HIPAA DATA SECURITY

ASSESSMENT

Data at Rest. Data in Motion. Data Protected.

The scope of electronic protected health Information protected by HIPAA is increasing each day. Names, email addresses, biometrics, medical record numbers, URLs, and more are all classified as HIPAA relevant data. Staying compliant, and protecting your patients and staff, requires on-going vigilance and evaluation.

Meeting HIPAA data protection principles requires FIVE KEY STEPS:

1

RISK ASSESSMENT EXECUTION

Provides an understanding of where sensitive data is, how it flows, how it is used and shared.

2

DATA CLASSIFICATION AUTOMATION

Allows you to focus on resources and controls.

3

SECURE WITH DATA PROTECTION CONTROLS

Leverage DLP, Identity and Access Management and Encryption.

4

UPDATE INCIDENT RESPONSE PLAN

Shows exfiltration of sensitive data.

5

COMPLIANCE

Demonstrate compliance through reporting.

DIGITALGUARDIAN®

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

ASSESSMENT

HIPAA Data Risk Assessment

Digital Guardian and DynTek have teamed up to offer a HIPAA Data Risk Assessment to help you evaluate potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information—as defined by HHS and NIST. Regardless of the maturity of your HIPAA compliance strategy and initiatives, this unbiased assessment is a critical step in an agile compliance program. Digital Guardian and DynTek's software-guided assessment will identify:

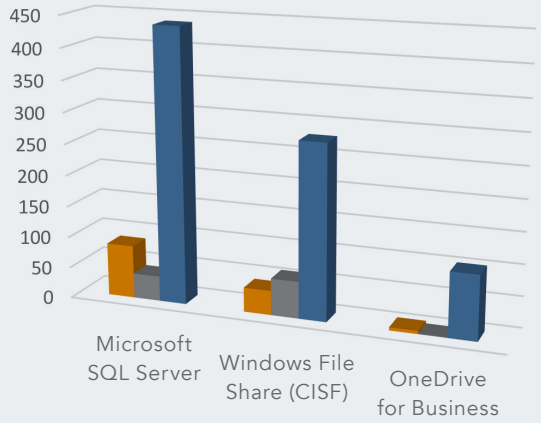
- Is PHI data your only sensitive data in the organization?
- How is it used or shared?
- Where does your 'data at rest' reside within the organization across network shares, databases or cloud storage?
- How does your 'data in motion' flow through and out of the organization?
- How are you monitoring it now?
- How do you educate on data usage and handle incidents?

The risk assessment will assess how exposed HIPAA data is in the enterprise and analyze risk based on severity. After the assessment, our team of security specialists analyze the collected information to deliver a comprehensive report that provides recommendations for remediating the identified risks. We leave you with a plan of action you can present to the organization to justify budget, showcase the effectiveness of your program or create new policies and strategy.

Sample of Data at Rest Analysis

Total Incidents By Repository

The total incidents by repository type shows the level of data exposure on file shares, databases and cloud repositories across the assessment. For this particular customer, it is clear that within the database environment investigated there is a high level of data exposure.



GET YOUR FREE ASSESSMENT NOW

Digital Guardian and DynTek are offering this HIPAA Risk Assessment to qualifying organizations at no charge for a limited time. Contact DynTek at marketing@dyntek.com or 877-297-3723 to learn more.

DYNTEK

DIGITALGUARDIAN®