



The Strong Encryption technology in *BackupEDGE™* can be a critical part of a HIPAA compliance strategy.

Will *BackupEDGE* alone make you HIPAA Compliant?

The Short Answer is **NO**

No software product or technical solution will make your organization HIPAA compliant! Compliance is primarily a matter of policies and procedures, most of which are not technology based. *BackupEDGE* can, however, be an important tool in assisting you in your development of a complete compliance strategy.

Overview

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 Backup and Disaster Recovery capabilities.

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**

Four of the five parts of HIPAA have no bearing on *BackupEDGE* functionality. 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 was scheduled to take effect in October 2003.

BackupEDGE software does not create or provide health-related transactions, 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.

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 for disclosures. But it is relevant at this point to review how *BackupEDGE* works.

BackupEDGE creates archives (backup copies) of some or all of the data and files on your computer system to a variety of media types, including tape, CD, DVD and Iomega REV. It can also backup to any Network-Attached-Storage (NAS) device, server, or appliance, whether the NAS is connected via the local network, wide area network, or the Internet.

It has a license option enabling public key data encryption. You may choose to encrypt data by specifying filenames, directories or file extension types. Encryption is very powerful, using the well documented and publicly vetted AES encryption algorithm with 256 bit keys, which are further protected by RSA 2048 bit public/private encryption. Encryption is performed at the file level, providing the following benefits...

- Only data that needs to be protected is encrypted.
- Overall performance stays high during archiving as only critical files are subject to CPU intensive encryption.
- Full compatibility with verification, quick file access and disaster recovery is maintained.

Each encrypted file is pre-compressed using the powerful ZLIB algorithms to ensure that no space is lost due to the inability of tape hardware compression implementations to compress encrypted data.

Optionally, you may choose to encrypt an entire archive (except the file headers), although this is not recommended.

The methodology used by *BackupEDGE* for data encryption is published to assure customers that standards are being followed and that no “back doors” or other security holes are in place.

With a *BackupEDGE* solution, all information to be backed up can be encrypted using a key that is itself encrypted and stored locally with the data. Data can only be recovered by a master key decrypting the locally stored key, and then using the locally stored key to decrypt the data. The most important feature of this arrangement is that while the data is stored remotely it is encrypted and not in a readable format. The remote storage facility would not have access to the master key, and without the master key, the local encryption key cannot be used to convert the data to a readable format.

For additional security, backups to NAS can be done over an encrypted link, whether or not the resulting archive is itself encrypted.

For additional security, backups to the Amazon Simple Storage Service (S3) are always done over an encrypted link, whether or not the resulting archive is itself encrypted.

Using *BackupEDGE* to create archives does not involve the use or disclosure of *PHI*. As all backed-up data is stored in an encrypted form, no access to *PHI* would be possible even if the archive media were misplaced, lost or stolen.

Of course, the use of *BackupEDGE* is 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 functionality that *BackupEDGE* offers. The Final Security Rule was published in February 2003, and became effective on April 21, 2003. Compliance with this Rule was 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 restrict access to *PHI* to those with the appropriate need.

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 stored data, and data that may also be transmitted via a network.

BackupEDGE is compliant with the Final Security Rule.

The *BackupEDGE* software contains all appropriate technical security mechanisms to protect your data.

Summary

BackupEDGE can form a critical part of Data Backup, Disaster Recovery, and Emergency Mode Operations strategies by providing offsite backups 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, not just data, but the entire system can easily be recovered in an emergency replacement data center.

Covered entities are required to have complied with the HIPAA Administrative Simplification Security Rule by April 21, 2005. If this has not yet been completed, *BackupEDGE*, as part of a comprehensive security plan, can be an important part of compliance strategy.

Note: It should be noted that all copies or backups of *PHI* data that is not encrypted but is stored externally is subject to the same safeguards and requirements of the original data.