PCSI Backup HIPAA Compliance Statement

The Health Insurance Portability and Accountability Act (HIPAA) was passed in August 2006 to enable better access to health insurance, reduce health care fraud and abuse, and lower the overall cost of health care in the U.S.

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.)

PCSI Backup enables covered entities to 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.

Specific Compliance Information for rsync.net Offsite Backup

Encrypted Data Transfer

All data is encrypted on the clients computers using 256-bit AES encryption then transferred to us. Encryption keys are passwords using complex methods and are stored by the end user and, if selected, that password is sent to a secure vault at PCSI backup. This data is then transferred to a separate encrypted container at a separate location and NOT stored with any backup data.

as well as personal technical support is provided, free of charge, to aid in their integration of such encryption.

Remote and Offsite Backup of Data

PCSI Backup is a provider of automated and manual data storage and is an essential component of any disaster recovery plan. rsync.net offsite backups, configured properly, can protect against hardware failure, physical and logical theft, viruses, worms, accidental or intentional deletion and natural disasters.

Encryption Keys

Users have a number of choices in the transmission and storage encryption algorithms they may use, and may use encryption keys provided by rsync.net or implement their own keys.

Access to Data

Customer data may be accessed over the public Internet, using password-protected OR public-key-protected SSH, SFTP, HTTPS transports.

Written contingency plan

The HIPAA Security rules requires that covered entities have a written contingency plan for responding to system emergencies, and that this plan includes a detailed plan concerning data backup and recovery and related processes in the event of a disaster.

Note: There is not a standard "HIPAA certificate of compliance" for backup products and services. PCSI Backup attempts to adhere to the spirit For more information about HIPAA and HIPAA compliance, please contact your legal counsel or refer to the HIPAA section of the U.S. Department of Health and Human Services' website, which can be found at: http://www.hhs.gov/ocr/hipaa/