Security

PCRx Storage Solutions ™ encrypts data prior to transmission using a unique encryption key generated during installation of the software.

Users can opt to import and manage their own encryption key set, should they desire, but loss of a user generated key set will render the data unrestorable as there are no "master keys" or "back doors" of any kind. The encryption algorithm used by PCRx Storage Solutions ™ is extremely powerful and recovering data without the key is impossible and makes encryption key management vital to the security of your data. Our experience with data recovery has shown that users generally do a poor job managing their encryption keys. As a result, PCRx Storage Solutions ™ has implemented process control standards for securely managing the encryption key sets and does so by default. Users choosing to create and manage their own key sets must understand the importance of backing up the keys in manner that allows for retrieval under any circumstance.

Prior to transmission, data on the user's system is compressed and encrypted. During transmission, data is sent over a SSL (secure socket layer) port on your computer essentially encrypting the data twice on its way to PCRx Storage Solutions ™ 's storage servers. In comparison, the same technology used to transport critical financial data from personal computers to vendors for online transactions is far less secure since the source data (for example, your credit card number) is not itself encrypted; it is only encrypted during transmission and is decrypted when received by the vendor. With PCRx Storage Solutions ™ , the data remains encrypted on the server at all times. Restoral of archived data is equally secure; requiring multi-level authentication credentials and encryption key. PCRx Storage Solutions ™ 's architecture makes the transmission and storage of your data far more secure than the billions of dollars currently processed online in today's ecommerce environment.

In addition, PCRx Storage Solutions ™ 's software has built in security measures to ensure the integrity of your data. Simple deletion of files on the user's computer will not affect the archived data set. Malicious deletion and destruction of data is a serious threat to any business and can make recovery of the data impossible. Storing archived and primary data in one physical location puts organizations at unnecessary risk. Another unique aspect of PCRx Storage Solutions ™ 's service is Enhanced Performance Monitoring; this feature allows our engineers to determine if the backup service is configured properly and alerts the user to any exceptions we may find.

Ease of use, performance, icon overlays, stability and comprehensive email reporting, while not directly related to security, are important factors in the integrity of your backups and ultimately have an impact on the effectiveness of your organization's backup strategy. Many of these features were driven by the engineering team at PCRx Storage Solutions ™ , Inc., providing insight from data recovery cases seen on a daily basis from various aspects of failure.

Data Center

To protect your mission-critical data, PCRx Storage Solutions™ houses their servers in a SAS 70 Type II data center operated and owned by Latisys. Latisys maintains a tight multi-layered security system including electronic motion sensors, providing continuous interior and exterior observation and 30-day retained storage of video surveillance. The building's single entry point is outfitted with sophisticated security sensors, vandal-resistant and bullet-proof glass, full biometric hand scanning and CircleLock mantraps. Armed guards monitor the data center 24/7/365.

The outside of the building, or building envelope, was designed and constructed to withstand extreme temperatures, high winds, floods, fire, impact, pollution and electro-magnetic interference. Latisys uses dry-pipe, four stage VESDA® air-sampling smoke detectors, laser detection and light scattering technologies to provide the earliest possible warning of an impending fire. In the unlikely event of fire, the fire suppression system is automatically triggered to prevent damage, disruption and injury. Additionally, CleanGuard® fire extinguishers are strategically located throughout the data center.

Inside, water and moisture protection is paramount. On the roof of the data center, Latisys employs a fully adhered, rubber membrane system with isocyanurate insulation. Below grade, enclosed containment pump evacuation system controls all water runoff. To eliminate hot spots Latisys uses twenty rooftop, 135-ton, Trane compressors. They provide optimum cooling power to collocation areas, are 2N+1 capable and run with efficiency and reliability. Three 20-ton Liebert cooling loops provide focused, high-efficiency cooling to the Network Core and Power Room areas.

Facility Features and Specifications

- 56,260 sq. ft. footprint
- 30,000 sq. ft. mezzanine
- 500 lbs. per square foot ground level loading capacity
- 150 lbs. per square foot on the mezzanine
- 150+ watts per square foot
- 30-foot slab to ceiling ground floor clearance
- 17-foot clearance on the mezzanine
- Zero slab-on-grade penetration above and below
- Secure loading dock and freight elevator convenience

Uninterrupted access and premium bandwidth are provided using carrier neutral options and diverse network routes. Primary power is robust. Latisys can supply more watts per square foot than any other data center in the Midwest; with the availability of 12.5 megawatts for power-hungry applications. Redundant Uninterrupted Power Supply prevents power spikes, surges and brownouts. Equipped with N + 1 diesel generators, each with a 2,000-gallon belly tank, with enough stand-by power to stay up and running in the event of a commercial power failure.

About SAS 70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes.

There are two types of service auditor reports.

A Type I service auditor's report includes the service auditor's opinion on the fairness of the presentation of the service organization's description of controls that had been placed into operation and the functionality of the controls to achieve the specified control objectives.

A Type II service auditor's report includes the information contained in a Type I service auditor's report and also includes the service auditor's opinion on whether the specific controls were operating effectively during the period under review.

Why is SAS 70 Type II Compliancy Important to You?

In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting. The SAS 70 audit independently verifies the validity and functionality of a Data Center's control

activities and processes. These control activities and processes are important to customers within the financial, healthcare, and insurance sectors, as well as to publicly traded companies who must validate the security of their financial and sensitive information controls. A yearly audit is performed to not only verify that procedures are in place and effective, but that they are maintained.

PCRx Storage Solutions™ is able to provide customers with documentation of the SAS 70 Type II Compliancy pertaining to the data center. This not only saves valuable time and money for customers needing to meet SAS70 compliancy standards, but also in reaching PCI Compliance Standards as well.

Conclusion

Compared to tape, external hard drives and other methods of backup, PCRx Storage Solutions™'s architecture provides a much more secure environment for your data. Architecture built by insight gained from thousands of data recovery cases, coupled with best practices, internal process controls and professional managed infrastructure ensures the security of your data.