Data Security in Healthcare Needs a Checkup

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

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.

Patient Records/Data
Sensitive Healthcare Data Is On The Move

The 3 C's Driving Data Sharing Today

Research
• Clinical Trials
• Surveys & Research Findings
• Unpublished Medical Papers

Legal
• Payer Agreements
• Malpractice Filings & Settlements
• HIPAA & GDPR Audits

Finance
• Payer Filings & Records
• Financial Reports
• Compensation Plans

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

Why Traditional Data Protection Solutions Fall Short

What Makes Vera Different

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

34% of web and cloud-based applications that store critical health information are vulnerable to cyberattacks.

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

54% of healthcare data is still sent via email, a practice that is considered unsecure and risky.

6 of healthcare breaches come from unauthorized access or disclosure.

75% of business websites are in digital form, a practice that is considered unsecure and risky.

85% of all healthcare breaches come from unauthorized access or disclosure.

90% of all healthcare breaches come from unauthorized access or disclosure.

Why Traditional Data Protection Solutions Fail Short

What Makes Vera Different

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

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.

Withdraw access to sensitive files any time after they’ve been shared, regardless of who still controls the data once it is shared.

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

LEARN MORE
REQUEST DEMO

Sources:

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners. (fta-vr-in-1222-r1-79d)