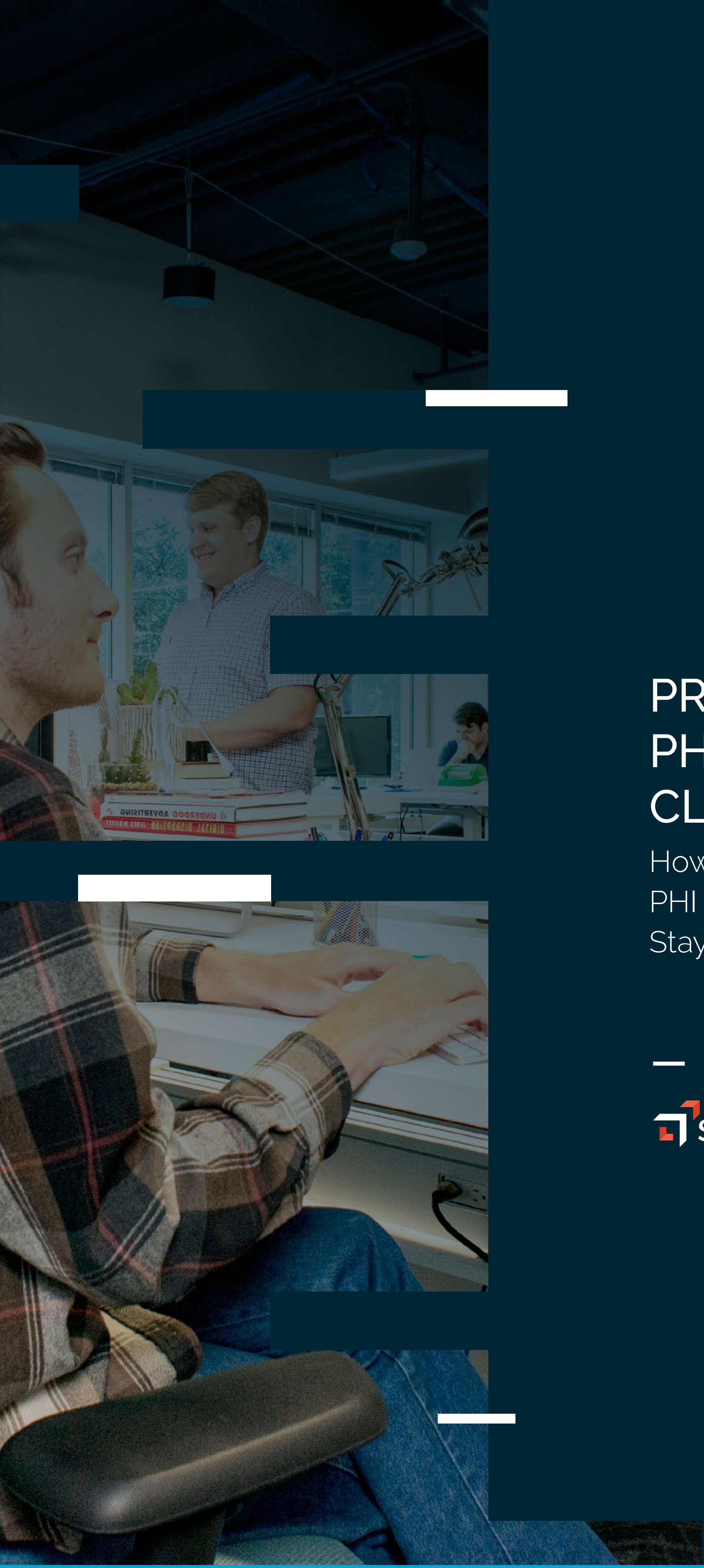
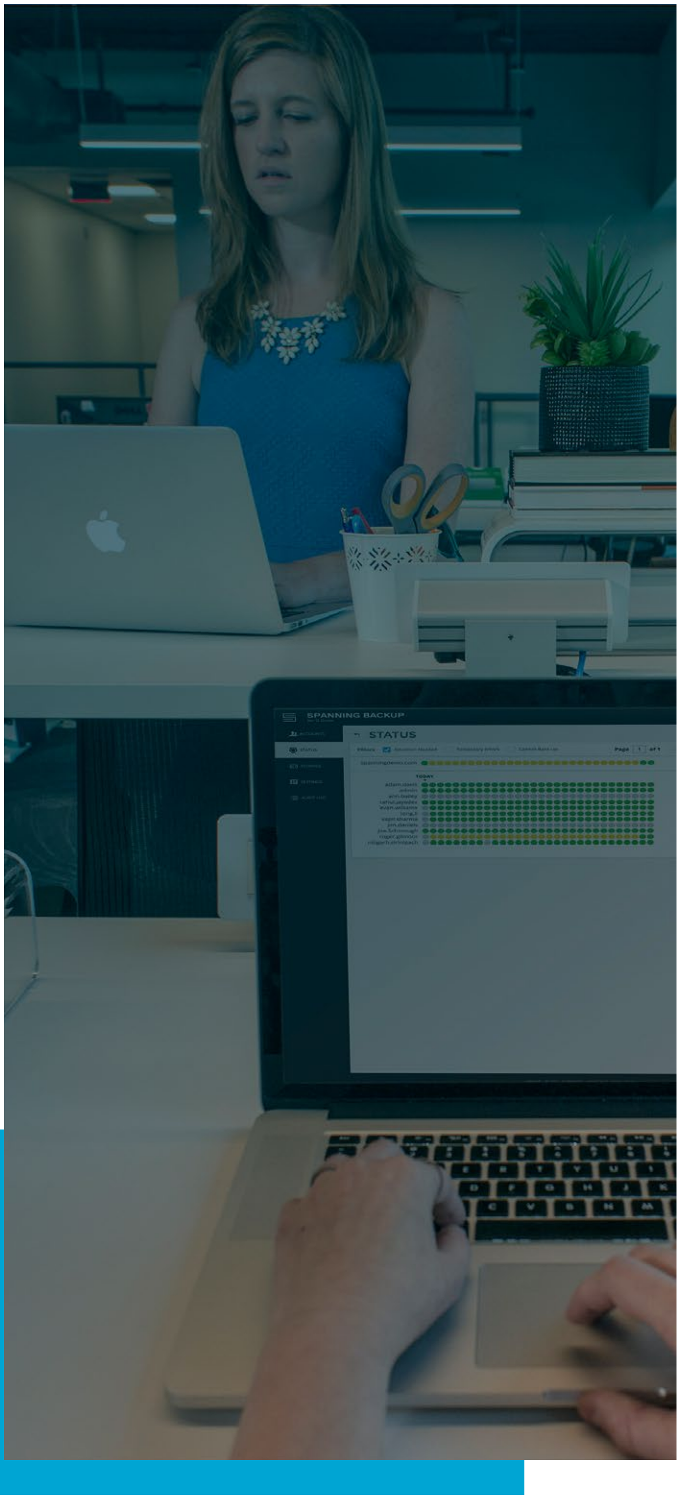


PROTECT YOUR PHI IN THE CLOUD

How to Protect
PHI SaaS Applications and
Stay HIPAA Compliant

SPANNING



CONTENTS

WHY READ THIS WHITEPAPER?

In the first couple of months in 2017 alone, the **US Department of Health and Human Services (HHS)** collected over 11 million dollars in fines due to **Public Health Information (PHI)** data breaches. It worked out to an average of $2.8 million per fine.

The onus is on us. Countless cases such as these underscore the fact that PHI data breaches due to malware, ransomware, device theft or even the occasional disgruntled employee are punishable by law. As the HHS highlighted in one such case "$2.5 million settlement shows that not understanding **HIPAA (Health Insurance Portability and Accountability Act)** requirements creates risk". Having a robust data protection plan to rapidly prevent and/or recover from data loss is not a nice-to-have, but a necessity.

READ THIS WHITEPAPER TO:

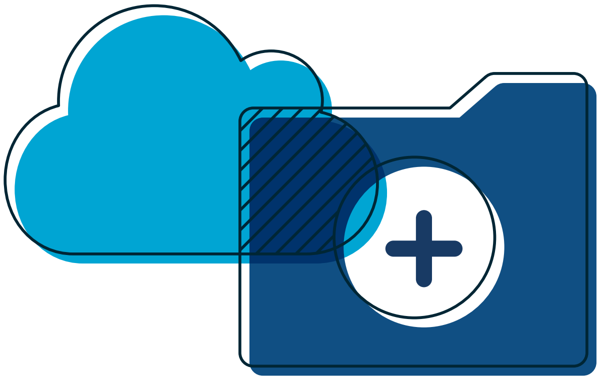
- Understand the implications of HIPAA on Electronic Public Health Information (e-PHI).
- Identify potential gaps in native data protection by cloud providers.
- Overcome these gaps to keep your organization HIPAA-compliant.

UNDERSTAND THE IMPLICATIONS OF HIPAA IN e-PHI

Healthcare institutions, pharmaceutical organizations, and other entities managing protected health information are increasingly turning to the cloud to improve agility, connectivity, and accessibility. SaaS applications like G Suite, Office 365, Salesforce, and Veeva are revolutionizing healthcare operations. However, data breaches are also on the rise and proper data protection, especially of PHI, remains a top concern. That is because PHI data is incredibly valuable on the black market; worth 10 times more than credit card information[1]. To address these risks, HIPAA was further buffered with the **Health Information Technology for Economic and Clinical Health (HITECH)** Act of 2008 and the Omnibus Rule of 2013. Let's understand HIPAA's stance on e-PHI in plain speak.

WHAT DOES HIPAA SAY ABOUT PHI IN THE CLOUD?

HIPAA mandates that covered entities and their business associates must comply with the HIPAA and specifically with the HITECH and Omnibus Rules that address e-PHI. As a covered entity, you are responsible for ensuring the security of PHI and must institute measures to guard against unauthorized use and disclosure of PHI.



WHO MUST COMPLY WITH HIPAA?

- **Covered entities**
  Health care providers, Health plans and Healthcare clearinghouses.

- **Business associates**
  Entities, Vendors or Subcontractors that create, receive, maintain, access or transmit PHI on behalf of a business associate.

"When a covered entity or a business associate engages the services of a CSP to process and/or store ePHI, on its behalf, **the CSP or the CSP subcontractor is a business associate under HIPAA."**

[1] http://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

HERE IS A QUICK RUNDOWN OF HHS GUIDANCE ON HIPAA AND THE CLOUD:

01

A covered entity can engage a CSP to store e-PHI provided that it enters into a HIPAA-compliant **Business Associate Agreement (BAA)**. The CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules. Don't skip the BAA! It cost Oregon Health & Science University $2.7 million because they did not have a BAA with their CSP.

02

The HIPAA Rules do **not** endorse, certify or require specific types of technology/products or providers.

03

Both covered entities and business associates must conduct risk analysis to identify and assess potential threats and vulnerabilities to the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.

04

The BAA is required even if the CSP handles only encrypted ePHI and lacks an encryption key for the data. A CSP providing such "no-view" services is not exempt from HIPAA Rules.

05

A summary of the three main HIPAA rules vis-à-vis e-PHI and cloud computing are:

- **Privacy Rule:** The CSP must still ensure that it only uses and discloses the encrypted information as permitted by its BAA and HIPAA's Privacy Rule. The BAA must require a business associate to return or destroy all PHI at the termination of the BAA where feasible.
- **Security Rule:** All ePHI must be properly secured from unauthorized access (a breach), whether the data is at rest or in transit. Physical, technical and administrative safeguards have to be put in place to protect the PHI.
- **The Breach Notification Rule:** All covered entities and business associates (including CSPs with no-view services) must report data breach incidents to the HHS.

FURTHER READING

HHS guidance on Guidance on HIPAA & Cloud Computing

Main HIPAA Rules

Ransomware Fact Sheet from HHS

WHAT DO CLOUD SERVICE PROVIDERS (CSP) SAY ABOUT PHI?

To be HIPAA-compliant, it is important to understand how your CSP manages e-PHI and fulfills HIPAA requirements. For instance, some cloud providers restrict organizations to a subset of their application services so that e-PHI can be properly safeguarded. IT administrators need to configure their cloud and SaaS environments accordingly.

FURTHER READING

Google Apps HIPAA compliance support

Salesforce for healthcare overview

Office 365 HIPAA FAQs

CHECKLIST FOR CSP-HIPAA COMPLIANCE.

- □ Check security standards followed, risk analysis reports and independent audit reports (and their frequency). Review the security controls included with their service and if they are mapped to the HIPAA/HITECH requirements.
- □ Ask about response times and disaster recovery plans.
- □ Review the security model, tools and strategies. Does the CSP use a multi-layered approach with anti-malware, DDoS mitigation, firewalls, IP reputation filtering, and multifactor authentication?
- □ Verify that the CSP subcontractors have been independently assessed.
- □ Ask about data segregation and security between tenants.
- □ In particular when outlining the BAA with the CSPs, check on the following:
  - □ Encryption of your data in transit and at rest Ownership of your data.
  - □ Data portability, with no vendor lock-in.
  - □ Enterprise integration, via open interfaces and APIs.
  - □ Complete compliance by protecting your unstructured data just like your structured data (EHR).

WHAT ABOUT THIRD-PARTY SAAS APPLICATIONS ACCESSING E-PHI?

You will likely need to add third-party services to your SaaS environment to protect and enhance your use of G Suite, Salesforce, or Office 365. In the eyes of the law, as well as your primary CSP, it is your organization's responsibility to ensure that appropriate HIPAA-compliant measures are in place with any third-party application or service before sharing or transmitting e-PHI. Security vulnerabilities involving third-party application software are on the rise. The HHS even published a newsletter highlighting the risks inherent in third-party application software.

Vet your vendors well! Sign additional BAAs with the provider of any SaaS application that will integrate with your cloud environment. Furthermore, include third-party SaaS applications as part of your regular HIPAA assessments.

AND LASTLY, WHAT ABOUT CUSTOM SAAS APPLICATIONS?

An important subset of SaaS applications that must also be HIPAA-compliant are the custom applications built to meet your organization's operational needs. These will likely run on a CSPs platform (like the internal-only custom apps built on Force.com, the Salesforce platform). These are often built to feed data into ERP systems, HR systems, and financial systems of record; so they're key to your organization's operations and will likely contain e-PHI. Keep to the same level of adherence to HIPAA rules with custom apps as with CSPs and third-party vendors. Checks such as full data encryption both in transit and storage, complete audit trails with access logs stored in a separate environment, automatic upgrades and patches will help ensure HIPAA compliance.

> It is your organization's responsibility to ensure that appropriate HIPAA-compliant measures are in place with any third-party application or service.

FURTHER READING

HHS newsletter on Risks in Using Third-Party Software

HHS resources for Mobile App Development

FTC checklist for Secure App Development

IDENTIFY GAPS IN DATA PROTECTION BY CSPS

You've grappled with HIPAA, done your due diligence and worked out a rock-solid BAA with your CSP, third-party vendor, custom software developer, et al. And then a data breach occurs. Welcome to the fine print.

Google, Microsoft, and Salesforce do an expert job of protecting your data from accidents and losses within their control – like server failures caused by a natural disaster. However, they are severely limited in how they can protect you from mishaps that happen on your side of things, leaving you vulnerable to data loss caused by several risk factors. Why? G Suite, Office 365, and Salesforce are not designed to be specialized backup and recovery services in addition to the core applications they provide, and there are policies in place that restrict the data recovery capacities of these vendors.

SAAS AND CSP VENDORS CANNOT PROTECT YOUR DATA FROM...

Human Error on Your Side

IT operations for Healthcare services is largely manual and error-prone. Data breaches due to human error, though accidental, can pose serious risks of HIPAA noncompliance as it constitutes a failure to protect e-PHI. An example of this case is accidental deletion. Your service level agreement (SLA) with your cloud vendor legally requires them to purge data you instruct them to delete.

Google warns, "Once an administrator or end-user has deleted any data in Google Cloud, we delete it according to your Customer Agreement and our Privacy Policy."

Malicious Insiders

Your e-PHI data can also be at risk from malicious insiders. In one case, the FBI reported that an IT director for an organ donation nonprofit repeatedly gained unauthorized access to her employer's network via a remote connection from her home and intentionally deleted numerous database files and software applications, as well as their backups. Further, attempting to conceal her activities, she disabled the logging functions on several servers and erased computer logs that recorded her remote access to the network.

> 80% of healthcare data breaches reviewed in the report resulted from human error - privilege misuse, miscellaneous errors, physical theft and loss.
>
> —
>
> Verizon's Data Breach Investigations Report 2017

Sync Errors

It is common for SaaS applications to be integrated with other systems, and that increases the possibility of data loss due to a failed sync. One of our clients, for example, experienced data loss when an HR folder was moved within Google Drive and didn't sync correctly. As a result, all files were lost – including some that weren't even owned by the user moving the folder.

Hacking

Healthcare hacking is fast overtaking human error as the main cause of data breaches. The **Office for Civil Rights (OCR)** of the HHS reported that four of the top five data breach incidents in 2017 were caused by healthcare hacking. Due to the rising incidents of ransomware, the HHS issued a ransomware factsheet in 2016 followed up by email warnings that it "presumes a breach in the case of ransomware attack" which must be reported by the entity within 60 days of discovery.

> 2017 on Track to Exceed 2016 Trend of 'One Health Data Breach Per Day'. Hacking Responsible for 53% of Breached Patient Records.
>
> —
>
> Protenus Breach Barometer Report 2017

DAMAGE CAUSED BY THESE GAPS

Recovery is Either Impossible or Costly

Your CSP has no way of knowing if data deletion or manipulation is malicious, accidental, or intentional. So, when accidents do happen, CSPs can't help you recover data quickly, if at all. Even when a CSP can help you recover lost data, the process can be confusing, lengthy, and expensive. For example, recovering data through Salesforce can cost a minimum of $10,000 and can take several weeks.

Business Downtime

The cost of business downtime due to a breach is difficult to quantify, but can be significant as it impacts both employees and customers. In particular, a cyber attack adds to the complexity and time taken for recovery. In a recent survey[2] of security experts at RSA 2017, almost 60% said that the cost of downtime due to lack of access to systems for customers and employees was the biggest business impact of a ransomware attack.

Compliance Risk and Cost

If the breach affects more than 500 records, expect it to be publicly listed on the HHS Office for Civil Rights (OCR) breach portal, infamously known as HIPAA's Wall of Shame. And then there is the cost. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision.

Damage to Reputation

It doesn't matter how big your business may be, if you lose customer information, it will damage your reputation. 7 out of 10 patients (65%) were willing to change healthcare providers if the company was affected by a data breach. According to reports, the average estimated value of a corporate brand or reputation is $1.5 billion, which is not something that a business can really afford to throw away, especially on something that can be prevented.

That's why most CSPs recommend implementing a third-party backup solution. HIPAA too puts the liability on covered entities to "securely back up retrievable exact copies of electronic protected health information."

POSSIBLE COST OF COMPLIANCE[3]

- **HHS fines:** up to $1.5 million/violation/year
- **On-going credit monitoring for affected patients:** $10/individual
- **Federal Trade Commission fines:** $16,000/ violation (violation = per record)
- **Class action lawsuits:** $1,000/record
- **State attorney generals:** $150,000 – $6.8 million
- **Patient loss:** 40%

[2] https://www.imperva.com/docs/RiseofRansomware.pdf

[3] http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html

STAYING HIPAA-COMPLIANT IN THE CLOUD

You heard that right. Most CSPs recommend implementing a third-party backup solution to augment the protection they're able to provide. Google support tells its users, "For non-email data recovery solutions, please consult the Google Apps Marketplace, where one of our partners may have a solution suitable for your needs." And Salesforce says, "We recommend that you use a partner backup solution that can be found on the AppExchange." Furthermore, HIPAA puts the backup and restore accountability squarely on Covered Entities. HIPAA's Security Rule mandates that backups should be frequent, encrypted, tested and stored offsite and covered entities must be able to fully "restore any loss of data."

AVOID THE STRESS, COST AND LIABILITY OF A PHI DATA BREACH

Despite the huge damage of a data breach in terms of cost, reputation, and business losses, backup and recovery systems are currently in use at only 45% of surveyed healthcare organizations, and more than 38% are not planning to use backup and recovery systems at all[4]. Why needlessly put yourself and your organization under the looming stress and liability of a PHI data breach? A HIPAA-compliant backup and restore solution can ensure your complete compliance and eliminate worry over data loss (not to mention saving you from costly fines and negative press).

HIPAA-CHECK YOUR BACKUP AND RESTORE SOLUTION

Here is a list of HIPAA must-haves for e-PHI backup and restore.

HIPAA Check #1: Offsite Storage -> Cloud-to-cloud SaaS model

Choosing a cloud-to-cloud backup provider allows you to continue enjoying the cost-saving benefits that drew you to adopt SaaS applications. Instead of managing backups on-premises, an extremely time-consuming and error-prone activity, consider a cloud-based backup solution. They allow you to save time and money while managing backups effectively and allowing your IT team to focus on strategic endeavors.

HIPAA Check #2: Regular Backups -> Support for Automated and on-demand Backups

Automated backups allow you to "set it and forget it" as your backups will run automatically each day. On-demand backups enable manual backups that support data protection before major database or organizational changes are made.

[4] https://www.cleardata.com/wp-content/uploads/2016/12/2016-HIMSS-Analytics-Cloud-Study.pdf

HIPAA Check #3: 100% Restore -> Fast and accurate recovery
We've outlined the huge costs of e-PHI data loss. Combine that with HIPAA compliance risk and related fines, and you have a perfect financial storm – unless fast and accurate data recovery is part of your evaluation process. Look for a backup and restore solution that can get your data back from any point in time, in just a matter of clicks.

HIPAA Check #4: Audit Support -> Immutable Records
HIPAA compliance requires that you ensure changes to e-PHI are auditable, and that there is an immutable record of data at a backup point in time.

HIPAA Check #5: Encrypt or Destroy -> Data encryption at rest and in transit
HIPAA says that data being transmitted must be encrypted and data at rest must either be encrypted or destroyed. This ensures the privacy and security of e-PHI with robust encryption.

HIPAA Check #6: Third-Party Compliance -> SOC 2 and HIPAA compliance
Every link in the chain related to e-PHI should be HIPAA-compliant and highly secure; and that extends to third-party vendors providing backup solutions.

THE SPANNING ASSURANCE: 100% RESTORE. 100% PEACE OF MIND.

Spanning helps healthcare payers, providers, and organizations in the healthcare and pharmaceutical industries work in the cloud with confidence when using leading SaaS applications like G Suite, Office 365, and Salesforce.

Spanning Backup provides automated, daily backups of your application data and the ability to restore any lost or deleted data back into your environment from any point in time. The restore process makes it easy for both application administrators and end users to quickly recover lost or deleted data without calling in an IT expert.

PRODUCT SUITE

- **Spanning Backup for G Suite** protects all your data in Gmail, Drive (including Team Drives), Calendars, Contacts and Sites with the top-rated SaaS application data and recovery solution in the G Suite Marketplace. We're so confident, we give all our customers the industry's first 100% Restore Guarantee for G Suite.
- **Spanning Backup for Office 365** automatically backs up Office 365 Email, Calendars, SharePoint and OneDrive data daily. If data is deleted or damaged, you'll be able to get it back right away – and get everyone right back to work.
- **Spanning Backup for Salesforce** works in Salesforce, so there's no easier way to backup and restore your Salesforce data – from user-generated reports and email templates to objects, files, and metadata. Everything is backed up daily and always available for fast point-in-time, granular restore whenever data is overwritten or deleted.

> "As an FDA regulated business, we have certain compliance requirements that we have to achieve – the biggest one being data retention. Because I know Spanning just works and our data in the cloud is protected regardless of what happens at Microsoft, it's one less thing we need to worry about on a daily basis."
>
> Todd Miller
> IT DIRECTOR, MILLAR, INC.

Contact a product specialist to learn more about what Spanning Backup can do for your organization at +1.512.236.1277 or visit spanning.com.

SPANNING

Spanning Cloud Apps is the leading provider of backup and recovery for SaaS applications, protecting thousands of organizations from data loss due to user error, malicious activity and more. We are the only global provider of powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning is the most trusted cloud-to-cloud backup provider with millions of users around the world. Learn more at www.spanning.com.

501 CONGRESS AVE, SUITE 200
AUSTIN, TEXAS 78701
P +1.512.236.1277

SPANNING.COM