FAMILY SERVICE ROCHESTER

DATA SECURITY POLICY

SUBJECT:	EFFECTIVE DATE:	POLICY ID :
DATA SECURITY	Last Revised May 2017	

POLICY

Family Service Rochester ("FSR") is dedicated to the security of "personally identifiable information" or "PII" and "protected health information" or "PHI" maintained or transmitted by FSR in electronic form. As such, FSR has implemented administrative, physical, and technical safeguards to protect the security of PII and PHI. FSR Board, management, employees, contractors, and volunteers ("Workforce") are expected to comply with this policy for the protection of PII and PHI.

PROCEDURE

I. Identification and Criticality of Information Systems

FSR maintains the majority of its electronic PII and PHI within Its Electronic Health Record ("EHR"), a remotely hosted program that contains all medical record documentation and billing information for services performed by FSR. PII and PHI may also be maintained within other remotely hosted systems, on FSR's internal servers ("IT Systems"), or on the information systems of other agencies or entities with whom FSR has a contractual relationship.

FSR, in coordination with its IT Vendor, maintains an inventory of all information technology assets containing or accessing electronic PII or PHI. This inventory is updated periodically by FSR or the IT Vendor as changes are made.

The sensitivity of PII and PHI maintained in each FSR system as well as the criticality of the system to FSR operations is incorporated into this inventory process. The criticality of systems is utilized by FSR to appropriately utilize resources, prioritize risk management efforts, effectively plan back up and disaster recovery processes and implement other safeguards discussed in this Data Security Policy.

II. Oversight and Workforce Expectations

The Privacy Officer is responsible for oversight of the Data Security Policy and functions related to the security of FSR's data as described in this policy. The full expectations of the Privacy Officer are included in Attachment A to the Data Privacy Policy.

This Data Security Policy is supplemental to the Data Privacy policy to address the specific expectations of FSR related to PII and PHI maintained in electronic form. As such, all expectations of the Data Privacy Policy also apply to PII and PHI in electronic form. Any violation of this Data Security Policy may subject a Workforce Member to corrective action as described in the Data Privacy Policy and Employee Handbook.

III. Risk Assessment and Risk Management

FSR conducts a periodic risk assessment to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PII and PHI it holds. The risk assessment may be performed internally or utilizing third party resources. It will be performed as determined to be appropriate by the Privacy Officer.

While the process for each risk assessment may vary depending on the scope of the assessment, the person performing the assessment, and the ultimate goal of the assessment, each assessment will include documentation:

- Identifying the scope of the assessment;
- Summarizing data gathered and reviewed;
- Identifying and documenting potential threats and vulnerabilities;
- Assessing current security measures;
- Determining the likelihood of a threat occurrence;
- Determining the potential impact of a threat occurrence;
- Determining the level of risk; and
- Identifying potential security measures to address the risk.

In response to each risk assessment, FSR will complete a risk management process to ensure that identified risks are mitigated to the extent reasonable and appropriate to comply with HIPAA and MGDPA.

After consideration of the risks, options available, and input of affected Workforce Members, the Privacy Officer will determine how to best mitigate risks. In determining the appropriate measures to implement, FSR will consider:

- Its size, complexity, and capabilities;
- Its technical infrastructure, hardware, and software security capabilities;
- The cost of the security measure; and
- The probability and criticality of the potential risks to PII or PHI.

Once appropriate security measures are identified and decided upon, the Privacy Officer will oversee the implementation of the security measures. Following implementation of new security measures, the process may be re-evaluated to determine whether the selected security measure resulted in the desired effect.

Documentation of each risk assessment and the security measures implemented in response to identified risks will be documented. Documentation will be maintained by the Privacy Officer for a minimum of six years.

IV. Information System Monitoring

In order to ensure that the measures implemented by FSR are sufficient to protect the electronic PII and PHI, FSR has also implemented a monitoring system. This monitoring system includes periodic review of log-on attempts, audit logs, access reports, security incidents, and other system activity. Reporting and logs available vary between software programs.

Frequency of review for each audit report or log may vary depending on the nature of the PII or PHI stored in the system, the level of restriction or control available in the program, the vulnerability to unauthorized use, and the ease of access to the audit log. Monitoring may be performed by FSR or its IT Vendor. For remotely hosted programs, the applicable vendor is responsible for monitoring of system activity consistent with contractual terms. Documentation of all monitoring activities will be maintained and any potential Incidents will be reported to the Privacy Officer.

V. Reporting Obligations

In addition to routine monitoring of IT Systems by FSR and the IT Vendor, all Workforce Members are expected to remain vigilant regarding performance of IT Systems and other software programs. Any abnormal performance or potential security issues should be immediately reported to the Privacy Officer. Any security incidents identified in this Data Security Policy will be investigated and resolved as described in the Identification, Investigation, and Resolution of Potential Incidents section of the Data Privacy policy.

VI. Workforce Security and Access Controls

FSR allows each Workforce Member to access only the level of electronic PII or PHI appropriate for that individual's needs to complete job responsibilities. The programs and drives available can be adjusted by user log-in or by workstation. Access to additional software programs containing electronic PII or PHI are only granted to Workforce Members who need access to the software for performance of job duties and access to data or functionality within each software program may also be adjusted.

All authorities to access IT Systems and PII or PHI are granted based on the Workforce Member's job responsibilities and the Program with which the Workforce Member provides services. The Privacy Officer, in coordination with the Workforce Member's supervisor determines the appropriate level of access to be granted to an individual, including, but not limited to the extent to which the Workforce Member is permitted:

- Physical access to the FSR office space after hours
- Assignment to a workstation and access to specific software programs
- Access to FSR IT Systems and specific drives within the system

- Access to The EHR and/or other software programs containing PII or PHI
- Remote access and use of personal devices
- Access to databases maintained by other agencies, such as SSIS or FIS

A. Workforce Clearance

Prior to hire, FSR screens all Workforce Members to minimize the risk of non-compliance. Background checks are performed through Safescreeners or Netstudy 2.0, depending on whether the Workforce Member has direct client contact. Additional DMV record check and OIG excluded individual database check may be performed.

B. Unique User Identification

Each individual granted access to the IT system and software programs storing PII or PHI is provided a unique user identification and password. FSR does not utilize any shared user names to access PII or PHI. Workforce Members are prohibited from sharing passwords or accessing PII or PHI through another Workforce Member's user name. All creation of and changes to PII or PHI within the FSR software programs is recorded with the user name of the person performing the action.

C. Person or Entity Authentication

An individual is only permitted to access the PII or PHI maintained by FSR through the entry of a password. The system will not permit access where the correct password is not entered.

D. Access Authorization

Upon hire, the Privacy Officer will coordinate with the IT Vendor to establish a user name and password for the Workforce Member to access the IT Systems and appropriate software programs. Each Workforce Member is provided a unique username and each username is assigned authorities as determined by the Privacy Officer and Workforce Member's supervisor, consistent with this Section IV. When a key or laptop will be assigned to the Workforce Member, the Privacy Officer or designee will check out such equipment to the Workforce Member. Remote access authorities, if granted, will be established by the IT Vendor.

Software programs track access and changes to PII and PHI based on the username accessing the information. Logs and reports are created to track this information within the system, recording the username, date, and time of each access or change. To ensure that the username recorded by the program accurately reflects the individual accessing or changing the information, Workforce Members are prohibited from sharing usernames and passwords or from utilizing another Workforce Member's username and password.

E. Access Establishment and Modification

If a Workforce Member is reassigned, the Privacy Officer will modify authorities to access PII and PHI within the software programs as appropriate based on the Workforce Member's new

role. If the change requires modification to programs or other information available at the network level, the IT Vendor will be notified of the change so that user settings may be modified accordingly. The IT Vendor and Privacy Officer may periodically review each category of access to IT Systems and PII or PHI to ensure all authorities are appropriate.

F. Termination Procedures

Upon termination of employment, FSR terminates all access to PII and PHI. Workforce Members are required to return all keys, laptops and other FSR equipment prior to completion of their final day of work. The terminating Workforce Member's user name and passwords will be deactivated to prevent further access to FSR IT Systems. FSR will notify any outside agencies to which the Workforce Member has been provided a user identification that the agency should deactivate the access.

G. Security Awareness and Training

FSR trains and educates its Workforce Members regarding its security practices as a part of its comprehensive training program, described in the Data Privacy Policy. In addition to the formal training program, FSR may provide security reminders to its Workforce Members to maintain awareness of data security requirements and the expectations of the Workforce Members related to those requirements. These updates are typically provided as a part of periodic meetings with the staff, e-mail reminders, or other memos from the Privacy Officer. Copies of all security reminders will be maintained by the Privacy Officer.

H. Emergency Access Procedure

The Privacy Officer and the IT Vendor have administrative access to all FSR databases to be able to perform maintenance, monitor tasks and to access information as needed in the event of an emergency. The Privacy Officer or IT Vendor may grant access to third parties as necessary to maintain operation of IT Systems and perform functions under this Policy.

I. Automatic Logoff

Workforce Members should log out of programs containing PII or PHI and the network whenever leaving their computer for an extended amount of time. Workforce Members must log out of The EHR prior to leaving a workstation unattended with an individual.

To assure that access to PII or PHI is not left unprotected, each workstation will go into a screensaver lock after a period of inactivity as determined appropriate by the Privacy Officer. A password must then be re-entered to access the PII or PHI. Automatic log off times may be adjusted for specific programs or workstations at the discretion of the Privacy Officer.

J. Log-In Monitoring

The security of FSR's electronic PII and PHI is dependent on the effectiveness of the limitation of access to FSR's systems containing this information. This is accomplished through control of the use of each username and password to access the system. Workforce Members are prohibited

from logging in under another Workforce Member's username or permitting the other Workforce Member to log-in under their user name.

Log-in audit trails may be reviewed by the Privacy Officer or designee as part of the monitoring policy. For additional security, the IT Systems and software programs have been set up to automatically lock a user out after a number of failed log-on attempts. Once an account is locked, the Workforce Member must contact the Privacy Officer to reestablish the user name and applicable access.

VII. Computer Usage Generally

This Section V is intended to supplement computer usage policies contained within the FSR Employee Handbook and provide additional requirements and expectations related to IT Systems that access or maintain electronic PII or PHI.

FSR computers are to be used for FSR business only. Because of the business implications and potential for misunderstandings as to Workforce Member conduct, FSR computers are not to be used for personal use unless permission is granted in writing by the Privacy Officer. This includes, but is not limited to, internet access, computer games, documents and/or personal e-mail. This policy applies to all hours, regardless of whether the Workforce Member is on duty. Non-work-related programs should never be downloaded to a FSR computer. Even if personal use is permitted in writing, it should be infrequent, of short duration, and may not interfere with work duties.

Workforce Members granted access to FSR IT Systems and partner agency systems containing PII or PHI are granted such access solely for the purpose of performing job duties for FSR. Workforce Members are strictly prohibited from accessing any PII or PHI within FSR's IT Systems or partner agency systems for any purpose unrelated to FSR job duties. Accessing PII or PHI for a purpose unrelated to job duties may result in corrective action, up to and including termination of the Workforce Member.

FSR computers, e-mail, internet, or voicemail may not be used for any purpose which is illegal, against FSR policy, or contrary to FSR's best interests. No solicitation of non-FSR business, or any use of FSR provided computers, voicemail, e-mail or internet for personal amusement or gain, is allowed.

Each Workforce Member is responsible for the content of all text, audio or images that the Workforce Member places or sends over FSR's computers, voicemail, e-mail or the internet. Unless specifically authorized by the Privacy Officer, no voicemail, e-mail or other electronic communications may be sent which hide the identity of the sender or represent the sender as someone else or someone from another organization. All messages communicated on FSR's voicemail, e-mail/internet system should contain the Workforce Member's name.

A. Viruses and Other Malware

FSR protects FSR's PII and PHI through utilization of anti-virus and anti-malware software programs on the computers FSR uses. The IT Vendor has implemented web filtering to limit the internet websites available to staff to those appropriate for work-related functions.

To prevent computer viruses from being transmitted through FSR's e-mail/internet system, do not download any software without permission. All software and files downloaded, e-mailed or obtained from outside sources on any media must be scanned for viruses before using or placing on FSR's systems. All software must be registered, showing FSR as a user. Workforce Members are expected to use caution when opening e-mail attachments and performing web searches on behalf of FSR.

In the event a Workforce Member believes that the Workforce Member's computer may be infected or at risk to malicious software, the Workforce Member must immediately notify the Privacy Officer.

B. No Expectation of Privacy

To maintain efficient operation of FSR's computer systems and ensure compliance with policy, FSR has the right to monitor all computers, voicemail, e-mail/internet communications and usage patterns. Reasons for this monitoring are many, including, but not limited to, maintenance, cost analysis/allocation, testing compliance with this policy, and the management of FSR's liabilities.

All messages created, sent, or retrieved over FSR's computers, voicemail, e-mail/internet are the property of FSR and should be considered FSR information. FSR reserves the right to access and monitor all messages and files on FSR's computers, voicemail, e-mail/internet system. These communications are NOT private. Workforce Members should have no expectation of privacy in any items they create, send or receive on FSR's computer systems, e-mail, voicemail, or the internet.

C. E-Mail

FSR provides each Workforce Member with an e-mail address for business use. FSR utilizes Microsoft Exchange for its e-mail and the server is maintained secure within FSR network. Some Workforce Members may be provided e-mail addresses through the county or school where the Workforce Member is assigned. Workforce Members provided e-mail from other sources are expected to comply with policies of the school or county providing the e-mail in addition to FSR policy.

E-mail communication within FSR domain (e.g. between Workforce Members) remains behind firewall protection and is secure from outside access. E-mail encryption software is available to FSR Workforce Members when transmitting PII or PHI outside the FSR domain. FSR Workforce Members are expected to utilize available encryption technology prior to e-mailing PII or PHI. In addition to technical safeguards to protect e-mail communications, FSR staff are expected to utilize great caution when transmitting PII or PHI via e-mail. Any Workforce Member for the misdirection or transmission of PII or PHI via e-mail in an unsecure manner may be subject to corrective action.

D. Remote Access

FSR's IT Systems are set up to allow for secured remote access. Identified Workforce Members with a business need to remotely access FSR systems may be authorized for such remote use. When remotely accessing FSR networks, Workforce Members are expected to be conscious of

their surroundings and the security of the information they are accessing. All precautions to protect the information should be taken as if the information were being accessed from within FSR office.

E. Personal Devices

Workforce Members' use of personal computers and devices to access FSR information should be limited to situations where remote access is granted. Workforce Members are prohibited from downloading any information that could contain PII or PHI to a personal device unless specifically permitted to do so by the Privacy Officer.

Only specific Workforce Members identified by the Privacy Officer based on job duties will be permitted to sync smartphones or other personal devices with FSR e-mail server. Prior to permitting a sync, the Workforce Member will be required to encrypt the device, activate a pin password, and sign a personal device usage agreement.

F. Text Messaging

Text messaging is a convenient method of communication, but does not incorporate security functions to meet FSR's standards for PII and PHI. Text messages for work related purposes that do not contain any PII or PHI of FSR clients are permitted. Where a client has specifically authorized or requested that FSR provide an appointment reminder via text message, the location, date and time of the appointment may be texted to the number provided by the client. No other information regarding the appointment should be included in the text. If a client texts information to a Workforce Member, the Workforce Member is expected to respond by phone or other approved method of electronic communication. The texting of any PII or PHI other than the limited approved for appointment reminders is not secure and is strictly prohibited. Any Workforce Member found to be texting PII or PHI may be subject to corrective action.

G. Social Media

Use of Social Media Outlets, including, but not limited to Facebook, Twitter, and YouTube, is not permitted during work time. A Workforce Member must use the Workforce Member's personal e-mail address for all non-work related communication. To protect the integrity of PII and PHI and to prevent unwanted intrusion into FSR's IT Systems, FSR e-mail addresses should not be utilized on social media outlets unrelated to the Workforce Member's work. Only Workforce Members specifically assigned to maintain FSR's social media presence are permitted to post content to social media on behalf of FSR.

Workforce Members are solely responsible for what they post online. FSR encourages its Workforce Members to use the Workforce Member's best judgment when posting content to a social media outlet. Posting of any PII or PHI obtained through employment at FSR is strictly prohibited. Workforce Members are reminded that simply removing an individual's name from a post including PII or PHI may not be sufficient to de-identify the individual.

If pictures taken on FSR's property or locations where FSR provides services are posted, Workforce Members are responsible for ensuring that no PII or PHI is visible. An unauthorized

disclosure of PII or PHI via social media may subject the disclosing Workforce Member to corrective action up to and including termination.

VIII. Password Management and Electronic Signature

Passwords will be required to log in to a computer with access to the network and the EHR software program. Each Workforce Member will choose the Workforce Member's own passwords. All passwords must satisfy sophistication requirements of the applicable software program, and should not be trivial in nature. Passwords may not include the username, person's name, "password," FSR's name, simple keyboard patterns, dates, dictionary words, or names of people or places.

Workforce Members are required to change network passwords and software passwords at a frequency to be determined by the Privacy Officer. Systems will prompt the Workforce Member when a password change is required. Passwords will be changed at any time in which the security of such password has been compromised or a Workforce Member with knowledge of the password terminates employment with FSR.

Passwords are not to be given to any unauthorized person or otherwise shared for any reason. Passwords should not be written down or stored anywhere around the workstation for which they are used or in any other location where they could be discovered by an unauthorized individual. If a Workforce Member is concerned that his or her password may have been compromised, the Privacy Officer should be immediately notified so that the password can be changed.

FSR maintains portions of FSR's medical record documentation in The EHR. All documentation is authenticated in the EHR through use of an electronic signature. The use of an electronic signature is deemed to constitute a signature and has the same effect as a written signature on a document. The EHR system ensures that all electronic signatures: i) identify the individual signing the document by name and title; ii) include the date and time the signature is affixed; iii) ensure the documentation cannot be altered after the signature has been affixed by limiting access to the code or key sequence; and iv) provide for non-repudiation, that is, strong and substantial evidence that will make it difficult for the signer to claim the electronic representation is not valid.

Each Workforce Member who authenticates documentation in The EHR will create a unique electronic signature. The electronic signature will be added to a document through the use of an individual password. Workforce Members are prohibited from disclosing Workforce Member's individual electronic signature password or utilizing the individual electronic signature password of another user. Any prohibited activity described above constitutes a violation of this policy and may be subject to corrective action.

IX. Contingency Plan

FSR maintains a data back-up, disaster recovery, and emergency mode operations plan as part of its Disaster Recovery/Business Continuity Plan. This Section VII is supplemental to the Disaster Recovery/Business Continuity Plan for the purpose of addressing potential impact to PII and PHI.

A. Applications and Data Criticality Analysis

Resource expenditure related to data back-up and disaster recovery is prioritized consistent with the criticality analysis performed during FSR's IT System inventory process.

B. Data Backup Plan

FSR has implemented a comprehensive backup plan to ensure the availability of information for restoration in the event of an interruption.

The servers utilized by FSR are backed up daily. My document folders on individual workstations are redirected to encourage Workforce Members to store all PII and PHI on the server for incorporation into the back up process. Remotely hosted software programs, including the EHR, are backed up by the software vendor consistent with the terms of the contract.

Workforce Members are not permitted to store PII or PHI on individual workstations or laptops unless specifically authorized by FSR. In all instances where information is stored on individual laptops, the information should be a copy of information on the server rather than an original file. Laptops and workstations are not automatically included in the back-up process, but can be manually backed up as determined necessary by the Privacy Officer.

C. Disaster Recovery Plan

There are three (3) categories of unavailability of PII or PHI: 1) a failure in the software; 2) failure in a FSR server; or 3) loss or failure of a laptop or workstation. Once access is restored, the schedules and paper notes available to FSR will be utilized to restore any documentation that may have been lost due to the interruption. The Privacy Officer and IT Vendor will coordinate any necessary third party access to facilitate the restoration process.

Software Failure. In the event the EHR or other software is unavailable, FSR Workforce Members should immediately contact the Privacy Officer. The Privacy Officer will contact the appropriate software vendor to determine the cause of the unavailability and implement steps toward a resolution. Contact information for each software vendor is maintained by the Privacy Officer. The levels of priority in resolving the interruption are described in the service agreement with the software vendor. If there is a loss of a FSR database, the vendor will utilize a backup of the database to restore access.

Server Failure. In the event of a loss or failure of one (1) of FSR's servers, the Privacy Officer or designee should immediately be notified. The IT Vendor will be contacted to begin the restoration process. The IT Vendor will coordinate the repair or replacement of any hardware to restore function. Depending on the nature of the failure, the IT Vendor may utilize one of the backup hard-drives to restore data.

Laptop Loss or Failure. In the event of a loss or a laptop failure, the Privacy Officer and IT Vendor should be notified immediately. If the loss may result in compromise to the security of PII or PHI, the Incident investigation policy will be followed. To restore Workforce Member access, the IT Vendor will identify an alternative computer to be used by the Workforce Member.

D. Emergency Mode Operation Plan

In the event of interruption to IT Systems during a time in which services must be provided, FSR will transition to a paper records while the IT Systems are being restored. The Privacy Officer is responsible for determining when interruption to access will be of duration to necessitate use of paper records. Paper records are to be maintained on the Workforce Member's person or in a secured area at FSR office. Once access is restored, paper records will be utilized to enter the data into the IT Systems. Each Workforce Member is responsible for ensuring complete entry of all data and subsequent destruction of the temporary paper record in a manner that maintains confidentiality of the information.

If information about a client is needed during an unavailability of the IT Systems, FSR will coordinate with the client, partner agencies, and other resources to obtain necessary information for continued operations..

E. Testing and Revision Procedures

The back-up and disaster recovery processes are tested and revised by the IT Vendor. Documentation regarding testing procedures is maintained by the IT Vendor and may be requested as needed.

X. Facility Security Plan

FSR provides services at its office, in client homes, and around the community. FSR's servers are located at the office and are located in a back office area. FSR has a number of workstations that remain at the office and connect to the servers. Workforce Members transport some of FSR's laptops outside the FSR office. FSR Workforce Members are expected to return all laptops and other devices or media containing PII or PHI to FSR Office when not specifically needed for use outside the office in the performance of job duties.

The FSR office is locked after business hours with access limited to those individuals determined necessary by FSR. There are some areas of the FSR building that may be open for community use after FSR business hours. These areas of the building are separated from the remainder of the building by additional locks. FSR Workforce Members are prohibited from storing any PII or PHI in an area that may be open after business hours. The office has a security alarm system, including window alarms. Any keys provided to Workforce Members are checked out by the Privacy Officer or designee. Further, back office areas may be secured by a separate key pad lock with the code only provided to authorized Workforce Members.

Workforce Members are prohibited from allowing third parties to access the office after-hours unless specifically permitted by the Privacy Officer or physician. Workforce Members are expected to ensure the office locks behind them when leaving at the end of the day. Each Workforce Member is responsible for ensuring that the office is secured when unattended.

FSR's servers are located in a low-traffic back office area. Only the Privacy Officer, HR/Accounting Assistant and IT Vendor are permitted to access FSR's servers. Any Workforce Member who witnesses another person in the server room must immediately report such person to the Privacy Officer.

Visitors are primarily limited to the reception area. Any visitor permitted to access other areas of the office is required to check in at the front desk. Visitors are not authorized to enter areas containing PII or PHI unattended and must be escorted by a FSR staff member when in back office areas. Any Workforce Member who sees an individual or visitor of FSR unattended in an area other than the waiting room is expected to approach the person and offer assistance finding an authorized area.

Any changes to the locks or alarm systems securing PII or PHI will be recorded and the record will be maintained by the Privacy Officer. In the event emergency access to the IT Systems is needed, such access will be granted by the Privacy Officer and IT Vendor.

XI. Workstation Use and Security

All FSR workstations should be utilized in a manner that minimizes incidental disclosure of information displayed on the monitor. Monitors should be positioned away from high traffic areas. When a client or other third party is in view of a monitor, care should be taken to ensure only that client's information is visible on the screen.

Only Workforce Members are permitted to access workstations. Any non-Workforce Member found in a workstation area should be approached and escorted to the waiting room.

Workforce Members are expected to ensure the physical safety of each workstation. Food and drink should not be left in areas where it can be spilled into the computer. If beverages are permitted in the particular work area, they should have lids. Workstations and laptops should be maintained in areas with adequate ventilation. Papers, books, or other items should not be stacked on workstation CPUs.

Laptops that leave FSR office must be maintained secure on the person of the individual removing them. Laptop and tablet computers may not be left in unsecured vehicles or public areas. When possible, laptops should be transported in a locking case. A Workforce Member responsible for the loss or theft of a laptop may be subject to discipline for failure to safeguard the device.

XII. Device and Media Controls

FSR may periodically save PII or PHI to a laptop, external hard drive, USB drive, or other electronic device or media as determined appropriate by the Privacy Officer. PII and PHI should not be saved to a device or media by any Workforce Member without obtaining prior authorization from the Privacy Officer. Copy machines, printers and other devices may automatically store PII or PHI during use.

Any Workforce Member found to be saving PII or PHI on unauthorized media or devices may be subject to discipline. Workforce Members removing media or devices from FSR office are responsible for security of the media or device in transit. Media and devices should not be left unattended in an unlocked vehicle or public area. Workforce Members will be held responsible for any loss or destruction of media or devices in their control.

Prior to disposal of media containing PII or PHI, FSR will take steps to ensure the PII or PHI has been destroyed in a manner that ensures its confidentiality is maintained. This disposal can be accomplished by either 1) utilizing an IT professional to wipe and reformat the media or device in a manner that renders the PII or PHI unusable, including provision of a certification of such destruction, or 2) physically shredding or destroying the media or device prior to disposal.

Prior to re-using media or devices for other purposes, FSR will ensure that all PII or PHI has been removed from the media or device. Prior to re-use, the media or device will be wiped and re-formatted to ensure no PII or PHI remains.

The Privacy Officer, in coordination with the IT Vendor, is responsible for maintaining a list of devices and media containing PII or PHI as part of FSR's inventory process. For each media or device, FSR maintains a record of the primary storage location and the individual responsible for the media or device's physical security.

All PII or PHI is actually maintained in FSR servers. Prior to moving any servers or performing significant maintenance, a backup copy of the server is created by the IT Vendor. FSR laptops and workstations are only used to establish access to the PII or PHI, but do not store the information itself. As a result, a backup of the laptop or workstation is typically not necessary prior to movement, although backup may be created at the discretion of the IT Vendor. Similarly, PII or PHI maintained on electronic media is a secondary copy of information maintained on the IT servers and does not constitute original PII or PHI.

XIII. Encryption and Decryption

FSR has implemented encryption mythologies related to its wireless network, firewall security, remote access, file transfer protocols, and e-mail transmission. Workforce Members are expected to utilize available encryption methodologies when accessing or transmitting PII or PHI.

The decision to implement encryption and decryption technology, as well as the type of technology to be utilized, is part of the FSR risk assessment process. Where encryption is utilized, FSR will coordinate with its IT Vendor to utilize technology consistent with the current guidelines from the National Institute of Standards and Technology ("NIST") where possible.

XIV. Audit Controls and Integrity

The EHR and other software utilized by FSR to store PII and PHI maintain a number of audit trails and provide a number of audit reports. These reports are reviewed periodically by the Privacy Officer. All changes in the EHR software is tracked by user name, date, and time. For many functions, the actual changes made are also tracked to prevent unauthorized alteration.

FSR stores the majority of its PII or PHI in the EHR software. The EHR provides integrity controls to ensure information is not inappropriately altered. The system records the date, time and username of individuals making changes to PII or PHI. Changes to medical record documentation are authenticated utilizing an electronic signature. Audit logs available in the systems allow for review of the history of changes made to a particular record.