Central Data Storage

QAS INTERNATIONAL
ISO/IEC 27001:2013
REGISTERED COMPANY
Certificate No. UIT1156

How to Make Sure Your HIPAA-Compliant Business is Robust Enough to Weather Any Data Disaster:

A Practical Guide

About this eBook

At Central Data Storage, protecting your data is our only focus.

We understand it can be overwhelming when it comes to protecting your healthcare business and making sure you have the right data backup processes and disaster recovery plans in place, all while maintaining HIPAA-compliance.

That's why we've put together this practical guide.

This eBook will help you to:

- Better understand your HIPAA requirements and how to ensure compliance at all times.
- Understand the impact of a data breach and what it could mean for your business.
- Understand what threatens your data and what is the most common cause of data loss.
- Discover what HIPAA-compliant data backup and recovery looks like.
- Find out what HIPAA-compliant encrypted messaging and file sharing involves.
- Define clear steps to take as part of your data disaster recovery planning.
- Know what to do when disaster strikes and additional implications to consider.

Table of Contents

Introduction

For any business in the healthcare sector, preserving data security and remaining HIPAA-compliant are essential requirements for operational and commercial success – and these are conditions that need to be maintained at all times. Besides the day-to-day running of your affairs, industry standards for information handling and data governance still apply when unexpected events occur that pose challenges to the smooth working of your digital and physical infrastructure - and perhaps threaten the survival of the business itself.

Even when disaster strikes, it's imperative for your organization to make the quickest possible recovery and maintain the required data standards throughout.

There are different causes of data disaster that you need to be prepared for. These include human error, acts of nature, extreme weather or environmental conditions and cyberattacks. In each case, you'll need to ensure that you are able to get your business back up and running the same day as the data disaster occurs. This will ensure minimal impact on your operations and minimize the potential damage caused by pauses in service delivery and the corruption or loss of essential information.

The Need to Stay HIPAA-Compliant

Protected health information or PHI consists of all data relating to an individual's past, present or future health or condition – be that mental or physical. This includes data concerning medical services that person may receive, payments for healthcare and health insurance benefits.

With the digital transformation of much of the world's commerce, this information now routinely takes a digital form, to become electronic protected health information, or ePHI.

The Health Insurance Portability and Accountability Act (HIPAA) has a component called the Privacy Rule, which regulates who can have access to all forms of PHI and the ways that it can be used and disclosed.

In order to be HIPAA-compliant, these regulations require organizations to implement policies and procedures that limit the use and disclosure of PHI to the minimum number of people necessary and restrict access to protected health information to employees with specific authorization.

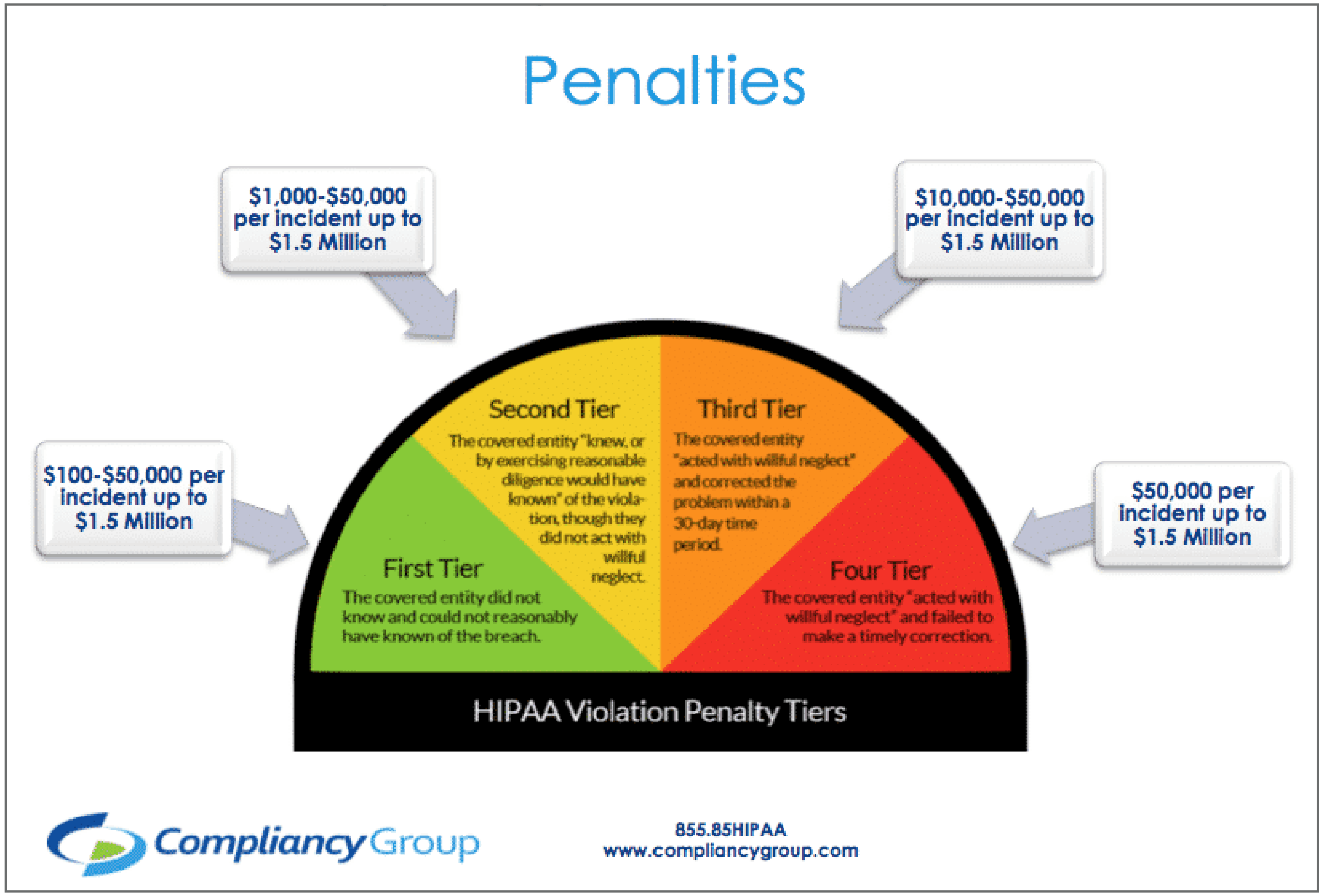
What's more, written authorization from the individual concerned is required before disclosing their protected health information.

The HIPAA Security Rule requires healthcare organizations to protect ePHI via appropriate administrative, physical and technical safeguards to preserve its confidentiality, integrity and availability. The Health Information Technology for Economic and Clinical Health (HITECH) Act expands the scope of HIPAA and promotes the use of electronic health records. HITECH increases liability for non-compliance, regulates breach notification and requires certain business associates of HIPAA-covered organizations to comply with HIPAA.

HIPAA is a federal statute that overrides conflicting rules at the state level – and there are potential civil and criminal penalties for not adhering to its requirements.

Federal fines for non-compliance are based on the level of perceived negligence found within your organization at the time of any HIPAA violation. Sanctions can range from $100 to $50,000 per violation (or per data record), with a maximum penalty of $1.5 million per year for each violation. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has also levied criminal charges for HIPAA violations in the past.

Financial penalties are only part of the story. If your organization ever incurs a HIPAA-compliance breach, the name of your practice is permanently listed on the OCR “Wall of Shame” (a web portal listing the names of offenders) -- including the offense, date, and number of individuals affected -- leaving your business open to bad publicity and reputational damage as well.


Penalties
$1,000-$50,000 per incident up to $1.5 Million
$10,000-$50,000 per incident up to $1.5 Million
$100-$50,000 per incident up to $1.5 Million
$50,000 per incident up to $1.5 Million
Second Tier
The covered entity "knew, or by exercising reasonable diligence would have known" of the violation, though they did not act with willful neglect.
Third Tier
The covered entity "acted with willful neglect" and corrected the problem within a 30-day time period.
First Tier
The covered entity did not know and could not reasonably have known of the breach.
Four Tier
The covered entity "acted with willful neglect" and failed to make a timely correction.
HIPAA Violation Penalty Tiers
CompliancyGroup
855.85HIPAA
www.compliancygroup.com

(Image source: Compliancy Group)

The Importance of Data Security for HIPAA-Compliant Businesses

In the health industry, a lack of availability of critical systems and data can not only lead to fines and damage to your brand image – it may also result in poor patient outcomes, or even loss of life.

To properly protect information and maintain HIPAA-compliance, you need to ensure that both you and your business associates are taking the required steps to minimize the risk of health data being improperly disclosed, damaged, stolen, or rendered unusable.

Major or minor incidents of all kinds may cause a power outage, data loss, or the corruption of critical data. Typically, less than half of businesses are able to recover all their data after a disaster and around 90% of enterprises that lose data from a disaster are forced to shut down within two years.

Small and medium-sized businesses (SMBs) are usually hardest hit, as they lack the resources that larger enterprises have, to bounce back after an extended outage.

For organizations in every sector, the reliance on digital technology now makes a disaster recovery data center pretty much an essential requirement to keep processes going at all times and to ensure economic survival.

Before deciding on its location, take these essential steps:

- Create a contact list of all your critical vendors, suppliers, partners, key clients and employees.
- Determine alternate communication channels (cell phone, two-way radio, etc.) for contacting them in an emergency.
- Document your hardware, software and licensing information.
- Decide which machines you will back up and which data is essential for your business to function.
- Decide how long you can operate without your business-critical systems.
- Create a plan to restore your essential data in a timeframe that meets your recovery time objective.
- Set regular backup times that meet your response point objective and monitor backup status.
- Back up all data to a secure off-site data center.
- Test your backup regularly and make sure it’s restoring data accurately and in a timely manner.

Threats to the Security of Healthcare Data

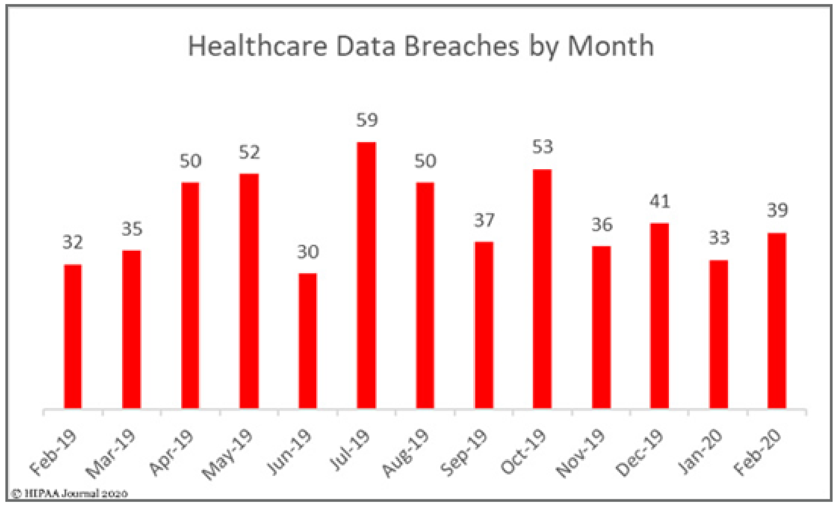
Protected health information – and ePHI in particular – presents a high-value target for hackers and cybercriminals. This might be for financial gain through selling the information, identity theft, extortion, or blackmail.

According to research by Coveware, healthcare ranked third among industries targeted by ransomware attacks in 2019, largely because attackers understand that the urgency to restore data required for medical treatment means they are more likely to get paid. Even if victims do pay a ransom, there's no guarantee that the perpetrators will release the keys required to decrypt your data.

The only effective safeguard against ransomware attacks is to have clean and up-to-date backups of all essential information held at a secure, HIPAA-compliant, off-site location.

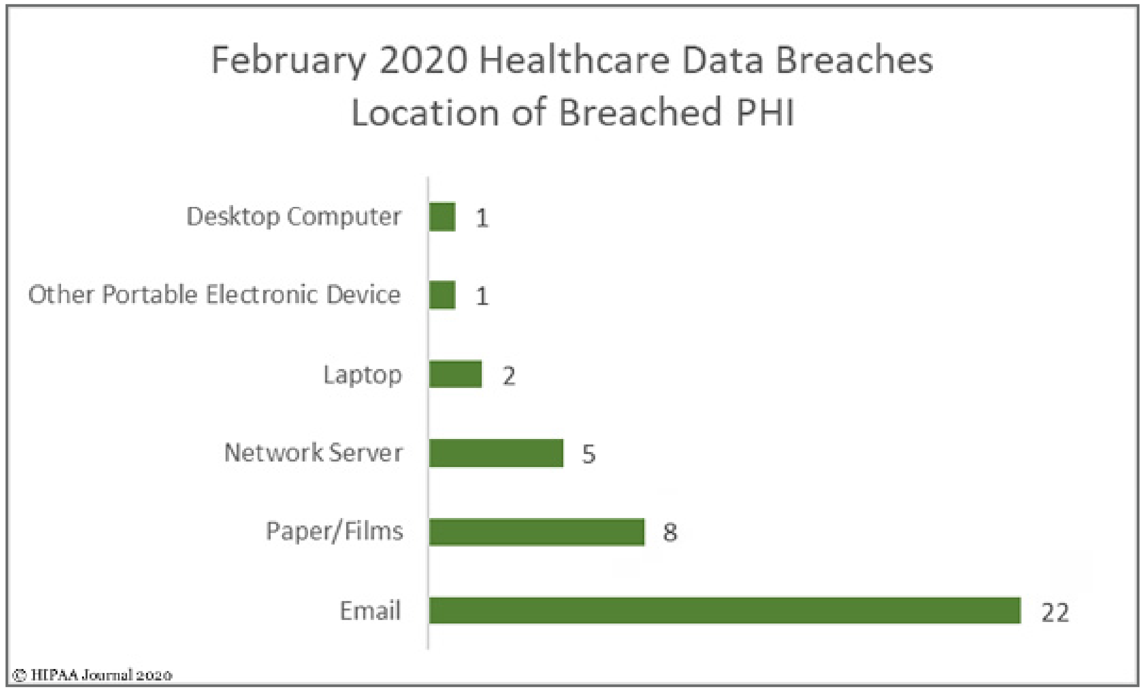
As much as 90% of data loss can be attributed to human error. A data breach can occur if someone accesses information without authorization – not always with malicious intent. The same holds true if an authorized user accidentally discloses PHI to a third party.

Data leakage or data exfiltration occurs when information is disclosed or copied to an unauthorized location. In many small and medium-sized businesses, all staff members use the database that stores client data and since they all have varying degrees of technological skills, accidents and errors are bound to occur.

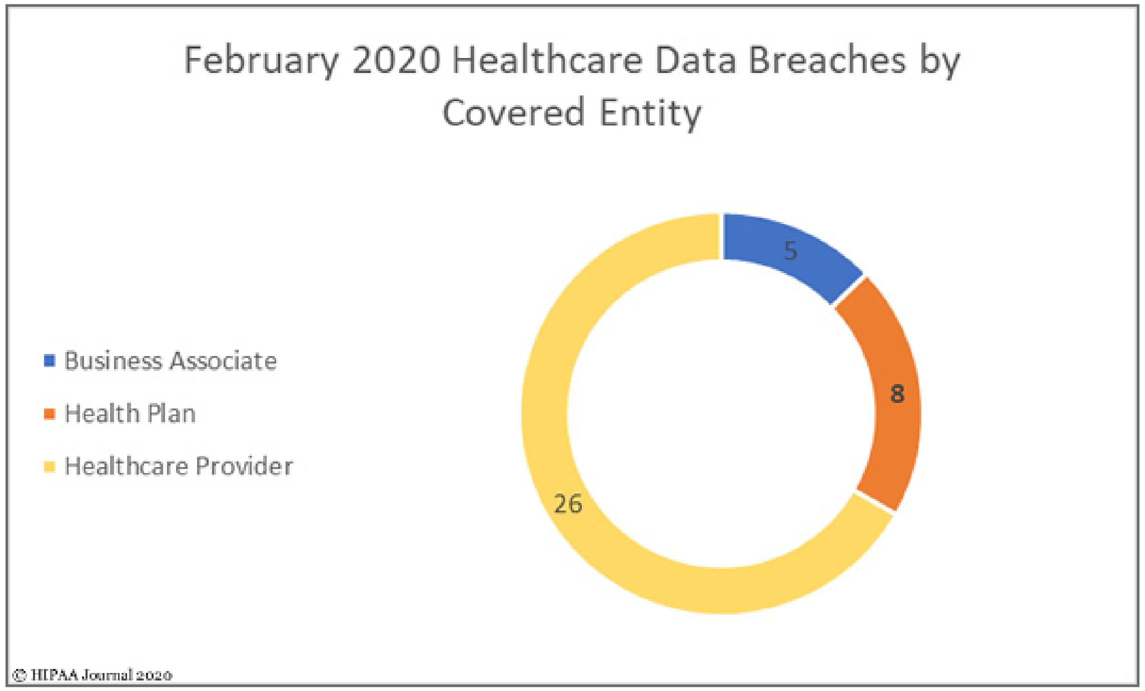


(Image source: HIPAA Journal)

According to the HIPAA Journal, there were 39 reported healthcare data breaches of 500 or more records in February 2020, with more records breached in February than in the past three months combined. Incidents were spread across 24 states, with circumstances ranging from external hacks and IT incidents, through to the improper disposal of paperwork containing PHI, to the theft of an employee's laptop.



(Image source: HIPAA Journal)



(Image source: HIPAA Journal)

To guard against scenarios like this, the HIPAA Security Rule requires organizations to adopt user authentication safeguards, which include unique multi-factor password protection, typically achieved using Active Directory and a token-based security key.

System administrators should also impose role-based access rules, giving users restricted access on a strict need-to-know basis. This helps prevent the use of backup data by unauthorized personnel.

All businesses will face some sort of data loss at a point, so it's essential you have a robust disaster recovery plan in place that can be implemented at a moment's notice.

The ability to recover critical business and patient data quickly is something that every business requires.

This emphasizes the need to create a recovery procedure with steps to remedy any data interruption – and to have an alternative recovery site for your critical systems and information.

The Added Complications When Disaster Strikes

Extreme weather events and natural disasters can occur at any time, as well as unforeseen crisis situations like the COVID-19 pandemic. Such incidents may cause physical damage to business infrastructure, the corruption or loss of digital assets, or create a need for new working practices like remote collaboration and social distancing.

A disaster recovery data center (or the physical infrastructure of a cloud service provider) should be close enough to your primary location to allow for reasonably convenient access to the recovery site, but far enough away to be well clear of any threats that might impact the primary facility.

When deciding on a location, you should keep a close eye on known weather, geological and seismic patterns.

Besides location, you'll want to know that a Disaster Recovery (DR) provider has experience working with a business like yours, in terms of size, operations and the challenges you face in remaining HIPAA-compliant.

Planning for the Unexpected

Early on in your disaster management strategy, you'll need to decide who will be responsible for overseeing both primary data storage and backup. Notify these people of their responsibilities, clarify their roles and establish expectations.

Decide which data disasters are most likely to affect your business and which will do the most harm. Draw up remediation strategies and take action to mitigate these threats pre-emptively.

Communicate these changes to all employees and make sure that everyone knows what's expected of them and the correct procedures to perform in the event of any incident.

When looking for a Disaster Recovery partner, create a short list of the available options and choose a provider who not only meets your data encryption, backup and recovery requirements, but also complies with government regulations.

Under HIPAA and HITECH, those requirements are extremely strict.

HIPAA-Compliant Data Backup and Recovery

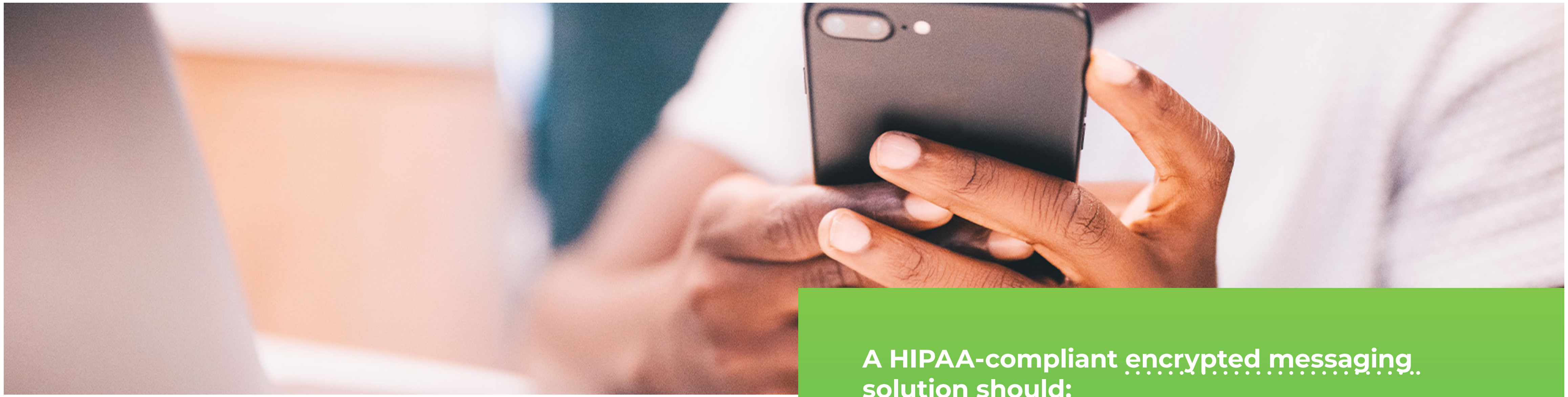
Under a secure backup, archiving and recovery solution that complies with HIPAA standards, all Covered Entities (CE), medical practices and Business Associates must securely back up "retrievable exact copies of electronic protected health information" in a recoverable format that enables users to fully restore any lost data. These backups must be frequent and regular.

Backup copies of ePHI must be held off-site from the original data storage point. Under HITECH, you must either encrypt or destroy all data held "at rest" in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.), in order to secure it. The HIPAA Security Rule also mandates the encryption of all data that's being transmitted (data in transit).

As such, your HIPAA-compliant data backup solution has to:

- Use data encryption – either by using storage hardware or operating system level encryption techniques. Network traffic must use strong AES 256-bit encryption when transmitting data externally.
- Employ user authentication safeguards – including unique multi-factor password protection.
- Use role-based access rules – with permissions on a need-to-know basis, following a "least privileged" design.
- Have off-site storage capabilities – with backups stored in a separate location to your primary production services.
- Use secure data center facilities with detailed monitoring and reporting functions – configured with alerts in the event of any failures.

HIPAA-Compliant Encrypted Messaging



For any healthcare organization whose workers routinely communicate PHI with each other by text via a public service provider, HIPAA-compliant encryption for text messaging is a key requirement. In addition, the HIPAA Security Rule demands administrative, physical and technical safeguards for messaging systems.

A HIPAA-compliant encrypted messaging solution should:

- Segregate healthcare text messages from personal communications.
- Require authorization and user authentication for accessing messages.
- Encrypt message data in transit and within the network, using TLS/SSL (or similar) between all server nodes.
- Encrypt all health related data on mobile devices.
- Exclude PHI from screen notifications by blocking text previews from message alerts.
- Fully archive all messages sent within your organization's network.
- Automatically audit and log all administrator activities relating to user management, security polices, authentication events and all read receipts of messages.

✓ **What is Encrypted Sharing?**

LEARN MORE

HIPAA-Compliant File Sharing Solutions

With regard to file sharing, HIPAA demands technical safeguards for protecting data, such as access controls, user authentication and encryption. Physical safeguards restricting access to your premises and files should be in place, extending protection to your IT infrastructure, employee workspaces and other equipment. And administrative safeguards should lay out actions, policies and procedures relating to the management and maintenance of ePHI protection.

A HIPAA-compliant file sharing solution should:

- Use file level encryption, requiring user authentication in order to view, download, edit, or delete specific files.
- Employ virtual disk encryption for cloud-based file storage or sharing services.
- Implement full-disk encryption for all physical hard drives.
- Use unique user IDs to limit access to authorized personnel.
- Use multi-factor authentication for user verification.
- Have an idle logoff feature, requiring users to re-enter their password and authorization after a set period.

Making Provisions for the Future

All of these data management requirements for HIPAA-compliance are stringent enough, but as technologies evolve, new technical challenges and threats are emerging.

Cloud technology is increasingly being used in a wide range of applications across the entire healthcare system, ranging from back-end development and data sharing, to consumer-facing portals and mobile apps. Poorly secured internet connections can contribute to making HIPAA-compliance a nightmare.

Multimedia data streams such as those involved in telemedicine and virtual consultations are increasing the healthcare system's attack surface. So too are IoT (Internet of Things) components, many of which are not designed with security in mind and whose default passwords are in a manual you can look up on the internet.

A report from Forrester Research reveals that two U.S. hospitals have recently been attacked via virtual care systems, after a hacker targeted a vulnerability in a medical IoT device (a remote patient-monitoring sensor) and gained access to their patient databases.

With healthcare resources often stretched to the limit, ransomware attacks on medical IoT devices and healthcare networks are also on the increase.

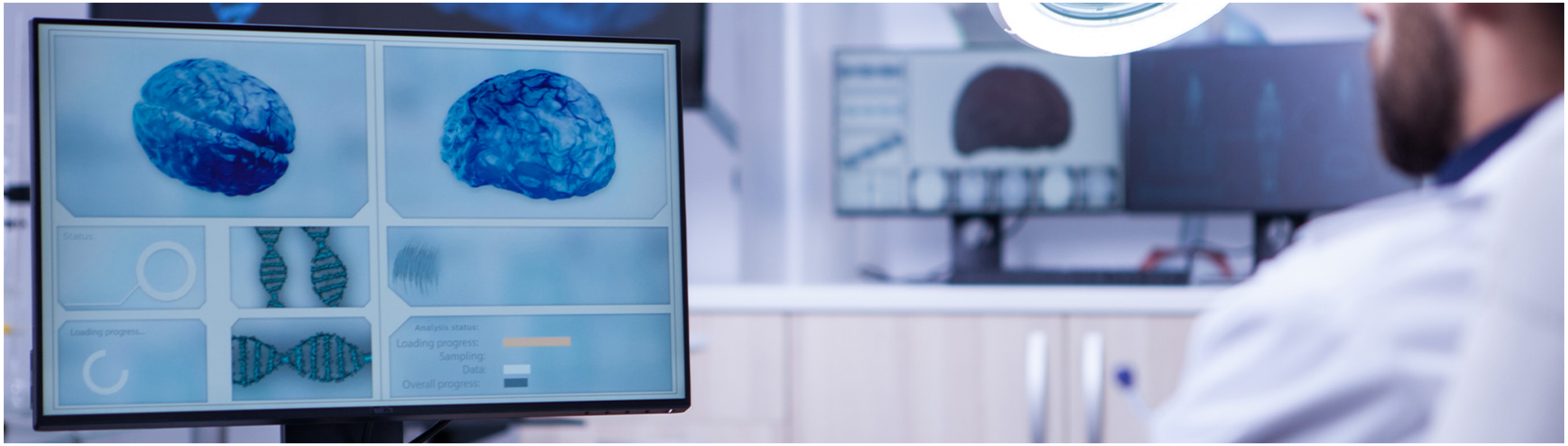
In this atmosphere, organizations in the health sector will have greater need than ever for reliable partners in data backup and recovery.

What You Need From A Good Data Backup Provider

An off-site data center, remote from any threats against your primary facility.

A private cloud offering, enabling you to keep your most sensitive data assets close to home.

Reliability and a proven track record in helping healthcare businesses remain HIPAA-compliant.



Why You Need to Act Now

With all the various kinds of data disaster that can occur (human error, weather, cyberattack etc.), you need to ensure you have data backup, recovery, encrypted messaging and file sharing solutions in place – and that these solutions are HIPAA-compliant.

In this time of uncertainty, you also need to protect your business, keep your competitive edge and position your organization to recover quickly from any setback.

Most importantly of all, you need to protect your business against the unexpected, as you don't know what the future will bring (human error, pandemic or a natural disaster).

Central Data Storage (CDS) is a software and services company that offers HIPAA-compliant data sharing, backup and recovery solutions for healthcare businesses. CDS manages over 6 billion patient files per month for organizations whose primary area of expertise isn't technology, or data administration, providing above military grade data encryption in an easy to manage solution.

If you need to keep your business compliant with HIPAA regulations and proof it against any data disaster, sign up for a one month free trial of CDS Backup + Recovery.

✓ **Interested in finding out how Central Data Storage can help you?**

EXPLORE NOW

Central Data Storage

Contact Us

info@centraldatastorage.com Toll-free +1-888-907-1227

www.centraldatastorage.com