Information Security Overview

To maintain the highest standards of confidentiality and security in your document management process, MCS can provide written documentation outlining our Data Security Policy for the following:

1. HIPAA/HiTech compliance
2. Access to data 24/7 with no additional licensing fees
3. Unique access account identifier or user ID with associated password
4. Encryption software to protect personal health information (PHI) or personally identifiable information (PII), both at rest (inside the database) and in transit (while downloading and uploading from online portal, MCSDirect)
5. Firewall configuration
6. Anti-virus protection
7. Daily back-up policy
8. Employee security training program
9. Business Continuity Plan for corporate and hub offices
10. Intrusion Detection System (IDS)
11. Server Hardening practices
12. Server/Workstation Patching methodology
13. Security incident reporting (in case of a breach)
14. Proof of recent security audit conducted by a 3rd party
15. Physical Security standards followed, such as SOC II/SAS70 or ISO27001
16. Outline of security levels of physical site(s) providing service

Physical Security

MCS takes the security of your records very seriously and is continuing to increase security measures to further protect your information. Our data center is located at a colocation facility in Philadelphia, PA, and has the following features to keep your data safe:

Power Systems

- Dual commercial power feeds
- N+1 redundant electrical design and distribution
- Automatic switching from primary to backup power supply
- Completely isolated ground system
- Fully redundant uninterruptable power supplies (UPS)
- Diesel generator backup
- Onsite fuel tank

Safety and Security

- Monitoring 24 hours a day, 7 days a week, 365 days a year
- Access restricted to authorized client personnel and employees
- Axis IP-based interior and exterior surveillance cameras
- Entrance and exit controlled by HID contact-less access cards and biometrics
- Cabinet access controlled by a dial system
- Silent alarm & fire detection with automatic notification

Environmental Controls

- CRAC units serviced by a 12-inch distribution loop (850 tons of cooling)
- Twelve 20-ton Glycol CRAC units
- 47% +/- 10% humidity control system HVAC units
- All units are N+1 configuration
- Glycol loop is driven by two redundant 2,240 GPM pumps
- All MEP systems are monitored by Site Scan critical facility monitoring system

Fire Supression

- Clean agent FM 200 multi-zone fire protection system
- Multi-zoned, dry-pipe, dual interlocked pre-action fire protection system
- Below floor water detection system

Cabling

- Power cabling under raised flooring
- Structural capacity of raised floor is 1200 lbs/sq ft of concentrated load
- Network cabling in overhead cable trays

Application Security

The MCSDirect online record retrieval portal was created to provide clients with 24/7 secure access to their documents. The site itself is SSL secured with redundancies at the web server and database level to create a secure environment. MCSDirect has multiple layers of security that can be customized to the client's needs. The application does not define groups specifically, but each user has a given set of attributes that include:

- Cases they have access to
- Files they have access to
- Rights to perform activity on the system, including:
    - Ordering
    - Viewing status

- Viewing records
- Adding on to existing requests
- Downloading of records
- Sharing of Records

MCSDirect also has an administrative function that allows the administrator to view audit logs for users who they are administrators of. Each page the user visits is logged to our auditing system, along with the browser version, IP Address, date, time and username.

Secure Communications

When records are uploaded from MCS to the MCSDirect site, a notification is sent to the requesting party with an encrypted link to the records. This link expires after a certain period and will no longer work. After clicking the link to the records, the system will prompt them for their password to make sure that the email has not been forwarded accidentally to someone who can then open the records.