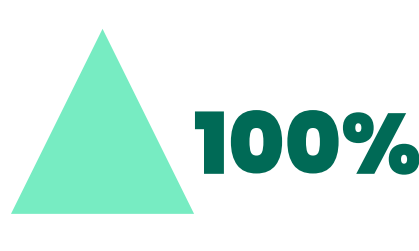
of healthcare data breaches come from unauthorized access or disclosure.³



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

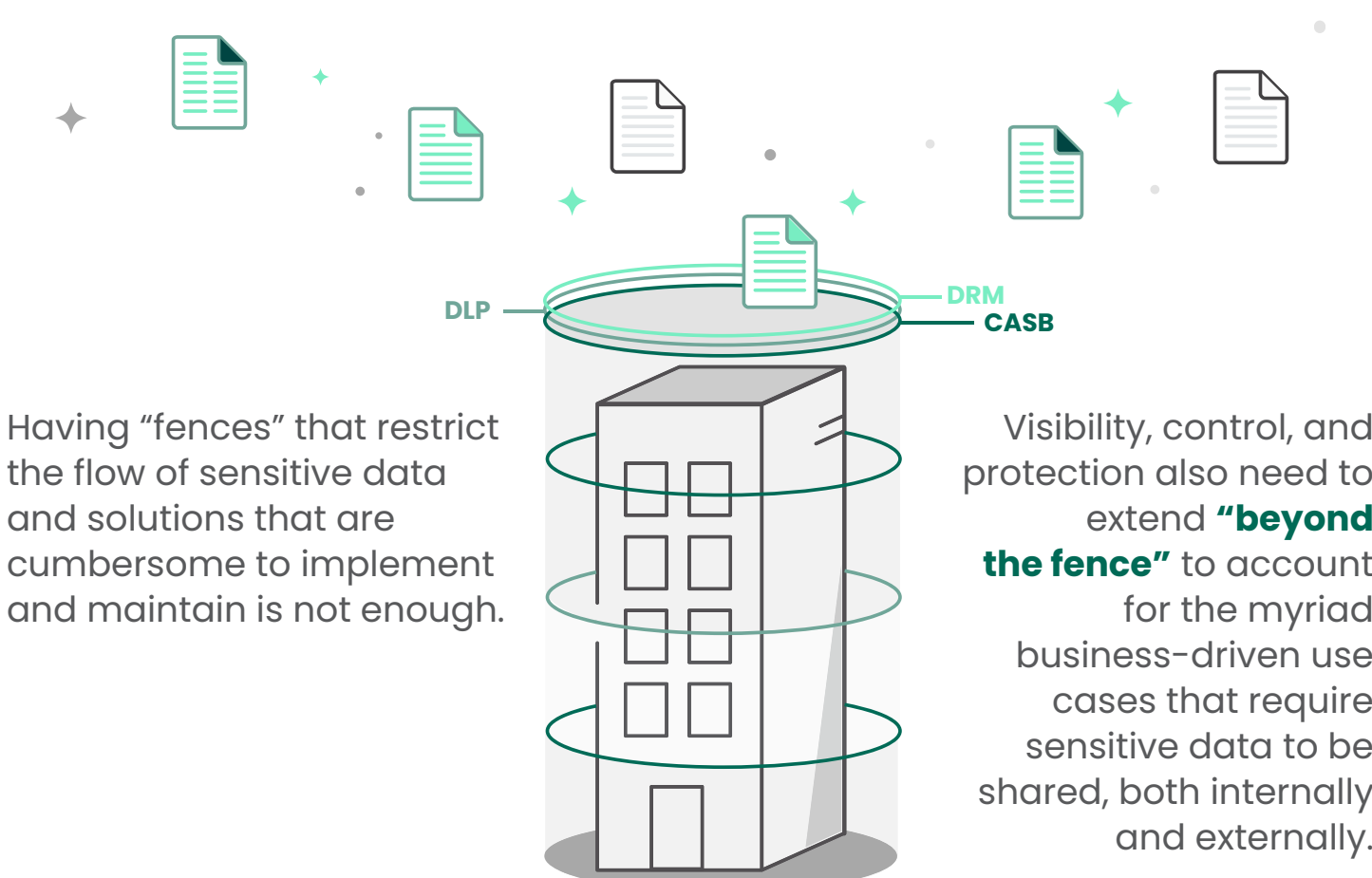


of all business assets are in digital form, which is why data-centric security is critical.⁵

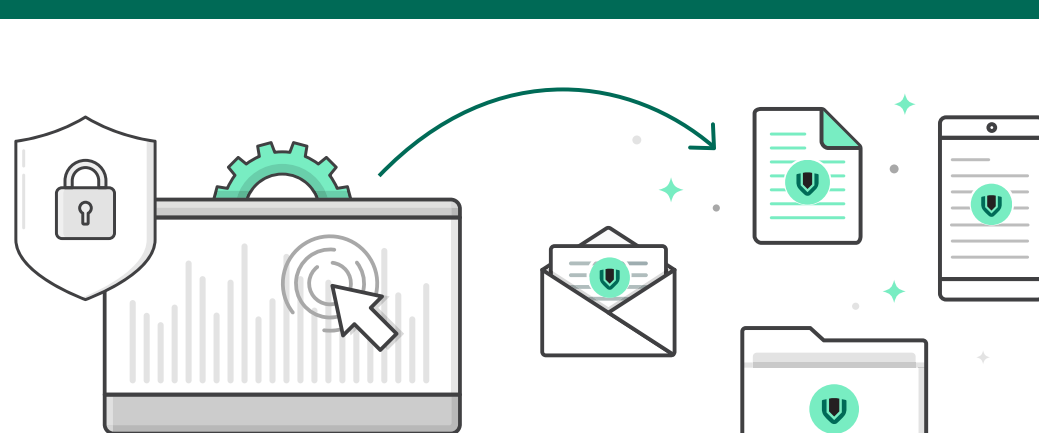


of web and cloud-based applications that store critical health information are vulnerable to cyberattacks.⁶

Why Traditional Data Protection Solutions Fall Short



What Makes Vera Different



Complete data protection

that extends beyond the perimeter of your firm 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

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

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.

REVOKE

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

Ready To Bullet Proof Your Data Security? Contact Vera Today!

LEARN MORE

REQUEST DEMO

emails@fortra.com

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.