DATA PRIVACY POLICY

Table of Contents

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

POLICY

Family Service Rochester ("FSR") expects its Board, managers, employees, volunteers, and contractors ("Workforce") to comply with Minnesota Government Data Practices Act (Minnesota Statutes Chapter 13, collectively "MGDPA"), the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-164, collectively "HIPAA"), and other applicable requirements related to the privacy and protection of "personally identifiable information" or "PII" and "protected health information" or "PHI."

PROCEDURE

I. Oversight of Data Privacy

A. Privacy Officer

A Privacy Officer shall be appointed by the Board of FSR. The current Privacy Officer is the Director of Human Resources and Operations. All employees shall be notified of such appointment and of any change in the Privacy Officer. The Privacy Officer has overall responsibility to oversee FSR's compliance with data privacy and security requirements under this Data Privacy Policy and the Data Security Policy. The Privacy Officer's duties are described in Attachment A. For purposes of Privacy Officer functions, the Privacy Officer reports directly to the Board.

The Privacy Officer may engage the assistance of and delegate responsibilities to other FSR Workforce or Business Associates as needed to carry out the Privacy Officer's duties. Any such delegation does not affect the Privacy Officer's responsibilities regarding oversight of the above listed duties.

B. Workforce Training

Each Workforce Member shall receive privacy and security training regarding the policies and procedures with respect to PII and PHI. The training shall be tailored and appropriate for the group to which the training is presented. All new Workforce Members shall receive the training within a reasonable time of joining the Workforce. When FSR's policies and procedures are materially changed, the Workforce Members affected by the changes shall be re-trained within a reasonable time.

FSR's education and training program utilizes a variety of training methods including, but not limited to, in person training, internet based training, newsletters, and memos. Training may be provided by FSR's Workforce Members, legal counsel or outside consultants. Workforce Members may undergo training through internal sessions or external meetings and conferences.

All training shall be documented in written or electronic form and the documentation shall be retained for at least six (6) years by the Privacy Officer.

C. Subcontractors

Subcontractors and other vendors who are outside the Workforce of FSR will be required to take reasonable and appropriate steps to maintain the privacy and security of any PII or PHI that the subcontractor or vendor may receive from FSR.

If the subcontractor or vendor is a "Business Associate" as defined by HIPAA, FSR will obtain assurances from the Business Associate and enter into a Business Associate Agreement with the Business Associate prior to allowing the Business Associate to access, create, maintain, or transmit any PHI on behalf of FSR.

If FSR is aware of a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the Business Associate Agreement, FSR will take reasonable steps to cure the breach and end the violation. If such steps are unsuccessful, the Business Associate Agreement with the Business Associate will be terminated, if feasible.

FSR will periodically revise its Business Associate Agreement with its Business Associates as may be required to incorporate changes under the HIPAA Regulations.

D. Complaints

A client has a right to file a complaint if the client feels that the client's privacy has not been adequately protected. Such complaint can be filed with the Privacy Officer. If the client receives services from a HIPAA Program at FSR, the client may also file a complaint with the US Department of Health and Human Services ("HHS"). If the client receives services from a MGDPA Program, the client may also file a complaint with the Minnesota Attorney General's office or the city, county or state agency with whom FSR contracts.

FSR requests that complaints be submitted in writing. If an client or client representative makes a verbal complaint to a member of FSR Workforce, such Workforce Member should document the complaint and forward the complaint to the Privacy Officer.

The information provided on the complaint should be as complete as possible. FSR requests the following information be included: name of the complainant (can be anonymous), date the complaint was filed, date and time of incident (if applicable), location, names of any Workforce Members who were involved, names of any Business Associates involved, and a short summary of the complaint.

The Privacy Officer will maintain documentation related to each complaint in compliance with the documentation and record retention requirements.

E. Identification, Investigation, and Resolution of Potential Incidents

All Workforce Members, agents, and Business Associates of FSR are required to immediately report any actual or suspected unauthorized access, use, or disclosure of PHI or PII or any actual or suspected violation to the Data Privacy or Data Security Policies (collectively "Incident") to the Privacy Officer. Failure to report an Incident may in itself result in discipline of the Workforce Member.

FSR will periodically review or audit the uses and disclosures of PII and PHI in its control, as provided in this Policy and the Data Security Policy, to identify potential Incidents.

1. Investigation of Incidents

Once an Incident is identified on internal audit or reported to the Privacy Officer, he or she will initiate an investigation of the Incident. This investigation will involve the collection of information including Workforce Members or Business Associates involved; the nature of the Incident; the number and names of individuals involved; and the types of PHI or PII involved.

An investigation may be conducted by the Privacy Officer or his or her designee. Legal counsel may be consulted to conduct the investigation and render legal advice to FSR at the discretion of the Privacy Officer.

The purpose of the investigation will be to determine whether there has been a violation of MGDPA, HIPAA, or FSR policy. If an investigation determines there has been a violation of MGDPA or HIPAA, the Privacy Officer will also determine whether the Incident is a Breach requiring notification.

Regardless of whether an Incident is a Breach, if the Privacy Officer determines that a Workforce Member or Business Associate has violated MGDPA, HIPAA, or FSR policy, corrective action may be taken against the Workforce Member or Business Associate.

2. Notifications

Where an investigation determines that an Incident has resulted in a violation of MGDPA or HIPAA, the Privacy Officer will determine, in coordination with legal counsel where appropriate, whether the Incident is a Breach requiring notification.

Where the Incident resulted in an unauthorized use or disclosure of PII or PHI obtained under a contract where FSR is a Business Associate, FSR will notify the contracted party as required by the contractual provisions.

Any required notification will be provided without unreasonable delay, consistent with the obligations of the law creating the notification obligation.

a. HIPAA Notifications

Where an Incident affects a HIPAA Program and resulted in a use or disclosure of PHI not permitted by HIPAA, the incident is presumed to be a Breach requiring notification. The Privacy Officer can either accept this presumption and provide HIPAA required notifications or

perform a breach risk assessment to determine the probability that the PHI was actually compromised.

If a breach risk assessment is performed, it will include at least:

- The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person who used or received the PHI;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If the breach risk assessment determines that the probability of compromise of the PHI is low, the Privacy Officer may determine and document that notification is not required.

If the Incident is a Breach under HIPAA, FSR will provide notification to individuals affected. If the Breach affects more than 500 individuals in one state or jurisdiction, notification will also be made to the media and HHS. If less than 500 individuals are affected, the Breach will be included in FSR's annual report to HHS.

b. MGDPA

Where an Incident affects a MGDPA Program and results in a use or disclosure of PII or PHI not permitted by MGDPA, the Privacy Officer will determine whether the incident compromises the security and classification of the data.

If the Incident is determined to compromise the security or classification of the data, then it is a Breach for purposes of MGDPA and notification will be provided to all affected individuals, consistent with obligations under MGDPA.

In providing any required notifications, FSR will also consider the other state data breach notification requirements. If data breach notification requirements of any state are triggered, FSR will provide notification consistent with the obligations of the applicable law. These notifications may include consumer reporting agencies, state attorneys general, or other regulatory notifications.

3. Mitigation of Harm and Prevention of Future Incidents

Regardless of whether an Incident amounts to a Breach, FSR will take reasonable steps to mitigate harm and prevent future Incidents

Mitigation may include, but is not limited to:

Obtaining assurances from the person to whom the information was disclosed that it will not be disclosed further.

- If the unauthorized acquisition, access, use, or disclosure is found to amount to a breach, notification will be provided following the Breach Notification Policy.

- Establishment of a toll free telephone number for individuals to call to obtain information regarding the breach for a period of not less than ninety (90) days.

- Recovery or destruction of documents or other media improperly disclosed.

- In the case of a high risk of harm to the individual, offering to pay for credit monitoring for a period of time.

FSR will review the actions of Workforce Members and Business Associates involved in the Incident and take appropriate measures to discipline the behavior and prevent future incidents.

After the occurrence of an Incident, FSR will also review all related policies and procedures to determine if modification, clarification, or addition is needed. Any policy changes implemented as a result of an incident will be communicated to the Workforce Members and Business Associates affected by the change. Additional training may be provided to Workforce Members as needed.

4. Documentation.

A record of each Incident will be maintained by the Privacy Officer. The record of each incident will include, at minimum: documentation of the investigation; a copy of the breach risk assessment, if performed; a copy of any notices; and a copy of any documents created in the process of mitigation of the harm or prevention of future breaches.

F. Non-Retaliation

Neither FSR, nor any Workforce Member of FSR, will intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for:

- Exercising the individual's rights;

- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing related to the privacy or security of PII or PHI;

- Participating in any process provided for under HIPAA or MGDPA;

- Filing a complaint under this Policy; or

- Opposing any act of FSR made unlawful by the HIPAA, MGDPA, or any other law, so long as the individual held a good faith belief that FSR was acting unlawfully and the manner of opposition is reasonable and does not involve a violation of the regulations.

Any such intimidating, threatening, coercive, discriminatory, or retaliatory behavior is a violation of these policies and may subject the individual to applicable sanctions.

G. Corrective Action

FSR will take appropriate corrective action against a Workforce Member who fails to comply with FSR policies and procedures relating to privacy and security of PII or PHI. These corrective actions may include, but are not limited to, retraining and re-evaluation, verbal warning, written warning, termination of employment, or termination of contract.

The level of sanction will be determined by the Privacy Officer and Executive Director and documented in the Workforce Member's human resources file. If the Workforce Member is not an employee, the documentation will be maintained by the Privacy Officer.

II. Control and Disposal of PHI and PII

FSR will implement appropriate safeguards to maintain PHI confidential and secure. Workforce expectations regarding safeguards implemented will be communicated to Workforce Members and incorporated into policies and procedures. FSR may implement additional privacy safeguards as are determined to be needed by the Privacy Officer. Workforce Members affected by such changes will be notified at the time of implementation of such measures, or within a reasonable time of such implementation.

To the extent reasonably practicable, PII and PHI will be stored in areas of FSR where the information is secure and the access can be limited. Administrative, physical, and technical safeguards implemented to protect PII and PHI in electronic form will be described in the Data Security Policy.

Workforce Members permitted to take PII or PHI outside the FSR office are responsible for the privacy and security of such information while it is outside the FSR office and in the control of the Workforce Member. Workforce Members are expected to take steps to protect PHI and PII and prevent any loss or unauthorized disclosure.

When information containing PII or PHI is no longer needed by FSR, such information will be disposed of in a manner that protects the privacy of such information. All documents and materials containing PII or PHI will be shredded or otherwise destroyed prior to disposal. Computers and other electronic media are similarly disposed of by FSR in a manner that protects the confidentiality of any PII or PHI.

III. Uses and Disclosures of PHI and PII

FSR expects all Workforce Members to limit uses and disclosures of PII and PHI to the extent necessary to perform job functions for FSR. FSR limits the amount of PII and PHI available to Workforce Members as necessary to perform job duties. The granting, modifying, and termination of access to PII and PHI is described more fully in the Data Security Policy.

Where a Workforce Member is permitted use of PII and PHI to perform job functions, such access should only be used for FSR purposes. Accessing PII or PHI for personal or other purposes unrelated to FSR activity is strictly prohibited and may result in corrective action of the Workforce Member.

When disclosing PII or PHI to individuals or organizations outside FSR, the Workforce Member should take reasonable steps to ensure the disclosure is permitted under applicable law and the amount of information disclosed is limited to the amount necessary to accomplish the purpose of the disclosure. Similarly, when requesting PII or PHI for FSR purposes, Workforce Members should reasonably limit the request for the required purpose. Where FSR engages in a routine request or disclosure of PII or PHI, such as submission of a routine report to a contracted agency, FSR may implement policies or processes regarding the appropriate amount of PII or PHI to be included.

When a Workforce Member performing functions related to a HIPAA Program or MGDPA Program will be disclosing PII or PHI to a different program within FSR, the Workforce Member is expected to treat the disclosure as if it were to an individual or entity outside FSR and to ensure the disclosure is permitted under HIPAA or MGDPA.

Prior to any disclosure, except a disclosure requiring an opportunity for the client to agree or object, FSR shall verify the identity of the person requesting PII or PHI and the authority of the person to have access to the PII or PHI, if the identity or authority of the person is not known to FSR.

Any questions regarding the amount of PII or PHI to be used or disclosed for an FSR function, verification of the identity of a person requesting PII or PHI, or the permissibility of a use or disclosure should be directed to the Privacy Officer.

A. Personal Representatives

If the client is a competent adult or an emancipated minor, the individual can sign all forms and make all decisions related to use and disclosure of the client's PII and PHI. If, under applicable law, a person has authority to act on behalf of a client in making decisions, FSR must treat that person as a personal representative with respect to the PII or PHI relevant to such representation. Thus, to the extent a client has executed a power of attorney, such power of attorney may have authority to act on behalf of the client. Any questions regarding a power of attorney should be directed to the Privacy Officer.

1. Deceased Individuals

PHI related to a deceased client remains PHI and subject to HIPAA Policy for fifty years following the death of the client. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased client or the client's estate, FSR will treat such person as a personal representative, with respect to PII or PHI relevant to such personal representation. Thus, where an executor or administrator has been appointed, that executor or administrator will have authority to act as if they were the client for authorizations related to PII or PHI. FSR may also disclose PHI regarding a deceased client to a family member or other person who was involved in the deceased client's care or payment prior to death to the extent such information is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the client or the executor or administrator of the estate and known to FSR.

2. Minors and Incompetent Adults

A person who may legally consent on behalf of a minor or incompetent adult under Minnesota law should be asked to sign any forms and make any requests pursuant to PII or PHI. If a parent, legal guardian, or other person acting *in loco parentis* seeks access to a minor's PII or PHI, the access shall be granted unless 1) FSR is aware of a court order restricting such access; 2) the minor is an emancipated minor as determined by state law; 3) the parent, guardian, or person acting *in loco parentis* has assented to an agreement of confidentiality between FSR and the minor; 4) state law prohibits disclosure of information to a parent, guardian, or person acting *in loco parentis*, or 5) federal or state law otherwise prohibits access to the information.

A minor may have the authority to act as an individual with respect to protected healthcare information relating to a healthcare service if the minor may lawfully obtain such healthcare service without the consent of a parent, guardian or other person acting on loco parentis and the minor consents to such service.

Where FSR is aware of additional restrictions related to the disclosure of PII or PHI of a minor, FSR will comply with the applicable restrictions. For example, if FSR is aware of a court order restricting the access of a parent to information regarding a minor, FSR will similarly comply with such court order.

Any questions regarding the validity of a personal representative, as to whether access should be granted, must be directed to the Privacy Officer.

B. Limitations on Uses and Disclosures of PHI under HIPAA

This Section III.B. applies to PHI obtained by FSR related to its HIPAA Programs.

Any use or disclosure of PHI not otherwise addressed in this Section III.B. requires authorization from the client. Examples of disclosures requiring authorization of the client include:

- For marketing purposes
- For research not approved by an IRB
- to an employer or school (e.g., return to work or school slips); and
- certain types of information subject to additional privacy protections, such as psychotherapy notes, alcohol or drug abuse treatment records, and HIV records.

Where an authorization is required, FSR prefers the use of its release of information form. If a third party authorization form is provided, FSR must ensure it includes all elements required by HIPAA prior to the disclosure of PHI. A list of the HIPAA required elements is provided in Attachment B. Use or disclosure of PHI may be permitted under HIPAA without authorization in the following situations:

1. <u>Treatment, Payment, and Healthcare Operations</u>

FSR may use and disclose PHI to individuals or entities for treatment, payment, or healthcare operations purposes, except for psychotherapy notes, for which special rules apply. FSR is not required to have a client's consent or an authorization to disclose PHI for these purposes.

Treatment means the provision, coordination, or management of health care and related services by one (1) or more healthcare providers, including the coordination or management of health care by a healthcare provider with a third party; consultation between healthcare providers relating to a client; or referral of a client for health care from one healthcare provider to another.

Payment activities undertaken by a provider to obtain reimbursement for the provision of health care may include, but are not limited to, determinations of eligibility or coverage, billing, claims management, collection activities, review of health services with respect to medical necessity or appropriateness of care, and utilization review including pre-certification and pre-authorization of services.

Healthcare operations means quality assessment activities (including outcomes evaluation and case management and care coordination); review of competence or qualifications of healthcare professionals and their performance; accreditation, licensing, certification or credentialing activities; conducting or arranging for medical review, legal services, and auditing functions; business planning and development (including conducting cost-management and planning-related analyses); and business management and general administrative activities of the entity.

PHI may be used or disclosed, as necessary, by FSR or to another healthcare provider for treatment of the client or to obtain payment for services provided. Information may also be used for FSR's own healthcare operations.

Disclosures may be made to another healthcare provider or health plan for the other entity's healthcare operations, if both FSR and the recipient of the PHI have a relationship with the client and the disclosure is for one of the following purposes:

- quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (the primary purpose of these studies cannot be to obtain generalized knowledge);
- population based activities related to improving health or reducing health care costs;
- protocol development;
- case management and care coordination;
- contacting providers and clients about treatment alternatives;
- evaluation of providers;
- evaluation of health plan performance;
- conducting training programs;

- accreditation, certification, licensing or credentialing activities; or
- healthcare fraud and abuse detection or compliance.

2. Individuals Involved in Care

FSR may disclose certain limited PHI to a client's family member, relative, close personal friend, or any other person identified by the client as involved in the client's care. The PHI disclosed must be limited to the amount directly relevant to such person's involvement with the client's care or payment related to the client's care. FSR may also use PHI to notify, or assist in the notification of a family member, personal representative of the client, or other person responsible for the care of the client of the client's location, general condition, or death.

If the client is present or available prior to the use or disclosure and has the capacity to make health care decisions, PHI will only be disclosed if the client has agreed; the client was provided the opportunity to object and did not; or it was inferred from the circumstances, based professional judgment, that the client did not object.

If the client is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the client's incapacity or an emergency circumstance, FSR may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the client and, if so, disclose only the PHI that is directly relevant to the person's involvement with the client's health care. FSR may use professional judgment and experience to make reasonable inferences of the client's best interest in allowing a person to schedule an appointment or arrange transportation for a client.

FSR staff requests that each client provide a list of individuals involved in the client's care to be maintained in the client's record. Clients are requested to update this list as changes are made. FSR Workforce Members are expected to review FSR documentation to determine the extent of involvement of a person prior to disclosing PHI. If the Workforce Member is unsure of the person's involvement in the care of the client, the Privacy Officer should be consulted. FSR may, at any time, request authorization or consent (which may be verbal) of the client prior to disclosing PHI to a person involved in the client's care.

3. Victims of Abuse, Neglect, or Domestic Violence

FSR has mandatory reporting obligations related to suspected abuse, neglect, or domestic violence. FSR may disclose PHI and PII as necessary to fulfill those reporting obligations. There may be situations in which mandatory reporting obligations may not be triggered, but FSR is permitted to report information regarding potential abuse, neglect, or domestic violence. All reports of abuse, neglect, or domestic violence will be consistent with Minnesota law. Workforce Members with questions regarding these obligations should contact their direct supervisor, director, or the Executive Director.

4. To Avert a Serious Threat to Health or Safety.

FSR also has a duty to warn or take reasonable precautions to provide protections from violent behavior of a client or other person when FSR is aware of a specific, serious threat of physical

violence against a specific, clearly identified or identifiable potential victim. Even where the duty to warn is not mandated under Minnesota law, FSR may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if FSR, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat, or is necessary for law enforcement authorities to identify and apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Provider reasonably believes may have caused serious physical harm to the victim, or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

FSR will disclose PHI under this provision to law enforcement or a third person who is in a position to prevent the threat or protect the potential victim. Information disclosed will be limited to the minimum amount of information necessary to avoid the threat or harm. Workforce Members with questions regarding these obligations should contact their direct supervisor, director, or the Executive Director.

5. Disclosures Required or Permitted by Law

Any request for disclosure under this Subsection 4 should be approved by the Privacy Officer prior to disclosure.

FSR will use or disclose PHI as required by law and in a way that complies with the law. Such use or disclosure does not require client authorization. PHI may also be disclosed by FSR as required by the Secretary of HHS to investigate or determine FSR's compliance with the HIPAA Regulations.

There are additional limited situations regarding when FSR may disclose PHI without authorization related to i) judicial and administrative proceedings; ii) law enforcement purposes; iii) public health activities; iv) health oversight activities; v) decedents; vi) organ and tissue donation; vii) research; viii) to avert a serious threat to health or safety; ix) specialized government functions; and x) worker's compensation. A description of the additional requirements, to be reviewed by the Privacy Officer, for these disclosures are enclosed at Attachment C.

6. Business Associates

FSR will disclose PHI to Business Associates only where satisfactory assurances have been received that the Business Associate will properly safeguard the information and comply with the HIPAA through the execution of a Business Associate Agreement.

7. Disclosures by whistleblowers and Workforce Member crime victims

A Workforce Member is permitted to disclose PHI where he or she believes in good faith that FSR has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by FSR potentially endangers one or more individuals, workers, or the public; AND the disclosure is to: i) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant

conduct or conditions or to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards; or ii) an attorney retained by or on behalf of the Workforce Member or Business Associate for the purpose of determining the legal options of the Workforce Member or Business Associate with regards to the conduct.

8. De-Identified PHI

PHI that has been de-identified consistent with requirements under HIPAA through removal of required identifiers or certification of a qualified expert is no longer considered PHI and no longer subject to restrictions under HIPAA. FSR may use and disclose PHI to create information that is de-identified or disclose PHI to a Business Associate for such purpose. Health information that has been de-identified does not have to meet the authorization requirements provided that disclosure of a means of re-identification constitutes disclosure of PHI and re-identified information is PHI.

9. Limited Data Set

A Limited Data Set ("LDS") may be used or disclosed by FSR for research or healthcare operations without authorization of the client only where satisfactory assurances, in the form of a Data Use Agreement satisfying specific requirements under HIPAA, have been obtained that the recipient will only use the LDS as permitted by HIPAA.

10. Restrictions on Disclosures

Where FSR has agreed to client's request to restrict disclosures, FSR will comply with such request. However, if the client is in need of emergency treatment and the restricted PHI is needed to provide such treatment, the restricted information may be used or disclosed to the extent needed to provide the emergency treatment. If restricted information is disclosed in the provision of emergency treatment, FSR will request that such provider receiving the information will not further use or disclose the information.

11. Disclosures Consistent with Notice

FSR will disclose information only as consistent with its Notice of Privacy Practices.

C. Limitations on Use and Disclosure under MGDPA

Minnesota law imposes additional restrictions regarding how PII and PHI obtained from a state, county, or other government entity can be further used and disclosed by FSR. FSR will comply with MGDPA obligations regarding these limited uses and disclosures. The specific requirements on the use and disclosure of PII and PHI obtained from a state, county or other government program depends on the FSR program involved and which agency is disclosing the information. As such, FSR Workforce Members are expected to familiarize themselves with the applicable policies and procedures of the state, county or other government entity from which FSR obtains the information and apply those policies and procedures to the Workforce Member's activities. For example, if the PII or PHI is obtained related to performance of services under FSR's contract with Olmsted County, the Workforce Member should follow Olmsted County's policies and procedures related to the PII or PHI in addition to FSR's internal

policies and procedures. In the event of a conflict, the rule that provides the most protection to the information should be applied. Any questions should be directed to the Privacy Officer.

IV. Additional Expectations and Requirements for HIPAA Programs

A. Waiver of Individual Rights.

FSR will not request or require clients to waive their rights under HIPAA as a condition of the provision of treatment.

B. Documentation.

FSR will maintain documentation as required by HIPAA. This documentation includes, but is not limited to, policies, procedures, complaints, violations, sanctions, breaches, disclosures, Notice of Privacy Practices, Acknowledgment of Notice of Privacy Practices, Business Associate Agreements, and HIPAA Compliance training. Documentation may be maintained in a paper or electronic format. All documentation will be made available to those persons responsible for implementing the procedures to which the documentation pertains. Documentation will be reviewed periodically and updated as needed. All documentation created or maintained under HIPAA must be maintained on file for a period of at least six (6) years. For documentation such as policies, procedures, Notice of Privacy Practices, and designation of Workforce Members which may be modified or revised over time, the document which has been replaced must be maintained, including its effective dates, for a period of not less than six (6) years from the last date on which it was effective.

C. Cooperation with the Secretary.

FSR will cooperate with the Secretary of HHS to the extent required by law. FSR will submit compliance reports as may be requested by the Secretary of HHS. FSR will cooperate with any investigations or compliance reviews the Secretary of HHS may choose to undertake. This cooperation will include providing access to information, including facilities, books, records, accounts and other sources of information, during normal business hours, or, if exigent circumstances exist, at any time the Secretary of HHS requires. FSR will require all Workforce Members, Business Associates, and providers to cooperate and provide requested documents to the Secretary of HHS. If requested information is in the exclusive possession of a third party, FSR will assist the Secretary of HHS, to the extent it is able, in obtaining the requested information.

D. Incidental Disclosures.

During the course of providing treatment to clients, FSR Workforce Members may communicate with clients and/or client's family members. FSR will take reasonable steps to ensure the privacy of these communications including, but not limited to:

- Utilization of private areas by staff when discussing client information with the client and/or client's family members. If these areas are not available, the staff will attempt to use an area of low visitor and staff activity for the communication.

- Ensuring all individuals present are appropriate during the discussion of client information prior to beginning such discussion.

- Attempting to verify the identity of the person with whom staff is speaking on the phone through requesting of basic information and leaving minimally necessary information on voice messages.

While clients are receiving treatment or services at FSR, some of their PHI may be used in a way in which it may be viewed by other individuals. Such uses are only permitted in order to further the treatment of the client and communication between the treatment providers. FSR Workforce Members should take appropriate steps to ensure that minimal PHI is left in places where it can be viewed by other individuals and to limit the number of individuals who enter a space where PHI may be stored.

E. Notice of Privacy Practices

FSR will maintain a Notice of Privacy Practices consistent with obligations under HIPAA. FSR is in an organized healthcare arrangement related to some of its MGDPA Programs and may utilize the Notice of Privacy Practices of the contracted county or other agency related to such programs.

A copy of the current Notice will be posted in a prominent location in the FSR office.

A copy of the current Notice will be given to each client receiving services from a HIPAA Program. In the case of an emergency, the notice will be provided as soon as reasonably practicable after the emergency treatment situation. FSR will obtain acknowledgment from the client that he or she has been provided a copy of the Notice.

The notice may be provided in an electronic, rather than paper form, where the client has agreed to electronic notice and such agreement has not been withdrawn.

The current notice will be provided to any client upon request, even if a copy was previously provided in paper or electronic form.

FSR may revise the Notice of Privacy Practices from time to time to reflect changes in the regulations or changes in FSR policy. Any changes will not be effective prior to the date which the revised notice is available to clients receiving services from the HIPAA Program.

The Privacy Officer will maintain copies of all Notices, including their effective and end date, per the HIPAA records retention policy. Clients may receive, upon request, copies of the revised Notice of Privacy Practices or any previous notice.

V. Client Rights under HIPAA

A. Access to medical records or PHI in a Designated Record Set

FSR must provide clients access to information contained in their medical records under the Minnesota Health Records Act and to PHI contained in a Designated Record Set under HIPAA.

A designated record set includes: i) Medical records; ii) Billing records; and iii) other records to the extent that they were used, in whole or in part, by FSR to make decisions about the client. However, the following information is not a part of the Designated Record Set: peer review information; quality assurance information; performance improvement information; attorney-client privileged materials; documents created in anticipation of litigation; incident reports; compliance information and investigations; risk management materials; complaints, investigation of complaints, and their disposition; and personnel records.

A client has right to inspect and obtain a copy of his/her PHI in a designated record set or medical record, for as long as FSR maintains the PHI. The request should be made in writing.

FSR's Privacy Officer or designee is responsible for receiving and processing the request to inspect and/or copy the PHI.

Where the PHI subject to a request for access is maintained in an electronic form and the client requests an electronic copy of the information, FSR will provide the client access to the information in the electronic form and format requested by the client, to the extent the information is available in such format. If not available in the requested format, the information will be provided in an electronic format as agreed by FSR and the client.

If the client requests FSR provide the access through transmission of the information to another person designated by the client, the information will be provided to the designee so long as the request is in writing, signed by the client, and clearly identifies the designee and where to send the PHI.

FSR may deny access to the PHI or a portion of the PHI in limited situations. The Privacy Officer must review and approve any denial of an access request to determine compliance with HIPAA and Minnesota law.

B. Request for Amendment

A client has right to request an amendment of his/her PHI or a record about the client in a designated record set for as long as the PHI is maintained in the designated record set.

Requests for amendment must be in writing on the form provided by FSR and include a reason to support the amendment.

FSR's Privacy Officer is responsible for receiving and processing the request for amendment.

FSR may deny an client's request for amendment in limited situations

C. Accounting of Disclosures

A client has the right to request and obtain an accounting of disclosures made by FSR of his/her PHI for the six (6) years prior to the date the accounting is requested. The request for the accounting must be in writing.

FSR's Privacy Officer is responsible for receiving and processing the request, consistent with 45 CFR 164.528.

D. Request for Confidential Communications

A client is permitted to request confidential communications or alternative methods of communication. The request must be in writing. FSR has an approved form that may be provided to the client.

FSR will comply with all reasonable requests. FSR will not require the client to disclose the reason for their request. FSR may condition the reasonable accommodation on: how payment will be handled (if applicable); and specification of an alternative address or method of contact.

Once a request is granted, FSR will comply with the confidential communication or alternative method of communication, subject to the conditions above. If any Workforce Member does not comply with a granted confidential communication, such non-compliance may be subject to corrective action.

E. Request for Restrictions

An client is permitted to request additional restrictions of uses and disclosures of PHI. The request must be in writing. FSR has an approved form that may be provided to the client. Requests should be forwarded to the Privacy Officer or her designee as soon as received.

FSR will agree to and comply with a request that PHI not be disclosed to a third party payor for payment or healthcare operations only where the client has paid for the service in full. All other requests for additional restrictions will be granted at the discretion of FSR. FSR may terminate a restriction, if: i) the client agrees to or requests the termination in writing; ii) the client orally agrees to the termination and the oral agreement is documented; or iii) FSR informs the client that it is terminating its agreement to a restriction as to information created or received after the notice is provided to the client.

If any Workforce Member does not comply with a granted request for additional restrictions, such non-compliance may be subject to corrective action.

ATTACHMENT A
Duties of the Privacy Officer

- Provide development guidance and assist in the identification, implementation, and maintenance of policies and procedures for compliance with MGDPA and HIPAA.

- Review initial and periodic information risk assessments and conducts related ongoing compliance monitoring activities.

- Work with legal counsel, administration, and committees so that we have and maintain appropriate privacy and confidentiality consent forms, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

- Oversee, direct, or deliver the initial training and orientation to all Workforce Members.

- Participate in the development, implementation, and ongoing compliance monitoring of all Business Associate Agreements.

- Establish a mechanism to track access to PHI as required by law and to allow qualified individuals to review or receive a report on such activity.

- Oversee FSR's implementation of all individual rights under HIPAA.

- Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning FSR's data privacy and security practices.

- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with policies for all Workforce Members and Business Associates.

- Initiate, facilitate, and promote activities to foster information privacy and security awareness within FSR.

- Review all system-related information security plans throughout FSR to align the security and privacy practices.

- Work with FSR Workforce Members involved with any aspect of release of PII and PHI to ensure full coordination and cooperation under FSR policies and procedures and legal requirements.

- Maintain current knowledge of applicable federal and state privacy laws and security laws and accreditation standards, and monitors advancements in information privacy and security technologies.

- Serve as information privacy and security consultant to the organization.

- Cooperate with the Department of Health and Human Services, Office for Civil Rights, other agencies and organization officers in any compliance reviews or investigations.

- Periodically report to the Board regarding FSR's compliance with MGDPA and HIPAA.

ATTACHMENT B
Required Elements of a HIPAA Authorization

If a third party's authorization form is used, FSR staff will ensure that the form includes, at minimum, the following information:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

- The name or specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

- The name or other specific identification of the person(s), or class of persons, to whom the Provider may make the requested use or disclosure.

- A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an client initiates the authorization and does not, or elects not to, provide a statement of the purpose.

- An expiration date or an expiration event that relates to the client or the purpose of the use or disclosure. The statement "end of research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.

- The signature of the client and the date. If a personal representative of the client signs the authorization, a description of such representative's authority must be included.

- A statement of the client's right to revoke authorization in writing, exceptions to the right to revoke, and description informing the client how to revoke the authorization, including a reference to the Privacy Notice.

- A statement of FSR's ability or inability to condition treatment on the authorization, stating either:

    - That FSR may not condition treatment on authorization, or

    - The consequences to the client of a refusal to sign an authorization when FSR can condition research related treatment on authorization.

- Statement that information used or disclosed may be subject to re-disclosure by the recipient and no longer protected by the HIPAA privacy rules.

ATTACHMENT C
Disclosures Under HIPAA Without Authorization

Disclosures for Judicial and Administrative Proceedings. FSR will disclose PHI in response to a subpoena when it is provided in combination with: i) a court order; ii) a qualified protective order; or iii) an authorization signed by the client or client's personal representative. If the subpoena is not accompanied by this additional documentation, FSR may coordinate with the requesting attorney to ensure necessary documentation is in place prior to disclosure of PHI.

Disclosures for Law Enforcement Purposes. FSR may disclose PHI for law enforcement purposes to a law enforcement official:

- Pursuant to process and otherwise as required by law in compliance with reporting laws regarding certain types of wounds, in compliance with a court order, court-ordered warrant, subpoena or summons issued by a judicial officer, in response to a grand jury subpoena, in response to an administrative or civil subpoena, summons or demand, provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the information sought is as specific and narrowly drawn as practicable, and de-identified information could not reasonably have been used to meet the purpose of the request.

- To identify or locate a suspect, fugitive, material witness, or missing person, provided that only the following information is disclosed: name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, if applicable, description of distinguishing physical characteristics (including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos).

- In response to a law enforcement official's request for PHI about an individual who is, or is suspected to be, a victim of crime (other than abuse, neglect, or domestic violence as discussed above) if the individual agrees to the disclosure or the provider is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that the law enforcement official has represented that such information is needed to determine whether a violation of law has occurred; the information is not to be used against the victim; the need for the information is related to immediate law enforcement activity and delay could materially and adversely affect such activity; and the disclosure is in the best interest of the individual as determined by FSR.

- To alert law enforcement of the death of an individual if the Provider has a suspicion that the death may have resulted from criminal conduct.

- If a Provider believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the premises of the Provider.

Permitted Disclosures for Public Health Activities. FSR may use or disclose PHI i) to a public health authority that is authorized by law to collect or receive such information for the purpose of

preventing or controlling disease, injury, or disability; ii) to report adverse events to the FDA and to track FDA-regulated products; iii) to notify a person that the person has been exposed to a communicable disease (if otherwise permitted by law to make this disclosure); iv) to notify an employer of medical information related to an employee if FSR related to limited functions for medical surveillance on behalf of the employer; or v) to a school about an individual who is a student or prospective student related to immunization.

Permitted Disclosure for Health Oversight Activities. FSR may disclose information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative or criminal investigations, proceedings, or actions; inspections; licensure or disciplinary actions; or other activities necessary for the appropriate oversight of the healthcare system; government benefit programs for which health information is relevant to beneficiary eligibility; entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance. FSR will disclose information to a health oversight agency for oversight activities only where the investigation arises out of the receipt of health care or a claim for or qualification for public benefits related to health or where health is an issue.

Permitted Disclosures about Decedents. FSR may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. FSR may also disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for the performance of the funeral director's duties, FSR may disclose information prior to, and in reasonable anticipation of, the individual's death.

Permitted Uses and Disclosures for Organ and Tissue Donation. FSR may use and disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating such use.

Research. FSR may disclose PHI for research purposes only where the requirements of 45 C.F.R. § 164.512(i) are met. All studies in which FSR participates are approved by the Institutional Review Board ("IRB"). The researcher physician may only disclose PHI as necessary to prepare a research protocol or for research purposes and may not remove any PHI from FSR during the course of the research. All IRB documentation associated with each research study is maintained by the Privacy Officer.

Permitted Uses and Disclosures for Specialized Government Functions. FSR may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.

FSR may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign authorities as above.

FSR may disclose PHI to authorized federal officials for the conduct of lawful national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq*.) and Executive Orders.

FSR may disclose PHI to authorized federal officials for the provision of protective services to the President and others, or for the conduct of investigations, as required by law.

FSR may disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual PHI about such inmate or individual, if the correctional institution or law enforcement official represents that the information is necessary for provision of health care to such individuals; the health and safety of such individual or other inmates; the health and safety of the officers, employees, or others at the correctional institution; the health and safety of such individuals, officers, or others responsible for the transporting of inmates; law enforcement on the premises of the correctional institution; and the administration and maintenance of the safety, security, and good order of the correctional institution.

FSR may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Worker's Compensation. FSR may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.