

# HIPAA Compliance

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in August 2006 with the intention of enabling better access to health insurance, reducing health care fraud and abuse, and lowering the overall cost of health care in the U.S. Who must comply with HIPAA?

All covered entities who store patient data electronically must comply with HIPAA. Covered entities are defined as 1) health plans, 2) health care clearinghouses and 3) health care providers (doctors, dentists, etc.) How does RBS help me become HIPAA compliant?

Global Data Backup helps covered entities comply with both the HIPAA Privacy and HIPAA Security Rules. HIPAA Privacy Rule: Mandatory compliance - April 14, 2003

The HIPAA Privacy Rule sets standards for how protected health information "in any form or medium" should be controlled. The HIPAA Privacy Rule specifically requires that privacy and security be built in to the policies and practices of health care providers, plans, and others involved in health care. HIPAA Security Rule: Mandatory compliance - April 21, 2005

The HIPAA Security Rule is the first comprehensive Federal protection for the privacy of personal health information. The HIPAA Security Rule identifies standards and implementation specifications that organizations must meet in order to become compliant.

The general requirements of the HIPAA Security Rule establish that covered entities must do the following:

- Ensure the confidentiality, integrity and availability of all electronically protected health information the covered entity creates, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
- Ensure compliance by the workforce. How does RBS remote backup help me comply with the HIPAA security and privacy rules?

Encryption of data during backup: All data being backed up is encrypted with 448-bit Blowfish encryption prior to transfer and sent through a secure 128-bit SSL tunnel to the Global Data Backup datacenter.

Encryption of data on Global Data Backup servers: All backed up data maintains the 448-bit Blowfish encryption while stored "at rest" in the Global Data Backup datacenter.

Physical security: Global Data Backup servers are located in a Tier 4 datacenter protected by gated perimeter access, 24 x 7 x365 on-site staffed security and technicians, electronic card key access, and strategically placed security cameras inside and outside the building.

Remote/offsite backup: RBS is an automated remote or offsite backup and a key component in any disaster recovery plan as protection against hardware failure, theft, virus attack, deletion, and natural disaster.

Private and public encryption keys: Users have a choice of using a RBS generated 448-bit key or managing their own private key to encrypt their data.

Logical access: Backed up data may be accessed via the password protected administrative console by supplying a valid encryption key.

Written contingency plan: The HIPAA Security rule requires that covered entities have a written contingency plan for responding to system emergencies, including a detailed plan concerning the data backup and recovery process in the event of a disaster.

Note: There is no standard "HIPAA certificate of compliance" for backup software and services. For more information about HIPAA and HIPAA compliance, contact your legal counsel or refer to the HIPAA section of the U.S. Department of Health and Human Services' website: <http://www.hhs.gov/ocr/hipaa/>