

Qbase Online Backup and Recovery

HIPAA Compliance

IT Solutions

Qbase helps healthcare providers comply with HIPAA Privacy and HIPAA Security Rules.

The Health Insurance Portability and Accountability Act (HIPAA), passed into law in August 2006, aims to enable better access to health insurance while reducing healthcare fraud and abuse. All health plans, healthcare clearing-houses and healthcare providers who store patient data electronically, must comply with HIPAA.

Encryption of data during backup

Qbase encrypts all data using 448-bit Blowfish encryption prior to transfer and then sends it through a secure 128-bit SSL tunnel to the data center.

Encryption of data on the backup servers

All backed up data maintains the 448-bit Blowfish encryption while stored at the data center.

Physical security

Qbase Online Backup and Recovery servers are located in a Tier 4 data center, protected by gated perimeter access, 24/365 on-site staffed security and technicians, electronic card key access with strategically-placed security cameras inside and outside the building.

Remote/offsite backup

Qbase Online Backup and Recovery is an automated remote backup—a key component in any disaster recovery plan, protecting against hardware failure, theft, virus attack, deletion and natural disasters.

Private and public encryption keys

Users have a choice of a Qbase-generated 448-bit key or managing their own private key to encrypt their data.

Logical access

Users can access their data using the password-protected Qbase administrative console by supplying a valid encryption key.

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 into the policies and practices of healthcare providers, plans and others involved in healthcare.

HIPAA Security Rule

Mandatory compliance April 21, 2005

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

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

1. ensure the confidentiality, integrity and availability of all electronically protected health information the covered entity creates, receives, maintains or transmits,
2. protect against any reasonably anticipated threats or hazards to the security or integrity of such information,
3. protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required, and
4. ensure compliance by the workforce.

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, www.hhs.gov/ocr/hipaa

To learn more, contact your Qbase representative, visit us online at www.qbase.us, or call 888 458 0345.