

WHITE PAPER REPORT:

How Remote Data Backups, Inc. Helps Health Care Providers become HIPAA Compliant



Use our secure, automatic, offsite backup service to comply with HIPAA's Privacy and Security Rules.



Remote Data Backups, Inc.

A Decade of Data Protection

www.RemoteDataBackups.com

Fort Collins, CO USA

866.7.BACKUP (722-2587)

HIPAA-Compliance and Remote Data Backups

HIPAA (Health Insurance Portability and Accountability Act of 1996) was enacted to improve the access and portability of patient health records while maintaining strict privacy and security of electronically transmitted private information.

Health agencies who fail to comply with HIPAA's regulations now face strict fines and penalties.

Remote Data Backups helps you comply with HIPAA's Data Protection - Data Privacy and Data Security Rules.

Compliance with HIPAA's Privacy Rule

Mandatory Compliance Date: April 14, 2003 for majority of health care providers, with an extra year grace period for smaller health care providers

How Remote Data Backups helps you comply:

- **Secure Transmission**
RDB uses bank-level 128-bit AES encryption to transmit and store your data using a personalized encryption key that you choose, and (unlike our competitors) **only you have access to**. Data is safely stored in two world-class, mirrored data centers.
- **Physical Access**
Using Remote Data Backups ensures **secure, offsite data storage**. Our data centers feature the tightest physical and technical safeguards to prevent unauthorized access to our mirrored data centers. Both are hardened facilities with limited administrative access, finger scanners for physical access and motion detectors and camera tracking.
- **Logical Access**
Logical access to backed up data is strictly controlled with a secure user interface. Users can add a password as another layer of security (version 7x) or change the password if they feel the original has been compromised (version 8x).

Compliance with HIPAA's Security Rule

Mandatory Compliance Date: April 21, 2005 for majority of health care providers, with an extra year grace period for smaller health care providers

How Remote Data Backups helps you comply:

- HIPAA Security Rules require providers to have a **written contingency plan** for responding to system emergencies. A **data backup plan** is required as part of the contingency plan, which Remote Data Backups can provide you at no additional charge. The plan will ensure your data is securely and reliably backed up on a routine basis and that your backed up data will be readily available in the event you have a system failure or other form of data loss.
- Using RDB helps **reduce your Security "Media Control" risks** by eliminating insecure methods of data handling that result from traditional disk or tape backup techniques.
- Files are **securely transmitted** to RDB's data centers using encryption and Secure Socket Layer (SSL) authentication, access controls, auditing mechanisms, and event reporting as required by HIPAA's Security Policy.

Fines and penalties for non-compliance

Federal laws dictate a first fine of \$50,000, and second fine of \$200,000, in addition to liability fines and penalties, if a violation occurs and a healthcare provider is found not in compliance. Non-compliance with HIPAA guidelines could jeopardize healthcare provider's standing.

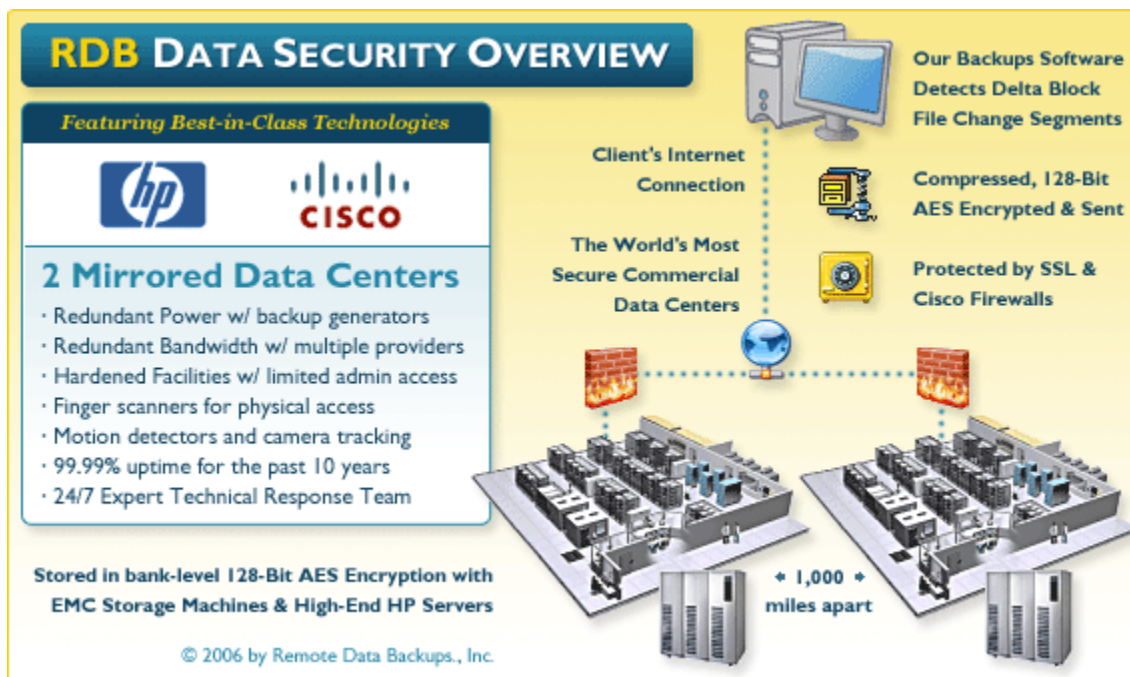
Remote Data Backups industry-leading privacy and security processes, technologies, and policies to store and protect their information and assist their efforts in demonstrating adherence to HIPAA compliance.

Backup Data Security Overview

We've layered state-of-the-art technology to deliver industry-leading security and performance.

Your data is bank-level AES encrypted before it leaves your computer, then transmitted and stored encrypted at our two world-class, underground, mirrored Data Centers.

No one can access your data without your Personal Encryption Key. Redundant fiber optic bandwidth via multiple providers ensures extremely fast and reliable data transfers.



Superior Backup Data Center Technology & Service

Our mirrored data centers employ the industry's leading enterprise technologies to provide our clients with the best security, reliability and performance on the market.



Enterprise HP Servers

Deploying servers from Hewlett-Packard, the world's largest consumer and SMB IT company, helps our data centers maintain over 99.99% historical uptime.



Cisco Hardware Firewalls

Sophisticated hardware firewalls from Cisco, the leader in Network security, securely protect your backup files from hackers, viruses, spybots, etc.



Redundant Bandwidth

We use multiple enterprise bandwidth providers on multiple fiber optic backbones to ensure consistently fast and reliable file transmission.



Physical Security, Power Backup & Support

Both data centers are hardened facilities with finger scanners, motion detectors and camera tracking, redundant power generators and 24/7 Expert Response.



Two Mirrored Data Centers

We store your data at two world-class, geographically separate, mirrored underground backup centers with redundant bandwidth, redundant power and an unparalleled level of data security and performance.

Level 4 Data Center Security

Our two underground data centers are the world's most secure commercial data storage facilities. Features include:

- a. Separated by 1,100 miles, in ultra-secure private limestone mines located 100-200 feet below ground
- b. All data received by either hardened Data Center is immediately replicated to its mirror — connected by point-to-point, high-speed WAN links
- c. Traffic is load-balanced between the two sites, eliminating degraded system performance
- d. Redundant bandwidth with multiple fiber optic telecom providers to ensure consistently fast and reliable transfers
- e. Each server platform has fail over and redundancy, continuous server monitoring and performance tuning, assuring that storage capacity is never exceeded.

Enterprise Network Infrastructure

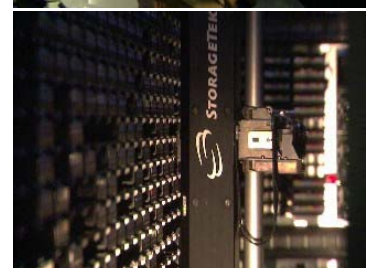
- a. Redundant power supply using backup generators, full power for 7 days
- b. High performance HP Servers & Cisco / Nokia firewall security
- c. Redundant completely independent electrical systems, power train, commercial power feeds, cooling system, UPS systems, dedicated A/C units, generator systems and fuel system
- d. Environment and climate controlled facilities, resistant to seismic activity and other natural disasters, with Class A vaults with OSHA certified fire suppression and EPA certified water treatment plants and clean air fire extinguishing systems (CAFES)
- e. Best practices networking and best-of-breed routers, switches, firewalls, servers, facilities infrastructure, power grids and telecommunications circuits are all deployed with backup components to maximize fail over and redundancy
- f. Failed account access attempts are logged and reviewed to prevent unauthorized access

Impenetrable Physical Security

- a. Level 4 (highest) security rating, 24/7 armed security, maintenance & service operation
- b. Finger scanners for physical access, motion detectors, CCTV monitoring & camera tracking
- c. Co-location equipment is locked in cage with sensors and alarm system
- d. Visitors require pre-authorization and photographic identification
- e. All access to computer equipment is logged

Data received by either Data Center is immediately replicated to the other, so an unlikely outage or disaster at one location will not affect your data availability or service performance.

This is a comforting fact in light of the frequency of recent natural disasters (hurricanes, floods, earthquakes, tornados, etc.) that can easily destroy a single, less fortified data center.



128-Bit AES Encryption

Your files are securely transmitted, stored and retrieved using government-level AES encryption.

If someone were to somehow intercept your data during a backup or restore, or gain access to our servers (which, of course, has never happened), it still take multiple supercomputers decades to decipher any of your data.

Advantages of encrypted backups

- It would be far easier for someone to steal your local backups (*tape*, *CD-DVD*, *Zip/Jaz*) than to intercept and decrypt your encrypted offsite data.
- Local backups containing your sensitive data are rarely encrypted or even protected by a simple password.
- Disgruntled employees, competitors, hackers, thieves, curious people who find lost tapes, etc. all jeopardize the safety of unencrypted backups. Backup tapes are pocket-size, so you might not even notice they are gone.

How Secure is 128-Bit AES Encryption?

If a super-computer could break the DES code in one second, it would take the same supercomputer 149 trillion years to decode a 128-bit AES key - longer than the existence of our universe. It is safe to say no supercomputer in the foreseeable future will be able to brute-force AES 128 bit. As long as no one finds your encryption phrase, your encrypted data can never be deciphered.

Secure Socket Layer (SSL)

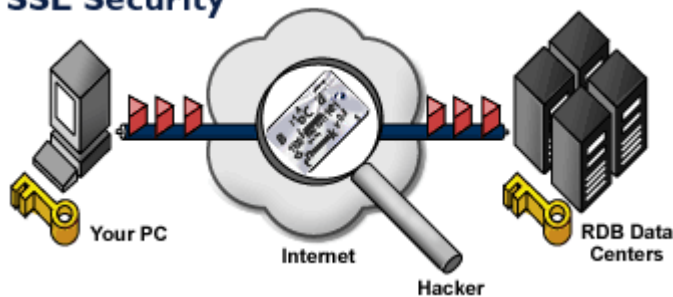
Digital certificates encrypt your backup data in transit using Secure Socket Layer (SSL) technology, the industry-standard for protecting Internet communications from hackers.

SSL negates packet sniffing

SSL encrypts each packet of data using complex digital keys by both your Internet Connection and our data centers.

Any data a hacker could possibly access appears as random, nonsensical characters, only decipherable by our servers which possess the digital key to decrypt, or unscramble, the data.

SSL Security



Without SSL, hackers can easily view your data transmitted through the Internet essentially as plain text.

Any sensitive information such as credit card numbers, contacts, etc., could easily be stolen or compromised.



Did You Know...

NIST (National Institute of Standards and Technology) determined that 128-bit AES is secure enough to protect U.S. Government classified information up to the TOP SECRET level.

AES is the government *and* commercial standard for encrypting sensitive digital information, including financial and telecommunications data.

SysTrust Certified Backup

Our online backup system has been examined and SysTrust Certified by the independent accounting firm PriceWaterhouseCoopers.

SysTrust is an assurance service developed by the American Institute of Certified Public Accountants ([AICPA](#)) and the Canadian Institute of Chartered Accountants ([CICA](#)).



SysTrust Certification is critical assurance for any CPA, bank, lender or financial institution subject to an audit of their data security system. Failure to meet industry standards, or loss of data due to improper security data procedures, can result in penalties and fines of up to \$1000 per infraction (customer).

A SysTrust Certification is designed to offer assurance to a broad audience—management, boards of directors, customers, and business partners—about the information systems that support a business or one of its segments.

In a SysTrust engagement, a CPA performs an examination or audit to evaluate the system's reliability. A positive SysTrust report attests to the system's reliability and ability to operate without material error, flaw, or failure during a stated period of time in a specified environment.

SysTrust tests system reliability according to four essential principles:

- 1. Security**
The system is protected against unauthorized physical and logical access.
Restricted data center access, bank-level encryption, private key.
- 2. Availability**
The system is available for operation and use at times set forth in service-level agreements.
Our data centers have over 99.99% availability for the past 10+ years.
- 3. Processing Integrity**
System processing is complete, accurate, timely, and authorized.
Data is encrypted before it leaves the host, then transferred and stored in encrypted format.
- 4. Maintainability**
The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.
Software and data center updates don't interfere with client backups and restores.

Certification process encompasses our general IT infrastructure, including:

- Production data center and network operations
- Server configuration and database administration
- Storage management systems
- Disaster recovery processes
- System monitoring tools and processes
- System security (both logical and physical)
- Change management and common support processes.

Clients would be interested in a systems assurance examination for some of the following reasons:

- Internal and external users can lose access to essential services because of system failures and crashes.
- Systems can be vulnerable to viruses and hackers because of unauthorized system access.
- System failure can result in loss of access to system services or loss of data confidentiality or integrity.
- Negative publicity in the wake of high-profile system failures can undermine customer and investor confidence.

The Risks and Penalties of Sensitive Data Loss

Prevent data loss, data breach and unauthorized access by thieves, hackers, contractors, vendors, remote, mobile & former employees, etc. Avoid serious costs of sensitive data loss — negative publicity, legal liability, regulatory penalties, lost customers and business.

Protect Sensitive Data

How damaging would it be if your sensitive data fell into the wrong hands?

- Identity theft data, i.e. social security numbers, credit card numbers, passwords, PIN numbers, etc.
- Financial data including bank accounts, tax id numbers, transactions, etc.
- Valuable intellectual property and proprietary information
- Confidential client medical data, private employment records, etc.

Data Loss Risks

Do you have reliable safeguards in place to protect your data from being compromised by all these common threats?

- Lost & stolen laptops & PCs
- Former & disgruntled employees
- Mobile and remote employees
- Contractors, outsourcing help
- Vendors, customers, competitors
- Sophisticated computer criminals and hackers, remote access Trojans (RATs), pharming & phishing scams, spyware, adware, viruses, etc.

The Cost of Data Loss

The potential damage caused by a single data security breach cannot be understated:

- **Regulatory penalties**
Increasing federal and state laws include stiff fines and penalties for compromising sensitive client data;
- **Consumer notification**
Most regulations require you to notify all affected consumers of the breach — by mail, email, phone, website posting, or major media outlet;
- **Legal liability**
Litigation can cost you significant time, money and resources;
- **Negative publicity**
If the media catches your data breach, you might quickly lose public confidence in your organization;
- **Lost customers and business**
Inevitable and often irreversible consequences, even with effective and costly public relations campaigns.
- **Brand Name Damage**
If you suffer a well-publicized data breach, the public will always associate it with your company's name.

Healthcare & Dental Backup Clients

Thousands of medical professionals trust Remote Data Backups to protect their critical HIPAA-sensitive data. Here are just a few with print-friendly logos.