SDFI File Portal Security

SDFI®-TeleMedicine is "Secure Beyond Reasonable Doubt®!

Your SDFI data is safe within SDFI's File Portal. As part of the SDFI Standard Operating Procedure, your SDFI Secure Case Files are separately "pre-encrypted" at AES 256-bit before leaving your desk and before being transferred to and through a SSL certificate signature algorithm set at PKCS #1 SHA-256 with RSA encryption.

SDFI Secure Case Files are at temporally at rest within the SDFI File Portal for a maximum of 7 days, then they are eradicated from the File Portal. While SDFI Secure Case Files do rest temporarily inside the SDFI File Portal, they reside on Isilon proprietary storage clusters. Each Isilon drive is a self-encrypting device that uses separate AES-256 ciphers. Isilon encryption of data at rest satisfies a number of industries' regulatory compliance requirements including U.S. Federal FIPS 104-2 Level 2 protection.

Advanced File Portal user provisioning and permissions are used to manage each user account. Password lifecycles and Username length and strength requirements are used with secured administrative auditing and reporting tools.

The SDFI File Portal system resides in a SOC3 Certified Data Center and is McAfee Secure Tested. We have employed an extensive level of security safeguards, practices and standards, to ensure the safety of your independently encrypted data.

SDFI utilizes a set of Tier 1 redundant backbone connections for high performance connectivity for high performance routing. Our SOC-3 compliant facility offers redundancy in power, HVAC, fire suppression, network connectivity, and security. All servers, devices, network connections and critical services are monitored 24x7x365. In addition to automated monitoring, our entire infrastructure team works directly onsite at our data center so we can respond to physical incidents or equipment upgrades as quickly as needed.

Drive redundancy and fault tolerance is also important. N+3 data storage redundancy is in place to prevent single point failure. Rack mount hard drive arrays running RAID 5 under RAID 50 provide continuous hot-swap disk redundancy and multiple layers of power redundancy prevent all forms of power loss.

Intrusion Detection and Prevention: Advanced multi-tiered security protocols are working together in layers to protect the network at all times. Firewalls monitor each firebox firewall appliance. Security monitoring software running on server equipment includes intrusion detection, virus scanning, system logs and the provide notifications of suspicious activity in real-time.

Compliances include: HIPAA, GLBA, SOX, SSAE16, PCI and ISO27002.

Please send technical questions to:

SDFI-TeleMedicine
ATTN: Technical Support
E-Mail: Support@SDFI.com
Phone: 310-492-5372