

## HIPAA COMPLIANCE

### Is Remote Backup HIPAA Compliant?

#### **The Short Answer:**

Remote Backup complies with the Final Security Rule, but please read on...

Remote Backup Software (RBS) compresses and encrypts data before it is sent to the RBS Server. The Encryption Key is known only to the customer, and is never transmitted to the Server nor to the backup service provider. Data are stored on the RBS Server in compressed and encrypted archives that are not accessible by the RBS Service Provider.

Remote Backup Software is adequate to help companies comply with the Final Security Rule. RBS also complies with the Privacy section, even though RBS Providers are not "Covered Entities" as defined by the current rules, and thus are not required to comply with it.

In addition, Remote Backup can help customers comply with other provisions of the rules as part of a larger data protection and disaster recovery plan. At the time of this writing there is no "HIPAA Compliance" certification for backup software, and it is important to note that under the current rules, no software is truly "HIPAA compliant," because there are no regulations that specifically address backup and privacy software.

#### **The Long Answer:**

In 1996, a bill known as the Kennedy-Kassebaum Bill was passed by the U.S. Congress and signed into law by President Bill Clinton. The new law was known as the Health Insurance Portability and Accountability Act of 1996, or more commonly, HIPAA. It had started as a measure to ensure that workers could keep their health insurance when they changed jobs. By the time of its passage, it had become much more complex and far-ranging, affecting the vast majority of all health-care entities in the United States.

Because of the complexity and wide range of HIPAA, there has been and continues to be a great deal of confusion about how it applies to many areas, including Remote Backup. This page will present a brief overview of HIPAA, and demonstrate how Remote Backup can be a valuable tool in meeting the requirements of HIPAA's Security Rule.

#### **Who Must Comply**

Those who must comply with HIPAA fall into two categories. The first category is Covered Entities. Covered Entities include all health plans, health care clearinghouses, or health care providers who transmit health information in electronic form.

The second category is the Business Associates of those Covered Entities. A Business Associate is someone who performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.

Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information (PHI), and where any access to protected health information by such persons would be incidental, if at all.

## **Must Remote Backup Service Providers Comply?**

Remote Backup Service Providers are clearly not Covered Entities.

Because Remote Backup Services does not involve the use or disclosure of PHI, and any access to PHI by a Remote Backup Service Provider would be incidental, if even possible, Remote Backup Service Providers are not normally considered to be Business Associates, and are therefore not covered by the HIPAA Privacy Rule. However, some Covered Entities may wish to have a Business Associate Contract in place regardless. How this is handled is up to the individual Remote Backup Service Provider.

Remote Backup Services do clearly fall within the requirements of the HIPAA Security Rule. Covered Entities must be compliant with the Security Rule by April 21, 2005. Remote Backup software and services are compliant today, and can provide a foundation for overall compliance.

## **HIPAA Overview**

**HIPAA consists of five parts:**

- **Title 1** - Health Insurance Portability - helps workers maintain insurance coverage when they change jobs
- **Title 2** - Administrative Simplification - standardizes electronic health care-related transactions, and the privacy and security of health information
- **Title 3** - Medical Savings Accounts & Health Insurance Tax Deductions
- **Title 4** - Enforcement of Group Health Plan provisions
- **Title 5** - Revenue Offset Provisions

Fortunately, four of the five parts of HIPAA have no bearing on Remote Backup. The one part that does apply is Title 2 - Administrative Simplification.

### **Administrative Simplification**

HIPAA Administrative Simplification consists of two areas. The first is commonly referred to as the Transactions and Code Sets Rule, although it also covers standardization of identifiers. This Rule requires standardization in all health-related electronic transactions, such as electronic transmission of insurance claims, verification of insurance, statements, explanations of benefits, remittance advice, etc. It is scheduled to take effect in October 2003.

Remote Backup is not a health-related transaction, and is therefore not covered under the Transactions and Code Sets Rule.

The second area of Administrative Simplification is made up of two Rules, the Privacy Rule and the Security Rule. Because these two rules are where the most confusion arises, we will examine them in some detail.

### **Privacy and Security**

Before the Privacy and Security Rules can be explained, we must understand what they are intended to protect. Both Rules are intended to safeguard any health-related information that can be traced to or used to identify an individual. Some examples of this type of information include name, address, Date of Birth, Social Security number, or any other identifier. This type of information is referred to as Protected Health Information, or PHI.

The Privacy Rule and Security Rule are intended to protect PHI in different ways. The Privacy Rule sets out limits on who can have access to PHI and for what purpose. The Security Rule regulates the Procedural, Physical and Technical means that are used to protect PHI.

## Privacy

The Privacy Rule places limits on the ways that PHI can be used and disclosed, and requires accounting of disclosures. But it is relevant at this point to review how Remote Backup works.

With a Remote Backup solution, all information to be backed up is encrypted by the local client before being transmitted, using a key that is stored locally. Data is stored on the remote server in its encrypted form. Data can only be recovered by transmitting it back to the local client, which decrypts it, again using the locally-stored key. The most important feature of this arrangement is that while the data is stored on the remote server, it is encrypted and not in a readable format. The remote server does not have access to the key, and without the key, the data cannot be converted to a readable format.

Remote Backup Services do not involve the use or disclosure of PHI. All back-up data is stored on the Remote Server in an encrypted form, and any access to PHI by a Remote Backup Service Provider would be incidental, if even possible. Remote Backup Service Providers are therefore not normally considered to be Business Associates, and are not covered by or required to be compliant with the HIPAA Administrative Simplification Privacy Rule.

## Security

The Security Rule is the one part of HIPAA that clearly applies to the type of services that Remote Backup offers. The Final Security Rule was published in February 2003, and became effective on April 21, 2003. Compliance with this Rule will be required by April 21, 2005.

The Security Rule legislates the means that should be used to protect PHI. It requires that covered entities have appropriate Administrative Procedures, Physical Safeguards, and Technical Safeguards to protect access to PHI.

### Examples of appropriate safeguards include:

- Establishment of clear Access Control policies, procedures, and technology to restrict who has authorized access to PHI.
- Establishment of restricted and locked areas where PHI is stored.
- Establishment of appropriate Data Backup, Disaster Recovery, and Emergency Mode Operation planning.
- Establishment of technical security mechanisms such as encryption to protect data that is transmitted via a network.

### Remote Backup is compliant with the Final Security Rule.

The Remote Backup client software contains all appropriate technical security mechanisms to protect the data that is transmitted to and from the Remote Backup Server.

Remote Backup can form a critical part of Data Backup, Disaster Recovery, and Emergency Mode Operations strategies by providing offsite backup that can be geographically distant from the client site to minimize the likelihood of data loss in a large-scale disaster. In the event of loss of the primary data center, data on a Remote Backup Server can easily be recovered from any replacement data center.

Covered entities will be required to comply with the HIPAA Administrative Simplification Security Rule by April 21, 2005. Remote Backup, as part of a comprehensive security plan, can be an important part of compliance strategy. *[This is what allows remote backup providers to claim their systems are "HIPAA-compliant." But one must then ask, is it proper to claim HIPAA-compliance where few or no standards exist for entities that are neither Covered Entities nor Business Associates?]*

**Resources**

The Department of Health and Human Services, Centers for Medicare and Medicaid Services HIPAA page can be found here:

<http://www.cms.hhs.gov/hipaa/>

The most recent summary of the Privacy Rule can be found here:

<http://www.hhs.gov/ocr/privacysummary.pdf>

The Final Privacy Rule can be found here:

<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/>

The Final Security Rule can be found here:

<http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf>