

FIRST STEP RECOVERY & WELLNESS

HIPAA Security Guidelines & Procedures

Executive Summary

The Security Rule:

The Health Insurance Portability and Accountability Act, HIPAA, contains a supplementary provision governing the creation, storage, transfer, deletion, and control of access to any client personal health information, PHI, existing in electronic format. This includes but is not limited to personal computers, network servers, access terminals, laptop computers, PDAs, so called flash or pen drives, floppy disks, CDROMs or DVDs. The HIPAA Security Rule, includes numerous issues and security risks that an entity must address and document how they are going to provide quantifiable solutions in the protection, validity and recovery of this form of PHI.

Part of the rule addresses the physical storage of the data, its recovery after a disaster or fire, who has access to the material, and how they have access.

The second part of the rule covers the transmission of that data electronically to other providers, insurance companies, clearing houses, branch offices, remote access from home, or the removal of the data from the workplace on an electronic device or media.

The only exclusion to this rule, was by necessity, Facsimile Transmissions (Fax) over conventional phone lines, as there currently is no effective way to apply a standard encryption methodology to this type of communication service. It was felt that it would cause an undo burden at present and negatively impact client treatment and care to try and include this specific class of devices within the rules governance.

Noncompliance can result in a fine of up to \$250,000 and ten years imprisonment for deliberate PHI disclosure for monetary or personal gain. There is also, by statute, potential exposure both corporate and individual to lawsuits, and local criminal court action.

There are basically three areas that require focused review of Electronic PHI:, Administrative, Physical and Technical.

ADMINISTRATIVE

1. A FSI HIPAA Security Officer must be appointed with independent authority to create, implement and enforce appropriate security procedures and structure. This duty is assigned to the FSI, Manager of Information Technology. *Currently Stephen Kroll.*

2. Standard industry Security procedures and methodology must be put in place to control the access to the information, with reasonable certainty that only those employees have a need to PHI can electronically access the information: *All FSI staff are required to read and sign a Form 336 before they are assigned an account on the FSI computer network. The form details the expectations & guidelines for use of FSI computers, the transfer of PHI to electronic media, and email accounts.*
3. Control and access to information on the system is managed using the Windows 2000 Server Authentication services for client logons, with appropriate rights assigned by the System administrator. Users are assigned a “logon” account and initial password, which can be used at any FSI PC to connect to the network and patient records. Logon attempts are limited to three invalid attempts, before the account will be locked-out. Only the Systems Administrator can unlock the account. Password changes are required every sixty days.
4. Our centralized server systems performs audits (monitors) all logon activities to the system, for aid in detecting any attempts at un-authorized access. Activity logs on all relevant computers, servers and network activity are constantly monitored and recorded. The Systems Administrator reviews these logs weekly to ensure system security and validity.
5. Patient records and PHI are backed up using a double prong approach. At our Greentree location, a magnetic tape has all of our electronic patient data and PHI information transferred to it once weekly. This tape is taken off-site as a key element in possible disaster recovery. Daily backups are made to a separate external hard-drive connected to the server to give us two local copies of the data. Additionally FSI has a second active server located at our Plaza site. An exact duplicate of the information is stored and actively synchronized to the main server at Plaza. These two servers are connected using a secured DES encrypted Virtual Private Network, VPN, using the internet as a connection link. Our local phone service provides our internet access. Both sites sit behind proven Cisco Firewalls, to hinder any remote access to the information from outside sources or hackers. Remote connection can only be accomplished using Cisco’s proprietary client software, which requires the user to have two separate codes to activate the connection.
6. Emergency operations simply require moving critical users or staff to the alternate site on a temporary basis until disaster recovery can be completed.
7. The main site, is protected by a physical alarm system, which monitors both the front and rear access doors to the site. If the alarm is activated, it remotely calls a 24-hour service which will alert the local Gateway Mall Security Officers that they need to investigate. Lincoln police are also dispatched if a suspected break-in is verified. Mall personnel, both cleaning and maintenance have been given an access code to disable the alarm upon entry to perform their required tasks. Our building’s Heating and Cooling System is located within our suite. FSI assumes any risk this might pose to incidental exposure to PHI.

8. All hardware and software installations are only performed by the IT staff after approval from the FSI Business Manager & Manager of IT Services. FSI staff is informed that they are not allowed to download and install any software on the computer network or PCs. Only the IT staff have required administrative privileges assigned to them.
9. An inventory of the hardware and software is kept by the IT department.
10. The It department monitors and deletes all user accounts, access keys to the Greentree site, and overall security adherence. The Plaza location is monitored by the Plaza Office Manager in coordination with the Manager of IT.
11. The network server and individual PCs have antivirus software installed and functioning, anti-spyware software is also active. All appropriate Microsoft Security Patches are installed on the network and PCs on a regular cycle.
12. Ongoing training is provided to the FSI staff covering security requirements and prudent computer usage for both password usage and Internet activity. Reminders are sent out in company wide emails, and specific “classroom” sessions are provided. Updates are also given at routine company activities, such as group luncheons.
13. Security agreements are collected and signed by all subcontractors, consultants, and business partners that might need or come into contact with client PHI. All data transmitted to these subcontractors is properly encrypted and formatted to meet all HIPAA and Federal Requirements.

PHYSICAL

1. Physical access restriction to both the Greentree and Plaza sites is in place for the buildings, after normal business hours. Outside doors are locked at both sites after approximately 11:00 P.M. on weekdays. Weekends vary per site. Both FSI offices have locked main access doors to our suites in the buildings. A restricted, “do not duplicate” key system is in place for the locksets on the doors. Staff are checked out restricted keys.
2. All individual offices and receptionist areas, have entry doors with keyed locksets. The storage rooms for the paper files also have doors with locksets at any entry point. The file storage rooms, at both sites, have doors at the entrances with locksets. The workroom area at Greentree has automatic door closures and signage posted on the doors advising that this is a secure, staff only area. The server room has a door and lockset with a restricted key, and automatic door closer. Additionally the lockset on this particular door, is designed to always remain locked.

3. Staff are required to lock their areas when leaving the room un-attended, if either paper PHI or computer equipment is contained within that area.
4. Proper, emergency lighting and signage is installed and inspected by the State Fire Marshal yearly. Fire escape routes are posted throughout both sites as required by state and federal regulations. Periodic testing of the building wide fire alarm system is performed at the Greentree site. Both facilities have a fully “sprinkler” fire suppression system installed.
5. Computer users are required to “lock” their computers if leaving the immediate area of their computer into the “screen saver mode.” A valid user logon must be used to regain access to the unit. Additionally, all PCs will automatically activate their “screensavers” after five minutes of inactivity by the user. Users are also required to log off of their computers when leaving the workplace.
6. Workstations are only placed in areas where they can have restricted access maintained by closing and locking of doors, to prevent unwanted client or intruder access. After hours all doors are shut and locked, requiring physical breakage of the barriers to gain access.

TECHNICAL:

1. All FSI users are given an email account on the system. Instruction and warnings are given employees as to the proper use and procedures of using the FSI email system. No client PHI is to ever be directly attached to an outgoing (external email) unless it is placed in a password protected or encrypted attached file.
2. Incoming email, containing PHI must be processed properly to ensure confidentiality. The staff will either transfer the PHI to a clients record folder on the network, transfer the email directly, or print the email to be placed into the client’s “file.”. The original email should then be deleted as soon as reasonably possible.
3. Data stored on floppy drives, or flash drives must have the file password protected. Permission to take the information off site must be granted by the employee’s direct supervisor and the Manager of IT.
4. All backup data leaving the site, must be transported in a locked container, then stored in a restricted, locked storage space off-site. Yearly CDROM backups of our client data are made and stored off-site as a validation/disaster recovery procedure.
5. Transcriptions being sent electronically or physically delivered to FSI will be saved in a password protected file, or encrypted.

6. All counselors and staff are required to have full access to the client records stored on the FSI network system. This precludes restricting access based on a role model. Validation of the integrity of the data stored is possible through the daily backups, weekly tapes, and yearly backups.
7. All users are required to logoff their PCs, at the end of their work shift, or when leaving their assigned work area for an extended time. Servers are rebooted weekly to assure accounts are cleared and reset.
8. The Manager of IT provides event collection and reporting for FSI management and supervisors. Incidental violations or major issues are documented and stored for recovery. Copies of the write-up are distributed to appropriate staff.

VIOLATION PROCEDURE AND CONSEQUENCE.

Specific consequences are assigned and documented for the control and management of HIPAA Compliance and Security procedures.

- A first minor violation will result in a warning and documentation of the event by the Manager of IT Services.
- A second minor violation will escalate the situation to involve the employee's supervisor & Manager of IT Services.
- A third minor violation will result in a consult with the Clinical Director of First Step and Business manager possibly leading to termination.
- All serious violations may or must result in immediate termination.