The data capacity and retention need of medical organizations continues to grow at a rapid pace. High resolution C-T (CAT), PET, and MRI scans, as well as ultrasound; x-ray imaging and high definition videos, require enormous amounts of storage as well as redundancy. Add to that, electronic medical records, documentation, financial records, insurance information, and more; and it quickly becomes evident just how much reliable, and expandable digital storage is needed in the modern healthcare office.

Title II of the Health Insurance Portability and Accountability Act (HIPAA) defines policies, procedures and guidelines for maintaining the privacy and security of health records as well as defining numerous consequences for abuses of the guidelines. HIPAA strives to prevent misuse of client data within the health care system with procedures and recommendations for privacy, administrative simplification, health care transactions and enforcement of these policies. HIPAA rules apply to health care providers, billing services, health plans, and other entities that transmit or store health care records.

The HIPAA Security Rule, which defines the administrative, physical and technical requirements for data access, storage and transmission can be, addressed both by the ioSafe NAS hardware and the included Disk Station Manager software features.

ioSafe Network Attached Storage (NAS) provides a secure, reliable, and affordable backup and file sharing solution for doctor’s offices, medical clinics, hospitals, and other medical organizations. Powered by the intuitive and feature-rich Synology® Disk Station Manager (DSM), the ioSafe NAS solutions offer administrators a storage solution, which meets HIPAA guidelines, with additional protection from disaster such as fire, flooding and theft.
HIPAA Safeguards with ioSafe NAS

Administrative Safeguards

*Windows Access Control Lists*
Windows ACL supports granular file control to give permissions to specific files or folders, which ensures flexibility and a high level of security at the same time. With native Windows ACL support, user permissions can be managed directly on the DSM interface.

*File Access Logging*
Medical personnel may collaborate on the same healthcare information, so administrators might need to monitor their behavior. With Windows File Access Logging, users’ behaviors such as who edits, deletes, moves, reads, writes which file at what time can be recorded.

*Windows AD and LDAP*
For hospitals that have established domain user accounts through Windows Active Directory (AD) or LDAP, there is no need to maintain two sets of credentials - ioSafe NAS can act as a LDAP and AD client to integrate with hospitals’ existing account system seamlessly.

Physical Safeguards

*Add extra protection with data lockdown*
The ioSafe floor-mount kits enables physical protection by bolting down the ioSafe units to any surface and be secured with a cable and padlock. The steel cage, which surrounds the ioSafe NAS unit, prevents access to the hard drives and networking ports, as well as the physical removal of the NAS unit. In addition to theft and tampering protection, securing the drive also prevents it from moving during a disaster.

Technical Safeguards

*Network Security*
Whether data is being accessed locally or remotely, patient privacy is maintained. Encryption is available in transmission both locally and over the WAN, as well as when the data is held on disk.

*SMB3 and Secure FTP*
SMB3 provides modern shared folder access, adding AES-based end-to-end encryption for local shared folder access on Windows, Mac, and Linux servers and workstations. For large file transfers, FTPS or SFTP, enable your organization with modern FTP standards that maintain HIPAA compliance with either SSL/TLS or SSH encryption.

© 2015 ioSafe Inc.
**Compliant Backup of Sensitive Information**

Whether you need to back up a server or a fleet of workstations, an ioSafe NAS can take advantage of encrypted backup transmission over rsync using SSH, SMB3, or a secure FTP connection. Additionally, backups to cloud services like Amazon Glacier are secured using SSL.

**Keeps Unwanted Connections Out**

A robust firewall is included in the DSM to control access to services over physical ports, or logical network ports. Geo-location filtering is also available to confine any external requests to specific geographic locations.

**256-bit AES encryption**

Data stored on an ioSafe NAS is safe with 256-bit AES encryption, since it can only be decrypted with the same key that was used to encrypt the data. Hence, hospitals don’t need to worry about sensitive healthcare information leaked when their NAS or disks fall into wrong hands.

**Hardware encryption engine**

With hardware encryption engine, the ioSafe 1515+ NAS can offload encryption calculation tasks away from the main CPU, so data transmission speed of the encrypted files will not be affected and the processing power is freed up for other important tasks.

**SSL/TLS encryption**

Healthcare information can be protected with SSL encryption during data transmission. If anyone tries eavesdropping on the hospital network, they will receive only scrambled, encrypted data.

**ioSafe NAS ensures business continuity in the event of a hardware failure**

With Synology High Availability (SHA) technology, hospitals can reduce service downtime by mirroring the data on the active ioSafe NAS to the passive ioSafe NAS, and having the active server automatically failover to the passive server when the former one goes offline.

**RAID protection prevent data loss**

With RAID technology, data is distributed across hard drives to ensure data redundancy and performance improvement, allowing files to remain accessible even when one hard drive fails. Synology Hybrid RAID (SHR) is the RAID technology developed by Synology, designed to make storage volume deployment easier and more flexible.

**Hot spares enhance data availability**

ioSafe 1515+ NAS servers support hot spare drives, allowing standby hard drives to repair a degraded volume/Disk Group/iSCSI LUN by automatically replacing a failed drive.
ioSafe Offers The Most Unique Disaster Recovery Protection In The Industry

*DataCast Fire Protection: Protects data from loss up to 1550°F for 1/2 hour per ASTM E119*

ioSafe’s DataCast endothermic fire insulation technology protects data from extreme heat. The DataCast formulation forms a chemical bond with water molecules that, at temperatures above 160°F, releases water vapor to limit the internal temperature of the NAS during a fire.

*HydroSafe Water Protection: Protects data from loss up to 10 feet for 72 hours*

ioSafe’s HydroSafe water barrier technology is designed to protect data loss from fresh or saltwater damage, including full immersion. HydroSafe technology keeps hard drives dry and secure in the event of a flood, storm or other natural or man-made disaster, while still allowing heat dissipation during normal operation.

*FloSafe Vents: Engineered to keep cool, data secure*

ioSafe’s engineered vents are specifically sized to provide sufficient cooling during normal operation. A labyrinth design prohibits radiant fire energy from reaching the internal drive with a direct line of sight. During a fire, steam from the DataCast is forced out the vents to effectively block all damaging heat, as the net flow of gas is always outward. Elegant and reliable, protection is accomplished with no moving parts, actuators or electrical power.

The ioSafe Solution

With the most robust disaster recovery in the storage industry, ioSafe NAS allows administrators to instantly create storage that assists with meeting HIPAA guidelines for any health care organization with many safeguards to keep data secure, accessible and protected from loss. With protection from fire, flooding and theft, ioSafe NAS offers the fastest onsite data recovery available all while keeping the data on premise. You maintain 100% control over the data’s location, access, encryption and firewall settings.

ioSafe technology can help improve data storage environments where security, risk, vulnerability, business continuity and disaster preparedness play a role in achieving compliance. Compliance is complicated and electronic data storage is just one aspect. ioSafe represents a very pragmatic solution to both improving security and disaster recovery for vulnerable data all included in a single product.

© 2015 ioSafe Inc.