iDocsNOW: Data security and compliance statement.

The security and privacy of data is a core part of our business and is our top priority. This document outlines our corporate statement regarding our data security program and the process we follow to ensure information security and compliance.

The iDocsNOW document management system helps customers comply with the network perimeter security and data retention criteria mandated in such regulations as the Health Insurance Portability & Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Federal Information Processing Standardization (FIPS), and the Government Information Security Reform Act (GISRA).

Encryption

Data Transfer: iDocsnow uses Secure-Socket Layer (SSL) v3(TLS) technology for mutual authentication, data encryption and data integrity. That includes the iDocsNOW Print Driver, Web Scan and Import processes. SSL is the industry standard security protocol for encoding sensitive information. SSL creates a shared digital key, which lets only the sender and the receiver of the transmission scramble or unscramble information.

Data Storage: To ensure data security, iDocsNOW stores all customer data AES 256 Block CBC encrypted, which meets FIPS 197 standards. This includes tape backups and CDs sent to customer locations. All files have unique keys known only to the customer. iDocsNOW staff does not have access to the unencrypted data.

Physical Redundancy

Customer data is backed up in real-time to two different servers located in separate data centers (Tampa, FL and Atlanta, GA). Both data centers house redundant web and database servers — fully configured with all software and data — so that in the unlikely event of a failure of any of the data centers, the backup data center will be available.

Off-Site Backups

All encrypted customer data is also backed up on tapes at our secure off-site locations nightly. The backup storage location is highly secure and includes alarms, controlled access and fire suppressors — everything necessary to ensure valuable customer data is always secure.

Access and Event Monitoring

iDocsNOW maintains and regularly reviews a real-time and long-term event and login access monitoring system to adhere to demands of regulatory compliance requirements like HIPAA and SOX.

Passwords

Passwords are stored SHA double hashed and the length and complexity can be pre-determined by your staff.

Physical Security

Our data centers are managed by iDocsNOW employees, ensuring that no outside parties gain access. The exact locations of the data centers were chosen to protect against catastrophic events and are confidential and undisclosed to protect against user data being targeted. These facilities are guarded 24 hours a day.

In addition, strong methods of entry protection such as biometric devices and secure token cards are used to ensure that only authorized personnel can gain access. Only select iDocsNOW employees have access to the data center facilities

and the servers contained therein and this access is tightly controlled and audited. All data centers are also CCITV monitored with one year of recording backup.

Data Security Compliance Statement

Our products and services meet the physical and technical standards and provide all necessary controls for our customers to maintain their administrative security compliance standards.

Specifically, iDocsNOW agrees to: implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic information that it creates, receives, maintains or transmits on behalf of our customers.

iDocsNOW has implemented reasonable and appropriate safeguards to protect our customers' business information. Furthermore, we agree to report to our customers any security incident of which it becomes aware, and will authorize the termination of any customer contract in the case of any material breach of this compliance statement.

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium. The CISSP is based on the three tenants of confidentiality, integrity and availability. These are balanced across ten domains: Access Control; Applications Security; Business Continuity & Disaster Recovery; Cryptography; Information Security & Risk Management; Legal, Regulations, Compliance and Investigations; Operations Security; Physical (Environmental) Security; Security Architecture & Design; Telecommunications & Network Security.

iDocsNOW