

Table of Contents

Contents

Privacy Compliance Policies Introduction	2
Definitions	3
Policy 1: Communication and Handling of Protected Health Information	7
Policy 2: Physical Security Standards	11
Policy 3: Security and Confidentiality Away from a Facility Setting	14
Policy 4: Use and Disclosure of Protected Health Information	16
Policy 5: Verification of Identity and Authority of Requestor	22
Policy 6: Requesting the Minimum Necessary	24
Policy 7: Disclosing the Minimum Necessary	25
Policy 8: Using the Minimum Necessary	26
Policy 9: Designated Recordsets	27
Policy 10: Notice of Privacy Practice Policies	28
Policy 11: Retention and Disposal of Protected Health Information	30
Policy 12: Client Access to Protected Health Information	31
Policy 13: Amendments to Protected Health Information	34
Policy 14: Accounting of Disclosures	37
Policy 15: Complaints by Clients Related to Protected Health Information	39
Policy 16: Research	42
Policy 17: De-Identification of Protected Health Information	44
Policy 18: Information Systems	45
Policy 19: Business Associates	46
Policy 20: Workforce Member Personnel Files	48
Policy 21: Workforce Member Training	49
Policy 22: Sanctions for Breaches of Client Privacy	50

Privacy Compliance Policies

Introduction

Specific regulations have been established by the federal government to protect the privacy of individually identifiable health information. To comply with these regulations, Family Counseling Center of Missouri, Inc. (FCC) has adopted a set of policies and procedures to address our clients' privacy needs.

These policies and procedures are in accordance with the Privacy Rule, promulgated under the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Confidentiality of Alcohol and Drug Abuse Patient Records statute and its implementing regulations, 42 C.F.R. Part 2. The Privacy Rule applies to a wide variety of health plans and providers, called "covered entities." Family Counseling Center of Missouri, Inc. is a covered entity and, as such, is subject to HIPAA's Privacy Rule.

Family Counseling Center is also a federally assisted alcohol and substance abuse program and is therefore additionally subject to 42 C.F.R Part 2 regulations. Although the regulations of the Privacy Rule and 42 C.F. R. Part 2 (Federal Confidentiality Regulations) are similar, they are not identical; in cases where rules conflict, Family Counseling Center will follow the more stringent set of rules.

Privacy Compliance Definitions

Definitions:

Breach: A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Business Associate: A person who acts in a capacity other than as a member of the workforce of a practice to perform or assist in the performance of a function or activity involving the use or disclosure of confidential information, or any other function or activity otherwise governed by the Privacy Rule. The term “business associate” does not include any member of the FCC workforce.

Examples of activities or functions that may be performed by a business associate of a practice include: claims processing or administration, data analysis, processing or administration, quality assurance, billing, and practice management. Business associates may also include persons who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to practices, if confidential information is received from the practice in the course of providing such services.

Client: The person who is the subject of protected health information (PHI) or that person’s personal representative. If the person is an adult and state law permits, the personal representative can be a court-appointed guardian or power of attorney. If the person is an unemancipated minor, the personal representative can be the parent or legal guardian. If the minor is a participant in a substance abuse program the minor can consent on his or her own behalf under the state law. If the person is a deceased client, the personal representative can be the executor, administrator, or other person allowed to act on behalf of the deceased client’s estate. A person becomes a client upon the first delivery of services by FCC (the initial moment of contact between an FCC workforce member and the person).

Complaint: Allegation that a client’s protected health information has been improperly used or disclosed. A client may file a complaint. The original complaint form is placed in the client’s clinical records.

Covered Entity or Entities: A health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Designated Licensed Health-Care Professional (LHP): The individual designated by the covered entity who is a licensed health care professional and who will not participate in any initial decisions to deny or grant access to PHI, but who will review all requests for access denied on reviewable grounds as established by the Privacy Rule.

Designated Record Set (DRS): A group of records maintained by or for a covered entity that satisfy items below. (Note that “or” not “and” is employed after item 2).

1. The medical records (including mental health records) and billing records about clients maintained by or for a covered health care provider;
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
3. Used, in whole or in part, by or for the covered entity to make decisions about clients.

Disclosure: Externally divulging/releasing PHI, created or possessed by the covered entity, in any manner.

Health Care Clearinghouse: A public or private entity that processes, or facilitates the processing of, PHI in a nonstandard format (or containing nonstandard data elements) into standard data elements or a standard transaction, and vice-versa.

Health Care Provider: A provider of health care services (e.g., mental health facility and its staff, hospital) that furnishes, bills, or is paid for health care in the normal course of business.

Health Care Operations: The activities of a covered entity that cause it to be categorized as a health care provider, health plan, or health care clearinghouse. Such activities include, but are not limited to, the following: (a) quality improvement including outcomes evaluation; (b) development of clinical guidelines; (c) protocol development; (d) case management and care coordination; (e) communication with providers and client about treatment alternatives; (f) review of competence or qualifications of health professionals; (g) training programs for students and practitioners; (h) provision of legal services; (i) fraud and abuse auditing and compliance programs; (j) business planning and development, management, and administration; (k) fund-raising for the benefit of the covered entity; (l) marketing for which authorization is not received; and (m) due diligence functions.

Health Oversight Agency: A governmental agency or authority, or designee, that is authorized by law to oversee the public or private health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights for which health information is relevant.

Inmate: A person who is confined in a correctional institution, such as a prison, jail, reformatory, work farm, detention center, home detention or halfway house.

Marketing: Making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service.

Marketing does not include communications that are made by a covered entity:

1. For the purpose of describing the entities participating in a healthcare provider network or health plan network, or for the purpose of describing if a product or service (or payment for such a product or service) is provided by the covered entity or included in a benefits plan;
2. That are tailored to the circumstances of a particular client and the communications are:
 - a. Made by a health care provider to a client as part of the client’s treatment; or

- b. Made by a health care provider or health plan to a client in the course of managing that client's treatment or for the purpose of recommending alternative treatments, therapies, health care providers, or settings of care.

The following also are not considered marketing:

1. Any face-to-face communication made by the covered entity to the client; or
2. A promotional gift of nominal value provided by the covered entity.

Minimum Necessary Provisions: The Privacy Rule requires a covered entity to make reasonable efforts *not* to use, disclose, or request from another entity more than the "minimum amount of confidential information necessary" to accomplish the intended purpose of the use, disclosure, or request taking into consideration practical and technological limitations.

Organized Health Care Arrangement: (a) A clinically integrated setting where health care is provided by more than one health care provider; or (b) an organized system of health care in which more than one covered entity (i) holds itself out to the public as participating in a joint arrangement, and (ii) participates in at least one specified joint activity either for each other or by a third party on behalf of each other.

Notice of Privacy Practices (NPP): This notice states that the covered entity will protect the privacy of identifiable health information in compliance with federal and state laws governing the use and disclosure of protected health information. To that end, FCC requires that all clients will be given a Notice of its Privacy practices-

Payment: (a) Activities undertaken by a health plan to collect premiums or determine benefits under the health plan; (b) activities undertaken by a health care provider in order to obtain reimbursement for health care services; or (c) any of the following activities: determining eligibility and adjudicating and subrogating claims; risk adjusting amounts due based on health status and demographics; billing, claims management, collection or obtaining payment under a reinsurance contract, and related data processing; reviewing PHI with respect to medical necessity or justification of charges; utilization review (UR) activities; or disclosure to consumer reporting agencies for collections.

Privacy Rule: The standards for privacy of individually identifiable health information issued by the Department of Health and Human Services on December 28, 2000 (45 C.F.R. 824.26 *et seq.*), as may be amended from time to time (most recent update August 14, 2002).

Protected Health Information (PHI): Individually identifiable information that was created, or received, by a covered entity and has been transmitted in any form or medium (i.e., on paper, electronically, or orally). The information must concern (a) the past, present, or future physical or mental health or condition of a client, (b) the provision of health care to a client, or, (c) the past, present, or future payment for the provision of health care to a client. Finally, the information must either identify the client or create a reasonable basis to believe that the information (including demographic information) can be used to identify the client.

EPHI: Electronic Protected Health Information, or ePHI, is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media, including computers, laptops, disks/CDs/DVDs, memory sticks, PDAs, servers, networks, dial-modems, email, web-sites, etc. EPHI is protected by Federal HIPAA legislation. EPHI is sometimes called "HIPAA data."

Psychotherapy Notes: Notes kept by a mental health professional that analyze conversations during a counseling session AND that are kept separate from the rest of the client's record. *(FCC does not define its regular case notes as psychotherapy notes but rather as progress notes. FCC strongly discourages the use of psychotherapy notes as defined above).*

Public Health Authority: An agency or authority of the United States, a state, territory, or Indian tribe that is responsible for public health matters as part of its official mandate. This includes a person or entity acting under a grant of authority from or contract with a public health agency. For example, state, city or county health departments and the Center for Disease Control and Prevention are public health authorities.

Public Official: A person who has been legally elected or appointed and who has been empowered by law/regulation to exercise the duties and functions of their office for the public good.

Secretary: The Secretary of the Department of Health and Human Services or his/her designee.

Treatment, Payment, and Health Care Operations: See above and below for definitions. Often abbreviated **TPO**.

Treatment: The provision, coordination, or management of health care and related services, consultation between providers relating to a client, or referral of a client to another provider for health care.

Use: The sharing, employment, application, utilization, examination, or analysis of PHI internally.

Verification: Process to verify the identity of a person requesting PHI and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity. The process must include obtaining any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement or representation is a condition of the disclosure under this subpart.

Workforce member: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the entity.

Policy 1: Appropriate Communication or Handling of Protected Health Information

Policy

This policy provides guidelines regarding the communication and handling of protected health information. This policy addresses only the most common situations that may arise and is not intended to be all-inclusive. How Family Counseling Center workforce members appropriately communicate or handle protected health information will frequently depend upon the surrounding facts and circumstances and the workforce members' roles in Family Counseling Center. Common sense must be applied in each case. The application of this policy should not endanger the safety or care of Family Counseling Center clients.

Procedure

Face-to-Face Communications Among FCC Workforce Members

FCC workforce members may discuss the client's PHI with each other only if it is necessary for the purposes of treatment, payment, or health care operations and is consistent with the workforce member's job duties. Otherwise, any PHI concerning any client should be held in the strictest confidence unless the client first signs an authorization (e.g., for marketing purposes). Even with a signed authorization, the minimum necessary standard will apply.

A client's PHI should not be discussed in any public place or area where it might be inappropriately overheard (e.g., waiting areas, staff break rooms/lounges, hallways, group settings in residential facilities including kitchens and living rooms, public transportation). In emergency situations during which workforce members must discuss a client's PHI in public areas, workforce members should stand aside and use low voices so that their discussion will not be overheard.

Face-to-Face Communications with Non-FCC Persons

Conversations with persons involved in a client's health care treatment, such as family members, relatives, close personal friends, or other persons identified by the client, should occur only after the client has given his or her written authorization, except in emergency situations. (Refer to FCC Policy and Procedures manual, CR-13 and CR-23 and Privacy Compliance Policy Number 4).

The appropriateness of a conversation involving PHI will ordinarily depend upon the surrounding facts and circumstances. Each FCC workforce member who communicates PHI in a face-to-face conversation with another person is responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent practicable without interfering with the intended purpose of the communication. At a minimum, the workforce member should:

1. Verify the identity of the person requesting the PHI (see Privacy Compliance Policy 5);
2. Once identity has been verified, follow procedures for disclosure of PHI in Privacy Compliance Policy 4 and for use/disclosure of minimum necessary in Privacy Compliance Policies 7 and 8.

Conversations should take place in areas where they will not be overheard.

Procedures Relating to Interpreters or Sign Language: Professionals who provide sign language or interpreting services to FCC clients should follow the same policies as FCC workforce members. This means that, when interpreting or using sign language where PHI may be transmitted, the most private setting available, out of hearing or view of others, will be used.

Face-to-Face Communication with Clients

Face-to-face communications with clients where PHI is revealed should take place in private areas. If clients attempt to discuss PHI with FCC workforce members in public areas, workforce members should redirect to secured areas or end the conversation.

Emergency Situations

If the client is unable to provide his or her written authorization because of an emergency situation (e.g., client is psychotic or unconscious), the workforce member may use his or her professional judgment and experience to make reasonable inferences if it is appropriate or is in the best interest of the client to disclose the PHI to another person.

1. In cases where professional judgment is required, FCC workforce should discuss with a designated supervisor(s) familiar with these guidelines prior to releasing PHI;
2. If deemed necessary to release PHI, only the PHI directly relevant to the person(s) involvement with the client's health care should be disclosed.

In addition, see Privacy Compliance Policy 4 (disclosure without authorization) and FCC Policy and Procedures manual, CR-23-24.

Telephone Communications

Telephone communications concerning a client's PHI are governed by the same rules as those discussed above for face-to-face communications. The appropriateness of telephone communications involving PHI will ordinarily depend upon the surrounding facts and circumstances.

Each FCC workforce member who communicates PHI over the telephone to another person is responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent practicable without interfering with the intention of the communication.

When making or receiving telephone calls regarding PHI, workforce members should be in secured areas (e.g., private office with door shut, area designated "staff only") whenever possible. If it is not possible to be in a secured area, workforce members should use a low voice and should not repeat individual identifying information. (Workforce members may use clients' names, but it is preferable to avoid using last names whenever possible).

When FCC Workforce Members Receive Phone Calls Requesting PHI

The workforce member should follow the steps below.

1. Verify the identity of the person requesting PHI by
 - a. Voice recognition (See Privacy Compliance Policy 5);
 - b. A call back procedure (See Privacy Compliance Policy 5);
 - c. Provision of client identification (e.g., account number for billing purposes).
2. Check to determine if a release for information (authorization) has been signed; however, do not reveal client's receipt of FCC services at this point.
3. If the authorization has been signed, then the information may be given to the requesting party, following procedures in Privacy Compliance Policy 4.
4. If authorization has not been signed, the workforce member's response depends upon the type of services the client is receiving.
 - a. If the client is receiving drug and alcohol services, then the workforce member informs the caller that Federal Confidentiality Regulations prevent him/her from acknowledging the client's participation in FCC services. (Refer to FCC Policies and Procedures manual, CR-6a).
 - b. If the client is receiving mental health services *only*, then the workforce member informs the caller that

- i. FCC policy requires a written authorization for release of PHI; however,
- ii. The workforce member will check with his/her supervisor and/or the client to determine if the request can be fulfilled.
- iii. The workforce member should *not* indicate, under these circumstances, that Federal Confidentiality Regulations prohibit release of PHI about the client.

Facsimile Communications

Facsimile communications are also subject to the same rules as those discussed above for face-to-face communications and telephone communications. The appropriateness of facsimile communications of PHI will also depend upon the surrounding facts and circumstances. As with telephone conversations, each FCC employee who communicates PHI over a facsimile machine is responsible for ensuring that the communication is reasonably designed to protect the PHI to the greatest extent practicable without interfering with the intended purpose of the communication.

At a minimum, the workforce member should:

1. Verify the identity of the person requesting the facsimile containing the PHI (See Privacy Compliance Policy 5).
2. The fax cover sheet shall not contain PHI
3. Check to determine if authorization has been signed; however, do not reveal client's receipt of FCC services at this point.
 - a. If authorization has been signed, then the information may be faxed to the requesting party, following procedures in Privacy Compliance Policy 4 and step 3 below.
 - b. If authorization has not been signed, then the workforce member follows the guidelines listed under "When FCC Workforce Members Receive Phone Calls Requesting PHI," item 4.
4. Providing that an authorization has been signed, the FCC workforce member confirms that
 - a. The facsimile number is correct. If the fax number has not been previously confirmed, this may be done through a phone call or sending an initial test fax.
 - b. The facsimile machine is in a secure location, not accessible to unauthorized individuals. (FCC's facsimile cover sheet statement references this requirement).

Other Facsimile Regulations

1. Facsimile cover sheets should use the confidentiality language below.

This information has been disclosed to you from records which are confidential and protected by federal law. Federal regulations (42 C.F. R. Part 2) prohibit you from making any disclosure of this information without the specific written authorization from the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical or other information is not sufficient for this purpose.

The information transmitted is intended only for the person or entity to which it is addressed. Law prohibits any review, retransmission, dissemination, re-disclosure, or any use of this information by persons or entities other than the intended recipient. If you received this in error, please contact the sender immediately via telephone to arrange for return its return to us.

2. Fax numbers should be reconfirmed annually. Designated FCC workforce members will engage in the reconfirmation process during a designated month each year. Results will be completed on the appropriate form and submitted to the privacy office.

3. Whenever possible, fax numbers that are programmed into the fax machine should be programmed by a single designated FCC workforce member to minimize misdirected facsimiles.
4. When a new number is programmed, a test facsimile should be sent requesting that the receiving party send it back with a date and signature verifying the number or with a confirming phone call.
5. If FCC sends a facsimile in error, reasonable efforts to contact the receiver should be undertaken to have the item faxed in error returned (or destroyed, if it is not possible to return the item) to protect from further disclosures. Notation should be made in the client's clinical record about the erroneous transmission when appropriate.
6. If FCC receives a facsimile transmission that is believed to have been sent in error, reasonable efforts to contact the sender should be undertaken and the material returned, to destroy the document, or to follow the instructions of the entity from which the facsimile was received.
7. Because PHI is often of a highly sensitive nature, mailing requested PHI is preferable to faxing, when time permits.

Electronic Communications

The transmission of ePHI by email or other means of electronic communication must be in a fully encrypted form. The FCC email system is not secure, therefore ePHI is not to be shared unless encrypted. The Security officer may be contacted for more information.

Required Confidentiality Agreement

FCC workforce members who receive or maintain PHI will be required to agree to the protection of PHI in accordance with the Privacy Rule and FCC policies pursuant to these regulations. They will sign a confidentiality agreement, which will be maintained in their personnel file.

Visitors and Confidentiality

Visitors to an FCC site are not required to sign the confidentiality agreement. However, a copy of the confidentiality agreement will be located next to the visitor sign-in materials at designated sites to be available for each visitor's review.

Policy 2: Physical Security Standards

Policy

Family Counseling Center is committed to helping to protect the confidentiality and privacy of Family Counseling Center data assets. Family Counseling Center will establish rules and procedures of how to develop and maintain physical security standards, in order to ensure that all workforce members maintain a secure work area.

Procedure

Security of PHI

PHI that is potentially within view of others, even if FCC workforce members are present, should be protected in a manner that such information is not communicated to persons without authorized access to this PHI. All documentation containing PHI should be maintained out of the view of unauthorized persons.

1. Where feasible, workstations will be positioned or shielded so that computer screens are not visible to the general public or unauthorized workforce. Where practical, copiers will be located in areas that are not accessible to the public. Fax machines will be located in secure areas. Output from these devices should be monitored to ensure that it is promptly delivered to the intended party.
2. While working with PHI, workforce members will keep the documentation within line of sight or within arm's reach.
3. FCC workforce members will secure their work areas when unattended. This includes breaks, lunch periods, or any other times that work areas are vulnerable to "snooping." In areas that have been identified as accessible to the public, offices should be locked when unoccupied. Where no doors are present in work areas, desks should be kept free of clutter, and all documents should be placed in drawers or cabinets (preferably locked).
4. Users will secure media (such as hard copy, diskettes, etc.), which contain confidential information according to Privacy Policy 11, Retention and Disposal.
5. FCC management will provide users with mechanisms (shredders, secured bins, etc.) for proper disposal of confidential printouts. Users will dispose of printouts at each program site. (See Privacy Policy 11).
6. Users will print documents only when necessary.
7. Copying of confidential documents will be minimized.
8. Users of electronic devices will follow IT Acceptable Use Policy to adhere to physical security standards.
9. Management and users will take any other reasonable and logical measure necessary to maintain a secure work area, even if this measure is not specifically enumerated above.

Lost or Stolen PHI/ePHI

If PHI/ePHI is lost or stolen, the privacy officer or designee should be notified immediately.

Any lost or stolen PHI/ePHI is to be handled in accordance with the Breach Notification rule of the HITECH Act.

Breach Notification

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- **Individual Notice**

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- **Media Notice**

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- **Notification by a Business Associate**

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no

later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

Policy 3: Ensuring Confidentiality of Protected Health Information for FCC Staff Working Away from a Facility Setting

Policy

In compliance with the Privacy Rule, Family Counseling Center policy protects clients' protected health information when Family Counseling Center workforce members are working away from a facility setting (including their homes) or are traveling. (See also Privacy Compliance Policy 2 on Physical Security Standards).

Procedure

General Requirements

1. When FCC workforce members travel in the field or are working from their home, they will take only PHI necessary to carry out their duties.
2. If client clinical records are checked out from an FCC site, then the policy for each facility should be followed.
3. PHI shall be transported in a locked portable storage device.
4. PHI that is potentially within view of others, even if FCC staff is present, will be protected in a manner that such information is not communicated to persons without authorized access to this PHI.
 - a. While working with PHI, the FCC workforce member will keep the documentation within line of sight or within arm's reach;
 - b. This documentation will be viewed in the most private settings available;
 - c. Only PHI documentation necessary for the task at hand will be in view;
 - d. Containers storing PHI will remain closed when not in use;
 - e. When having PHI material copied, the FCC workforce member will ensure that this material is viewed only by authorized persons.
5. Phone calls that involve PHI should take place in the most private settings available.
6. If possible, phone calls should not be made or received on cordless phones. If cordless phones are used, the workforce member should avoid using a client's last name or revealing other identifying information.
7. Upon FCC workforce members leaving an area where there are materials containing PHI, the workforce members will take the materials with them. If this is not practical or possible, they will ensure that the area is protected from viewing by those without authorization by
 - a. Locking the area;
 - b. Informing the facility that no one outside of FCC authorized workforce members is allowed to view the material; or
 - c. Some other reasonable intervention.
8. If PHI in any form is lost or stolen, the privacy officer or security officer must be informed immediately, not to exceed one business day, in order to initiate a mitigation process. (See Privacy Compliance Policy 2).

Procedures Relating to Vehicles

1. Vehicles containing any PHI will be kept locked while unoccupied. PHI will be kept locked in the trunk of the vehicle, when possible, and always stored in a designated locked portable storage device.
2. All PHI within a vehicle will be maintained so as to protect from plain view through windows of the vehicle.
3. In the event of a vehicle accident, any FCC workforce member who suspects there is PHI in the vehicle will make every reasonable attempt to make sure that the PHI is not accessible to

anyone who does not need to have access to it, after assuring the health and safety of any individual(s).

4. PHI shall not be stored in vehicles overnight.

Procedures Relating to Electronic Devices Used Off-Site

1. Electronic devices containing PHI should not be left unsecured in your absence.
2. Any documentation or equipment such as computers, laptops, disks/CDs/DVDs, memory sticks, PDAs, servers, networks, dial-modems, email, web-sites, etc. that may contain ePHI will be secured from access by those without authorization to ePHI. This stipulation covers all locations, including an FCC workforce member's home.
3. Any laptops or portable devices containing ePHI are to be fully encrypted.

Procedures Relating to Facsimile Machines Used Off-Site

Because PHI is often of a highly sensitive nature, mailing requested PHI is preferable to faxing, when time permits. If faxing is necessary, then the following apply:

1. When sending or receiving a fax containing PHI, the workforce member will ensure only those authorized to view have access to the material during the process of transmission;
2. The fax cover sheet will not contain PHI;
3. The workforce member will be waiting to receive the fax at the fax machine when transmission is expected, if the material could be accessed by those without authorization to view the PHI.

Policy 4: Use and Disclosure of Information

Policy

Family Counseling Center provides both mental health and drug and alcohol treatment and is therefore subject to the Health Insurance Portability and Accountability Act (HIPAA) as well as Federal Confidentiality Regulations (42 C. F. R. Part 2). While Federal Confidentiality Regulations apply only to drug and alcohol protected health information, Family Counseling Center has elected to adhere to its provisions for all of our clients.

Family Counseling Center's policy provides for the client's voluntary written authorization for use or disclosure of his/her protected health information. In limited circumstances, a client's PHI may be released without a client's written authorization. Protected health information for clients receiving mental health treatment *only* is subject to less stringent restrictions than the PHI of clients receiving drug and alcohol treatment. As a result, the circumstances under which the PHI of mental health clients may be released without a client's written authorization are broader than those of PHI governed by Federal Confidentiality Regulations.

After studying the Privacy Rule and Federal Confidentiality Regulations, Family Counseling Center has chosen to define "*consent*" as a broad, general permission by the client to Family Counseling Center to treat him or her and to define "*authorization*" as a more specific, detailed permission by the client to Family Counseling Center to use/disclose protected health information. Authorizations have core requirements that are listed in this policy.

Procedures for Clients Receiving Drug and Alcohol Treatment

General Procedures for Use and Disclosure

1. FCC may not use or disclose PHI without a valid authorization completed by the client, with limited exceptions.
2. When FCC workforce members receive an initial request to disclose PHI, they should obtain written information regarding the identity of the requestor, the date of the request, the nature and purpose of the request, and any authority that the requestor has to request such information, as detailed in procedures listed below. Additional disclosures requested by the same party and regarding the same PHI do not require new written requests, providing that an original, valid authorization has been signed.
3. If unauthorized FCC workforce members receive a completed authorization form for the release of PHI, they will direct it to the client's therapist or program director.

Disclosure of Requested PHI with an Authorization

1. When an FCC workforce member receives a request to disclose PHI, he/she should reference the client's clinical record to determine if an authorization for the request for disclosure is present. The workforce member will not, at that point, indicate the client's presence in treatment. (The requesting party may be a third party or the client him/herself).
2. If an authorization is present, the workforce member will verify that the request for disclosure matches the information authorized to be released.
 - a. If the request for disclosure matches the authorization, the workforce member will disclose the information. If the request for disclosure does not match the current authorization, the workforce member must contact the client to obtain an authorization specific to the request for disclosure.
 - i. Provided the client agrees and completes a new and appropriate authorization form, the workforce member will disclose the information.

- ii. If the client does not agree, the workforce member will inform the requesting party that the information cannot be disclosed.
- 3. If an authorization is not present, the workforce member will discuss the request for disclosure with the client to determine whether the client agrees to disclose the information.
 - a. If the client chooses to authorize the disclosure, the workforce member will develop an authorization form specific to the request; the client will sign the authorization, and the authorized information will be disclosed.
 - b. If the client chooses not to sign an authorization or if the client is not available, the workforce member must contact the requesting party and inform that party that Federal Confidentiality Regulations prevent him/her from acknowledging the client's participation in FCC services.
- 4. When PHI is disclosed for purposes other than treatment, payment, or health care operations, the workforce member must document the disclosure via the Accounting of Disclosures form (See Privacy Compliance Policy 14).

Authorization Required for Photographing, Videotaping, or Recording

FCC must obtain a client's written authorization before photographing, videotaping, or recording that client for internal administrative or clinical use.

Situations in Which PHI May Be Used Without Authorization

PHI may be *used without authorization* by FCC for internal purposes listed below.

- 1. *For internal treatment*
Workforce members may use client information in order to make decisions about treatment (e.g., to provide the client with information about or recommendations of possible treatment options or alternatives that may interest the client, to inform the client about mental health benefits or services).
- 2. *For quality improvement activities*
 - a. FCC may use client information for quality improvement activities. Quality improvement activities are classified as health care operations and include client satisfaction surveys; peer review; clinical supervision; clinical staffing; use of incident, accident, against staff advice and noncompliance discharge reports; administrative reports; and auditing. (See FCC's Policy and Procedure manual, QI section).
 - b. FCC indicates in its Notice of Privacy Practices that it may use PHI for QI activities. While these activities are considered health care operations and therefore do not need authorization, FCC's use of PHI for QI activities is subject to the client's right to restrict the use of his/her PHI. This request to restrict must be made in writing.
 - c. A minimum necessary standard regarding workforce member access in these activities applies. (See Privacy Compliance Policy 8).

Situations in Which PHI May Be Disclosed Without Consent or Authorization

PHI may be *disclosed without consent or authorization* only in the following situations:

- 1. To medical personnel when necessary to meet a medical emergency or the client is incapacitated and information from the client's clinical records is needed by medical personnel to make sound determination regarding emergency care;
 - a. In any case where PHI was disclosed in an emergency treatment situation, written authorization must be presented to the client for signature as soon as practicable.
 - b. If the client refuses to sign an authorization, such refusal should be documented in the client's clinical record. (See FCC Policy and Procedures, "Medical Emergencies").

2. To the intended victim or law enforcement in order to avert a serious threat to health and safety that are described in the Tarasoff requirements (See FCC Policy and Procedures, section CR-13);
3. To a public health authority (e.g., a public health official who is legally authorized to obtain or receive information related to cause of death for purposes of laws requiring or authorizing collection of vital statistics);
4. To report child abuse/neglect situations. (*Note: Missouri law mandates reporting of child abuse/neglect*);
5. To report elderly or disabled abuse/neglect/financial exploitation;
6. To report to governmental authority authorized to receive such reports other situations involving abuse, neglect, or domestic violence but only if:
 - a. The client agrees to the disclosure; or
 - b. FCC is expressly authorized by statute or regulation to disclose the PHI, and FCC believes that the disclosure is necessary to prevent serious harm to the client or other persons; or
 - c. The individual is incapacitated, and a law enforcement official has informed FCC that an immediate enforcement activity depends upon the disclosure and that waiting for the client to regain capacity would materially and adversely affect the enforcement activity.
7. To the Food and Drug Administration (FDA). This applies if the client is subject to the jurisdiction of the FDA with respect to an FDA regulated product or activity for which that person has responsibility, for the purpose of activities related to quality, safety, or effectiveness of such FDA regulated products or activity (e.g., collecting or reporting adverse regulated products; enabling product recalls, repairs, replacement or look back; or conducting post marketing surveillance);
8. To a health oversight agency to conduct activities authorized by law, but only to access PHI for clients they fund. This includes officials who conduct an audit or evaluation of the program on behalf of
 - a. Any federal, state or local governmental agency that provides financial assistance to the program or is authorized to regulate the program;
 - b. Third-party payers covering clients in the program or peer review organizations performing a utilization or quality review (however, for all other purposes, FCC may require an authorization to release PHI to third-party payers); or
 - c. An authorized person determined by the director of the program to conduct audit or evaluation activities. Records may not be copied or leave the premises unless the person removing the records agrees, in writing, to secure the records and destroy them upon completion of the audit or evaluation;
9. To judicial or administrative proceedings, when a court order accompanied by a subpoena or other legal mandate compels disclosure;
 - a. The court order must be for a specific, limited purpose: to authorize the disclosure or use of client information that would otherwise be prohibited under the 42 C. F. R. Part 2 rule;
 - b. The court order may compel disclosure of a client's confidential communication to a substance abuse program, but only if the disclosure is necessary to:
 - i. Protect against an existing threat to life or of serious bodily injury, including senior, disabled and child abuse and neglect, and/or financial exploitation
 - ii. Investigate or prosecute an extremely serious crime; or
 - iii. Litigate in a proceeding in which the client offers testimony or other evidence pertaining to the content of the confidential communication.

- c. The amount of information disclosed must be limited to the minimum necessary.
10. To law enforcement that is directly related to a client's commission of a crime on the premises or against program personnel (or the threat to commit such a crime) and limited to the circumstances of the incident;
 11. To enable specialized governmental functions (e.g., national security, determination of eligibility for veterans benefits);
 12. For research activities as pursuant to Privacy Rule 164.512(i)(B) and 164.508;
 13. By whistleblowers. If a workforce member or business associate believes in good faith that FCC has engaged in conduct that is unlawful or otherwise violates professional standards, or the care, services, or conditions provided potentially endangers clients, workforce members, or the public, the workforce member or business associate may disclose PHI, but only to a public health authority, health oversight agency, or health care accreditation organization authorized to investigate or oversee the conduct at issue;
 14. To facilitate disaster relief;
 15. As required by law.

Any questions as to whether a use or disclosure is permitted or required by law should be directed to the appropriate program director or to the privacy officer.

Procedure for Disclosing Information That Does Not Require Written Consent or Authorization:

When information that does not require consent or authorization is requested by an outside entity, the following procedure should be used:

1. Except in the case of emergency, requests for PHI should be made in writing by the requesting person or entity.
2. The request for PHI should be forwarded to the client's therapist or program director for review.
3. The therapist or program director should determine whether the disclosure may be made without the client's consent or authorization. If it is determined that a release may be made without the consent or authorization of the client, the therapist or program director shall contact the requesting party and provide the applicable information.
4. If a request asks for information that cannot be disclosed without the consent or authorization of a client in addition to information that can be disclosed without the consent or authorization of the client, the therapist or program director is responsible for limiting the disclosure only to information that may be released without a consent or authorization.
5. Any disclosure made must be the minimum information necessary to achieve the purpose of the disclosure.
6. The disclosure must be documented in writing in the client's clinical record and include detailed information about the information disclosed.
7. The client will be informed that disclosure has been made, unless the therapist or program director believes it is not in the best interest of the client to inform him/her.
8. At any point, the therapist or program director may consult with the privacy officer or associate director with regard to this procedure.
9. When PHI is disclosed for purposes other than treatment, payment, or health care operations, the workforce member must document the disclosure via the Accounting of Disclosures form. (See Privacy Compliance Policy 14).

Core Elements of Authorization

Authorization must contain at least the following:

1. Description of the information to be used or disclosed with sufficient specificity;
2. Name/identification of the person(s) or class of persons authorized to use/disclose the PHI;
3. Name/identification of the person(s) or class or persons to whom FCC is authorized to make the use/disclosure;
4. Description of each purpose of the requested use/disclosure;
5. Expiration, by date, specific time period or an event relevant to the client or the purpose of the use or disclosure (statement “none” or “at the end of the research study” is sufficient where authorization is for research data base repository);
6. Signature of the client and date; if signed by a personal representative, a description of the representative’s authority to act for the client;
7. A statement regarding the client’s right to revoke the authorization and a description of how the client may revoke the authorization or a reference to the FCC’s Notice of Privacy Practices where such information is contained;
8. Either a statement that FCC may not condition treatment, payment, enrollment, or eligibility on obtaining the authorization or, when FCC may so condition treatment, payment, enrollment, or eligibility, a statement setting forth the consequences to the individual of refusing to sign the authorization;
9. The potential for information disclosed pursuant to the information to be subject to redisclosure by the recipient without further protection under the regulations;
10. Authorization must be written in plain language;
11. If FCC seeks an authorization from a client for a use or disclosure of PHI, FCC must provide a copy of the signed authorization to the client at the client’s request.

Compound Authorizations

Authorizations for use/disclosure of PHI may be used in combination only as follows:

1. Within a research study, an authorization may be combined with other kinds of written permission for that same study;
2. With regard to psychotherapy notes, an authorization for use/disclosure may only be combined with another authorization for a use/disclosure of psychotherapy notes. (Note: FCC strongly discourages the use of psychotherapy notes. See definition of psychotherapy notes);
3. Authorizations other than for use/disclosure of psychotherapy notes may be combined, provided that FCC has not conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on obtaining one or more of the authorizations.

Prohibition on Conditioning of Authorizations

FCC may *not* condition provision of treatment, payment, enrollment, or eligibility for benefits on provision of an authorization except in the following situations:

1. Treatment related to research;
2. Risk determination or pre-enrollment underwriting (excluding authorizations for use/disclosure of psychotherapy notes).

When Authorizations Are Not Valid

An authorization is not valid under the following conditions:

1. When the authorization is known to contain false information;
2. When the expiration date is known to have occurred;

3. When required elements are missing, or there is incomplete information for a required element(s);
4. When the authorization is known to have been revoked;
5. If the authorization does not meet the requirements regarding compound authorizations or conditioning of authorizations.

Revocation of an Authorization

A client may revoke an authorization provided under this policy at any time, provided that the revocation is in writing, except to the extent that FCC has taken action in reliance on the authorization.

Procedures for Clients Receiving Mental Health Treatment Only

Generally, the protected health information of clients receiving only mental health treatment should be handled according to the policy and procedures above. However, since such records are not subject to Federal Confidentiality Regulations, the HIPAA Privacy Rule allows PHI to be released without the client's written authorization for treatment, payment, and health-care operations. If FCC workforce members receive a request for PHI for which there is no written authorization (e.g., a request from a third party payer or a referral source), they should inform the requesting party that

1. FCC policy requires a written authorization; however,
2. They will check with their supervisor and/or with the client to determine if the request can be fulfilled.

Under these circumstances, workforce members should *not* indicate that Federal Confidentiality Regulations prohibit their releasing PHI about the client.

Policy 5: Verification of Identity and Authority of Requestor

Policy

Prior to disclosing individually identifiable protected health information to third parties, Family Counseling Center workforce designees will verify the identity of the requestor and ensure that the requestor has the proper authority to request such information.

Procedure:

1. The client must sign a valid authorization for the disclosure of confidential PHI before such PHI can be released, except in accordance with existing HIPAA requirements. (See Privacy Compliance Policy 4).
2. All requests for disclosure will be forwarded to the appropriate workforce member and will include the following:
 - a. The name of the requesting party or parties; and
 - b. Any documentation, statements, or representations from the person requesting the PHI of his/her authority to request such information.
3. The client must present identification prior to receipt of any records regarding him/herself.
4. If the requesting party is someone other than the client, the FCC workforce member may rely on the following information to demonstrate identity:
 - a. Presentation of agency identification, credentials or other proof of government status (a badge, identification card, etc.);
 - b. A written request on agency letterhead or an oral statement if a written statement would **not** be possible (e.g., a natural disaster, other emergency situations);
 - c. If the disclosure is requested by a person acting on behalf of a public official, a written statement on government letterhead that the person is acting under the government's authority, or a contract or purchase order evidencing the same;
 - d. A court order; or
 - e. A driver's license or other valid photo identification, if the requesting party is a private individual.
5. The FCC workforce member will verify identity of any phone requests from all individuals, including law enforcement officers, and other who have an official need for PHI by using:
 - a. Voice recognition (e.g., the caller's voice and authority are specifically known to the FCC workforce member);
 - b. A callback phone number procedure
 - i. When the caller represents an agency with which FCC frequently works, the FCC workforce member will ask for the agency's general number and call to verify the caller's identity;
 - ii. When the caller is a private individual, the FCC workforce member will ask the caller to attest to his/her identity or verify identity through information specific to client;
 - c. Provision of client identification (e.g., by an account number of billing purposes) before releasing information.
6. The FCC workforce member will verify facsimile number of any faxed requests (one time only). The main number of the sending agency will be called and the fax number verified, or a test fax sent. (See Privacy Compliance Policy 1).
7. The FCC workforce member who responds to the request is responsible for recording or copying verification information or obtaining badge number, etc., and for placing it in the client's clinical record.

8. The FCC workforce member may disclose information to the requestor if all requirements for use and disclosure are met.
9. The FCC workforce member will contact agencies or other entities for further verification of identity or authority to receive PHI, if necessary.
10. The FCC workforce member may deny access to information, if verification of identity or authority is not accomplished. When this situation occurs, the FCC workforce member will notify the privacy officer or designee, who may assist in contacting the requesting party.

Policy 6: Requesting the Minimum Necessary

Scope of Policy

This policy applies to requests by Family Counseling Center workforce member for protected health information from other covered entities. This policy does not apply to disclosures or uses of protected health information, both of which are addressed in separate privacy compliance policies.

Policy

Family Counseling Center must limit its requests for protected health information to the amount reasonably necessary to accomplish the purpose for which the request is made when requesting such information from other covered entities. Family Counseling Center should not request a client's entire record except when the entire record is specifically justified as the amount of protected health information that is reasonably necessary to accomplish the purpose for which the protected health information is requested.

Procedure

1. When an FCC workforce member determines that PHI needs to be requested from another covered agency, he/she will discuss the request with the client to determine the minimum necessary information to accomplish the purpose for which the PHI is requested.
2. The client will sign an authorization request that approves the disclosure of the agreed upon minimum necessary PHI.
3. When the FCC workforce member receives the requested PHI, he/she will review it to determine if it follows the minimum necessary guideline.
4. If the received information exceeds the minimum necessary for the stated purpose, the FCC workforce member will return the unneeded information to the provider and will notify the client of the return.
5. At any time, FCC workforce members may consult their supervisor for guidance in determining the appropriate types and amounts of PHI to be requested.

Policy 7: Disclosing the Minimum Necessary

Scope of Policy

This policy applies only to disclosures of protected health information by Family Counseling Center to other covered entities. It does not apply to the use of, or request for, protected health information, both of which are addressed by separate privacy compliance policies.

Policy

The minimum necessary rule applies to all disclosures of protected health information by Family Counseling Center, except in the following situations:

1. Disclosures to a client that are permitted by the Privacy Rule;
2. Disclosures to a client that are required by the Privacy Rule and are pursuant either to the client's right to access his/her PHI or the client's right to an accounting of his/her PHI disclosures;
3. Disclosures pursuant to an authorization;
4. Disclosures to the Secretary of Health and Human Services for purposes of enforcing or ensuring compliance with the Privacy Rule;
5. Disclosures required by law;
6. Disclosures required by FCC to ensure its compliance with the Privacy Rule.

Procedures

FCC must limit its disclosure of PHI to the amount reasonably necessary to accomplish the purpose of the disclosure. FCC should not disclose a client's entire clinical record except when specifically justified as the amount of PHI reasonably necessary to accomplish the purpose for which the disclosure is sought. Unless its reliance would be unreasonable under the circumstances, FCC may (but is not required to) rely upon the scope of a requested disclosure as being the minimum necessary for the stated purpose in any of the following circumstances:

1. Requests by public officials for permitted disclosures, if the public official represents that the PHI requested is the minimum necessary for the stated purpose;
2. Requests by another covered entity;
3. Requests by a professional who is a business associate of FCC, if the professional represents that the PHI requested is the minimum necessary for the stated purpose; or
4. Requests for research purposes and the person making the request has complied with all of the required documentation and representations for a permitted disclosure for such purposes.

See Privacy Compliance Policy 4 for specific steps in disclosure.

Policy 8: Using the Minimum Necessary

Scope of Policy

This policy applies only to uses of protected health information by Family Counseling Center. This policy does not apply either to disclosure of, or request for, protected health information, both of which are addressed in separate privacy compliance policies.

Policy

The minimum necessary rule applies to all uses of protected health information by Family Counseling Center, except in the following situations:

1. Uses pursuant to an authorization (e.g., research);
2. Uses required by law, as long as the use is limited to the relevant requirements of such law;
3. Uses in emergency situations as defined by FCC Policy and Procedures manual, section CR-23-24.

Procedure

1. FCC workforce must limit its use of PHI to the amount reasonably necessary to accomplish the purpose of the use. FCC should not use or discuss a client's entire clinical record except when the entire clinical record is specifically justified as the amount of PHI that is reasonably necessary to accomplish the purpose for which the use is sought.
2. FCC workforce members should use PHI only in accordance to their position /job classification as described in FCC's Policy and Procedures manual.
 - a. For each position/job classification, this section identifies the categories of PHI to which such persons generally need access to perform their job functions and any conditions and/or limitations placed upon such persons' access.
 - b. FCC must make reasonable efforts to ensure that the persons or classes of persons identified in the manual access PHI only in accordance with the limitations stated therein.
 - c. FCC workforce members who hold more than one position /job classification should use a client's PHI only in accordance with that workforce member's job function being performed at the time he or she accesses the PHI.

Policy 9: Designated Record Sets

Policy

Records maintained by or for Family Counseling Center will be identified according to the definition of designated record set covered by Privacy Rule.

Procedure

Designated Record Set Contents

For the purpose of implementing this policy, the term “designated record set” includes any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for FCC for client care or payment decision-making, including but not limited to:

1. Clients’ clinical records, paper or electronic (See FCC Policy and Procedures manual, S-10);
2. Clients’ billing records;
3. Any records or information used, in whole or in part, by or for FCC to make decisions about clients.

Information Not Considered Part of Designated Record Set

Information that is *not* part of the designated record set is defined as follows: documents used for census information, certain quality improvement or quality assurance activities (e.g., client satisfaction surveys), state auditors, or various electronic databases, etc., which are not used to make decisions regarding individual clients.

Exclusive Possession of Designated Record Set

When an individual or department has been given sanctioned, exclusive possession and control of PHI as part of its assigned duties, the individual or department will be responsible for all administrative duties of a data trustee in terms of security, data access, privacy, data backup, disaster recovery and accountability. If the individual or department does not have the technical expertise or equipment to protect the PHI adequately, arrangements must be made for technical assistance to ensure the confidentiality of the PHI.

Retention and Disposal of Designated Record Set

Designated record sets will be created, stored, released, transported, copied, and destroyed in accordance with the appropriate privacy compliance policies outlined in this document.

Policy 10: Notice of Privacy Practices

Policy

This policy helps to ensure that clients are aware of their rights and responsibilities concerning the use and disclosure of their protected health information. These rights and responsibilities are detailed in Family Counseling Center's Notice of Privacy Practices.

Procedure

Contents of Notice of Privacy Practices

Plain Language and Required Statement: FCC's notice must be written in plain, easily understood language. It must prominently display the following statement:

This notice describes how medical and mental health-related information about you may be used and disclosed and, if applicable, how drug- and alcohol-related information about you may be used and disclosed. It also describes how you can get access to this information. Please review it carefully.

Uses and Disclosures: FCC's notice contains several descriptions of the required and permitted uses and disclosures of PHI, including:

1. A statement that most uses or disclosures will be made only with the client's written authorization and the client may revoke such authorization in writing (except to the extent that FCC has taken action in reliance on the authorization);
2. A description of any more stringent law than the Privacy Rule governing any particular use or disclosure of PHI (e.g., Federal Confidentiality Regulations); and
3. A description that is sufficiently detailed and includes at least one example of uses/disclosures permitted for treatment, payment, and health care operations;
4. A description that is sufficiently detailed of each of the other purposes that FCC is permitted or required to use or disclose PHI without a client's written authorization.

Contacting Clients: A statement that FCC may provide reminders of appointments and information about other treatment alternatives or benefits.

Individual Rights: A list of a client's rights with respect to PHI and a brief description of how a client may exercise such rights, including the right:

1. To request restriction(s) on certain uses and disclosures, including a statement that the FCC workforce member is not required to agree to a requested restriction;
2. To receive confidential communications of PHI in certain ways and in certain locations;
3. To inspect and copy his/her PHI;
4. To request an amendment of his/her PHI, including a statement that FCC is not required to agree to a requested amendment;
5. To receive an accounting of disclosures of his/her PHI; and
6. To obtain a paper copy of the notice upon request, including a client who has agreed to receive the notice electronically.

FCC's Duties: The notice must include a statement that:

1. FCC is required by law to protect and maintain the privacy of PHI, to provide clients with notice of its legal duties and to abide by the terms of such notice;
2. FCC reserves the right to change the terms of the notice and to apply the revised privacy practices to PHI previously created or received, and a statement of how it will provide clients with a new revised notice.

3. FCC is required to notify a client if unable to agree to a requested restriction;
4. FCC will accommodate reasonable requests by a client to receive confidential health information communications by alternative means or at alternative locations.

Complaint: The notice must include a statement that a client may file a complaint with FCC and/or the Department of Health and Human Services for a suspected violation of his/her privacy rights. Clients funded by Missouri's Department of Mental Health may file a complaint with that agency. The statement must also include a description of the process to file a complaint and a statement of assurance that FCC will not retaliate against the client for filing a complaint.

Contact: The statement must contain the name or title and telephone number of the person to contact at FCC, DHHS, and DMH for further information.

Effective Date: The statement must contain the effective date of the notice.

Notice Review and Revisions Procedure: FCC will revise the notice whenever there is a material change to the uses/disclosures, the client's rights, FCC's legal duties or other privacy practices stated in the notice. Revisions will be made by a review committee that includes the privacy and security officers, the associate director, the executive director, and other FCC workforce members as needed. The privacy and security officers are responsible for updating the notice and distributing it to workforce members within two working weeks after it is revised. Designated workforce members will distribute the revised notice to clients within two working weeks after receipt.

When Notices to Clients Are Required:

FCC will provide a notice of its privacy practices (notice) to clients receiving mental health services and to any person upon request. Clients will be presented with FCC's Notice of Privacy Practices at the date of the first delivery of FCC services. FCC defines its first delivery of services as the date of admission to any of its programs.

When Notices Are Not Required

An inmate does not have a right to notice under this policy. These notice provisions do not apply to a correctional institution.

Emergency Situations

In an emergency situation, the client must be given a copy of the Notice of Privacy Practices as soon as practicable after the emergency treatment situation is resolved.

Obtaining the Acknowledgement by an Individual That Notice Has Been Received Except in emergency situations, FCC will obtain a written acknowledgement from a client of his/her receipt of the notice. Acknowledgement will be documented and placed in the client's clinical record. If a potential client refuses to sign an acknowledgement of having received Notice of Privacy Practices, FCC services will not be provided.

Notice to Clients with Special Needs: FCC staff must be attentive to the needs of individuals in providing the Notice of Privacy Practices and comply with applicable laws concerning non-English speaking individuals or individuals who may not be able to read a written notice.

Web Notice: FCC will post a notice on its Web site and make the notice available electronically through its Web site. An individual may still receive a paper copy of the notice even if he or she has received an electronic notice.

Policy 11: Retention and/or Disposal of Restricted Information

Policy

Family Counseling Center maintains client records that contain protected health information for a minimum of seven (7) years, unless otherwise required by local, state or federal law and regulations or funding sources. Storage systems are designed and implemented to ensure the safety, security, and integrity of client protected health information. When records are approved for destruction, they will be destroyed so that there is no possibility of reconstruction of information.

Procedure

Storage of PHI

All active client clinical paper records are maintained in designated, secured areas at each clinical site. All file cabinets are in a secured area...

Disposal of PHI

When client clinical records/designated record sets have met the minimum maintenance of seven years (or more, as required by local, state, or federal law and regulations or funding source) and are approved for destruction, they must be shredded before disposal. Any other generated paper PHI that is not part of a client's designated record set is not to be disposed of in a trash container; it is to be disposed of according to the shredding procedures at each site.

When other forms of records (e.g., electronic) are approved for destruction, they are to be securely transported to the security officer for disposal. Prior to disposal, the security officer shall ensure all ePHI has been erased to D.O.D. standards. If electronic media is inoperable, said media shall be further incapacitated by some form of physical destruction (holes drilled in HD, smashed, etc.).

Policy 12: Client Access to Protected Health Information

Policy

Clients have a right to access their protected health information stored in their designated record set (DRS). Clients have the right to inspect or obtain a copy of their protected health information. While client access to the designated record set is a required disclosure, it is not included in an accounting provided to clients. Information that is not contained within the designated record set is not subject to this policy.

Procedure

When Clients Have a Right To Access Their Information

FCC clients have the right to request to inspect and/or copy PHI contained in the DRS. FCC will determine the type of documentation to be included in the DRS and the designated staff responsible for receiving and processing clients' requests to access their PHI. (See Privacy Compliance Policy 9 for explanation of determining DRS).

Client shall not have access to computer records. All documents for review shall be printed by a staff member. In some cases a designated staff member may be asked to sit with the client as they review the document.

When Clients Do Not Have a Right To Access Their Information

Clients do not have the right to access any information that is not contained in the DRS. Additionally, clients may not access the following information:

1. Psychotherapy notes (Note: FCC strongly discourages the use of psychotherapy notes. See definition of psychotherapy notes); and
2. PHI compiled in reasonable anticipation of criminal, civil, or administrative actions or other proceedings.

When a workforce member believes that client access may cause harm to the client or others, access may be denied (see below).

How To Process Requests for Access to PHI

Requests To Access Form: The office manager or designee must inform clients of the form to be used when desiring access to their PHI. Prior to FCC's processing or reviewing the request, the client must complete this form.

Standards for Reviewing Requests: Program director or designee must review all client requests for access to PHI and determine whether the request will be approved or rejected in accordance with this policy. Unless the program director or designee decides that there are grounds for a denial, clients may have access to their PHI.

Response Time Frames: Program director or designee must respond to approve or deny and provide the appropriate access (or written denial) no later than 30 days after the receipt of the client's request; however, FCC will make every effort to respond within 15 days. In cases where the requested PHI is not immediately accessible, because it is either in storage or kept off-site, FCC workforce are allowed to act on the request within 60 days of the receipt of the request; however, FCC will make every effort to act on the request within 30 days.

Extensions: The program director or designee is allowed to request and secure a one-time extension of no more than 30 days within which they must take action on a request for access. To secure a one-time extension, FCC workforce member must contact the client who has requested access to his/her record within 30 days (or 60 days for off-site requests) from the date of the request and provide the client with written documentation to justify the delay in its response and the date by which FCC workforce will complete their action to the response.

Designation of a Reviewing Official: The privacy officer or designee will serve as the reviewing official (LHP) when there are reviewable grounds to deny access of a client's request to view or obtain PHI. The privacy officer or designee is not allowed to participate in the original decision and outcome of granting or denying access and must follow procedures as defined in this policy for reviewing the appropriateness of the denial.

Granting Access to Records

Guidelines: If a request for client access is granted, designated FCC workforce members will provide clients with the opportunity to inspect and/or copy their PHI. The information will be provided in the form requested if readily producible in such form; if not, then in hard copy.

The FCC designee releasing the information to the client may choose to provide a summary or an explanation of the PHI in lieu of providing an actual copy of the PHI. Prior to providing this summary or explanation of the client's PHI, the FCC designee must first obtain written agreement from the client to receive a summary or explanation and his/her agreement to pay for any fees incurred. Summaries or explanations of the PHI should be prepared by therapists or other FCC professionals involved in the client's care. In certain circumstances, FCC professionals will make an appointment with the client in order to review the PHI with him/her prior to the client making copies. These circumstances include, but are not limited to, situations in which the therapist or other workforce professional believes the information that the client requested may be difficult to interpret or potentially misunderstood by the client.

If the same PHI that is the subject of the request for access is maintained in more than one designated record set or at more than one location, FCC workforce may provide the requested PHI once in response to a request for access.

Fees Related to Access: FCC has the right to request payment from a client or other person requesting, on the client's behalf, a reasonable, cost-based fee for copying the PHI. Fees are limited to the cost of copying (including supplies and labor), postage, and, with the client's prior approval, the preparation of any summary or explanation of PHI. The cost cannot be greater than that provided under state law.

Denial of Access to Client Requests for PHI

Procedure for Denying Access: All client requests for PHI access must be reviewed by the program director or designee to determine whether grounds for denial exist (see below) and, if such request is denied, whether the client is entitled to a review of the denial.

If reviewable grounds for denial are expected, the program director or designee may contact the privacy officer or designee regarding how to proceed with request to access.

For all denials, FCC workforce must comply with the notice of denial requirements described in this policy.

Unreviewable Grounds for Denial of Access: The following describe unreviewable grounds to deny client's access to his/her PHI:

1. The PHI consists of psychotherapy notes (Note: FCC strongly discourages the use of psychotherapy notes. See definition of psychotherapy notes);
2. The PHI is assembled with a reasonable expectation that the PHI will be used for criminal, civil, or administrative action or other proceeding;
3. The request for PHI is from an inmate, and the PHI would jeopardize the health or safety of the client or of other inmates or any other having contact with the inmate;
4. The PHI was created or gathered by a covered health care provider in the course of research where the client consented to the denial of access when he/she consented to participate in the research and FCC workforce informed the client that access would be restored upon completion of the research;
5. The PHI is contained in records subject to the Privacy Rule where access could be denied under this rule (records or documentation not part of the DRS); or
6. The PHI is obtained from someone other than a health care provider under a promise of confidentiality and the access would be reasonably likely to reveal the source of information.

Reviewable Grounds for Denial of Access: Reviewable grounds of denial for access to a client of his/her PHI exist when

1. The program director or designee has determined that the access requested is reasonably likely to endanger the life or physical safety of the client or another person;
2. The PHI contains references to another person (excluding other licensed health-care providers) and the program director or designee has determined the access requested is reasonably likely to cause substantial harm to the other person; or
3. The request is made by the client's personal representative or guardian (including those of minors) and the program director or designee has determined that the access by the personal representative is reasonably likely to cause substantial harm to the client or another person.

Notice of Denials: Regardless of whether a denial for access is reviewable or not reviewable, FCC workforce must provide:

1. To the extent possible, access to non-excluded PHI;
2. Written notice of denial within 30 days, but within 15 days, if possible, (unless an extension has been requested) stating in plain language (a) the ground(s) for the denial, (b) the review rights, if any, available to the client, including a description of how the client may initiate a review, and (c) a description of the complaint process that a client may follow concerning his/her request, including the name or title and phone number of the contact person responsible for receiving complaints of privacy concerns, or with the Secretary; and
3. The location of the PHI if FCC workforce does not maintain the requested PHI.

Reviewable Denials

1. If requested by a client whose access is denied on reviewable grounds, the program director or designee must promptly refer the request for review to the privacy officer.
2. After receiving the request for review of a denial, the privacy officer or designee must determine, within a reasonable period of time, whether or not to deny the access requested based on the reviewable grounds standards.
3. The program director or designee is bound by the determinations of the privacy officer or designee and must promptly provide written notice of privacy officer or designee's determination with regard to a client's request and take appropriate action, if any.

Policy 13: Amendment of Protected Health Information Policy

Policy

Clients who believe information contained in their designated record set is incomplete or incorrect may request an amendment or correction to the information. Information not contained within a designated record set is not subject to this policy.

Procedure

Processing Requests for Amendment

Documents Subject to Amendment: A client may request an amendment of his or her PHI maintained in a designated record set.

1. The FCC workforce member will remind the client that a request must be in writing and contain a reason to support the requested amendment.
2. The workforce member will then assist the client in completing the Request for Amendment of Health Information form.

Who Is Responsible for Decisions To Grant or Deny an Amendment:

1. A licensed health-care professional (program director or designee) will review requests for amendment of PHI.
2. Such licensed health-care professional will consult with the author of the subject PHI prior to making a determination regarding the request for the amendment.

Response Time Frames and Extensions:

1. FCC workforce members must review and act upon requests for amendments to PHI no later than 60 days after receipt of such request, but within 30 days, if possible, either by granting the request in accordance with this policy, by denying the request in accordance with this policy or obtaining an extension within which to respond to the request.
2. FCC workforce member may request and obtain a one-time extension of no more than 30 days (15 days, if possible) within which to take action on a request for amendment. To obtain a one-time extension, the designated FCC workforce member must contact the requesting client, in writing and within the initial 60-day period (30-day period, if possible), stating the reasons for the delay in its response and the date by which the FCC workforce member will complete its action on the request.

If Approved

Approving an Amendment: If a request for an amendment is approved, the designated FCC workforce member must:

1. Notify the client of the acceptance of the amendment.
2. Furnish copies of the Request for Amendment of Health Information form to those individuals or organizations the client deems necessary. The client is required to identify these recipients on the original Request for Amendment of Health Information form.
3. Furnish copies of the Request for Amendment of Health Information form to FCC business associates or others who have the information subject to the amendment.
4. All additional and future disclosures will be noted on the correction/amendment form with a short notation indicating to whom the Request for Amendment of Health Information form was sent, the date, and the staff member processing the disclosure.
5. When a Request for Amendment of Health Information form is used, the designated FCC workforce member will make an entry at the site of the information that is being corrected, amended, or denied indicating, "See correction/amendment," and will date and sign that entry. The Request for Amendment of Health Information form will be attached to the entry.

6. Whenever a copy of the corrected/amended entry is disclosed, a copy of the Request for Amendment of Health Information form will accompany the disclosure.

If Denied

Reasons for Denial: FCC workforce may deny requests for amendment if the requesting client is attempting to amend PHI that:

1. Was not created by the FCC member, unless the requesting individual provides a reasonable basis to indicate that the originator of the PHI is no longer available;
2. Is not a part of the DRS;
3. Is not available for access under Privacy Compliance Policy 12: Client Access to PHI. This includes a) psychotherapy notes and b) PHI compiled in reasonable anticipation of civil, criminal, or administrative action or other proceeding (Note: FCC strongly discourages the use of psychotherapy notes. See definition of psychotherapy notes);
4. Is accurate and complete.

Providing Notice of the Denial: Regardless of the grounds for denial, FCC must provide a written notice of the denial within 60 days (30 days, if possible) of a request (unless an extension has been obtained) to the requesting client that states:

1. The authorized basis for the denial. The Request for Amendment of Health Information form will be completed with the denial reason clearly identified on the form. One copy of the form will be routed to the client and the original will remain in the client's designated record set;
2. The client's right to submit/provide a written statement disagreeing with the denial and the basis of such disagreement (Statement of Disagreement form) including an explanation of how the client may file his or her Statement of Disagreement with FCC, (the rebuttal will be attached to the identified reason for denial);
3. The client's right that, if no Statement of Disagreement is filed, the client may request that the FCC member include his or her request for amendment and the denial of such amendment with any future disclosures of the PHI that is the subject of the requested amendment; and
4. A description of the complaint process that he or she may follow with FCC, including the name or title and telephone number of the contact person responsible for receiving complaints of privacy concerns, or with the Secretary. (See Privacy Compliance Policy 15).

Statements of Disagreement: FCC will accept any Statement of Disagreement submitted by a client. FCC has decided a reasonable limit to this statement should be no more than two pages in length.

Rebuttal Statements: FCC may prepare a written rebuttal statement to any client's Statement of Disagreement. FCC will provide a copy of the rebuttal to the client who submitted the Statement of Disagreement.

Record Keeping of Denials: FCC will identify the PHI in the DRS that is subject of the disputed amendment and append or otherwise link: a) the client's request for an amendment, b) the denial of the request for the amendment, c) the client's Statement of Disagreement (if any) submitted to FCC, and d) the FCC rebuttal to the Statement of Disagreement (denial materials) to such PHI.

Future Disclosures of PHI Denied Amendment: If a Statement of Disagreement has been submitted by the client, FCC must include in any future disclosures of the PHI to which the disagreement relates either the denial materials described above, or, at the election of FCC, an accurate summary of the denial materials.

If no Statement of Disagreement is submitted by a client, the client must request that FCC include in any future disclosures either the client's request for the amendment and its denial, or an accurate summary of such information. If no request is made, such material need not be included in any future disclosure.

Amendment by Another Covered Entity

FCC workforce members, including business associates, must amend a client's PHI upon receipt of a notice of amendment from another covered entity.

Policy 14: Accounting of Disclosure of Protected Health Information

Policy

This policy describes how to facilitate accounting for disclosures of protected health information. Clients have the right to request an accounting of certain types of disclosures made of their protected health information. Workforce members of Family Counseling Center will provide an appropriate accounting of these disclosures consistent with this policy.

Procedure

General Disclosure Requirements

Clients have a right to receive an accounting of certain types of disclosures of their PHI made by FCC workforce members, including disclosures by or to business associates, for purposes other than treatment, payment or health care operations. Such an accounting will include those disclosures made in the seven-year period prior to the request date (unless the client requests disclosures made over a more limited time period). FCC will make such an accounting available in accordance with the requirements of the Privacy Rule.

Using the Accounting of Disclosure form, FCC workforce members must document the disclosures made and the titles of persons or offices responsible for receiving and processing requests for accounting at each FCC site. FCC workforce members must document the written accounting provided to clients.

Exceptions

Consistent with the Privacy Rule, the following types of disclosures, including disclosures by or to a business associate, are *not* subject to the accounting requirement:

1. Disclosures made to carry out treatment, payment, and health care operations of FCC;
2. Disclosures made to individuals of their own PHI;
3. Disclosures made pursuant to an individual's authorization;
4. Disclosures made for national security or intelligence purposes;
5. Disclosures made to correctional institutions or law enforcement officials having lawful custody of an inmate;
6. Disclosures that occurred prior to the Privacy Rule compliance date of April 14, 2003;
7. Disclosures of de-identified PHI; or
8. Disclosures made to law enforcement officials or health oversight agencies when such officials or agencies have made a request to suspend an accounting.

Required Content of the Accounting of Disclosure

Required content of the accounting of disclosure includes the following:

1. The name and identification number of the client whose PHI was disclosed;
2. Date of disclosure;
3. Name and address, if known, of the entity or person who received the PHI;
4. Brief description of the PHI disclosed;
5. Brief statement of purpose that reasonably informs the client of the purpose of the disclosure; or provide the client with a copy of the authorization or a copy of the written request for disclosure.

If multiple disclosures are made to the same entity or person for the same reason, it is not necessary to document items 1-5 for each disclosure. FCC may document instead the first disclosure, the frequency or number of disclosures made during the accounting period, and the date of the last disclosure in the accounting period.

Procedure for Responding to a Request for an Accounting

Responsible Department: The office manager or designee at each site is responsible for receiving and responding to requests for an accounting of disclosures.

Request for an Accounting Form: All requests for an accounting of PHI must be submitted in writing on the form provided to the client by the office manager/designee. The office manager/designee will assist a client in completing this form.

Verification of Individual Access for an Accounting: The office manager/designee is responsible for verifying that a client has the appropriate authority to request an accounting consistent with the Privacy Compliance Policy 5.

Response Time Frames and Extensions

FCC members will act upon a request for an accounting within 30 days following receipt of a request either by providing the requested accounting or, if unable to provide the accounting within the 30-day period, obtaining a one-time extension. FCC may obtain a one-time extension of no more than 15 days within which it must complete its response by contacting the requesting client, in writing and within 30 days of the request, and stating the reasons for the delay and the date by which FCC will provide accounting. The office manager will complete a delay form and sent it to the client. The client must be informed:

1. Of the delay;
2. The reason for the delay;
3. The date the accounting will be provided.

Such notification to the client of any delay must take place within the 30-day timeframe.

Costs for Accounting

FCC must provide the first accounting to a client within any 12- month period at no charge. FCC may impose a reasonable cost-based fee for each additional request by the same client within a 12-month period. Prior to imposing any fee for an accounting, FCC will first inform the client of the fee and provide the client with an opportunity to withdraw or modify his/her request in order to avoid or reduce the fee.

Suspension of the Right to an Accounting

Written Requests for Suspensions: FCC must temporarily suspend a client's accounting right in accordance with the Privacy Rule for a specified time if requested by a health oversight agency or law enforcement official in writing. If requested to suspend an accounting, FCC will ask the health oversight agency or law enforcement official to state, in writing, that the accounting would be reasonably likely to impede the agency's activities and the time period for the required suspension prior to implementing the suspension.

Oral Requests for Suspensions: FCC will abide by the oral requests of a health oversight agency or law enforcement official for the temporary suspension of a client's right to an accounting. FCC will document the name of the agency or official and the statement requesting the suspension and will limit the suspension to no longer than 30 days unless a written statement from the agency or official is received.

Policy 15: Complaint by Clients

Scope of Policy

This policy applies only to client complaints about perceived improper use/disclosure of their protected health information. All other client complaints, or grievances, will be addressed through the client grievance process found in Family Counseling Center Policy and Procedures manual, CR-9-10.

Policy

Family Counseling Center clients have the right to complain about perceived improper use/disclosure of their protected health information. A complaint is an allegation that a client's protected health information has been improperly used or disclosed

Procedure

FCC strongly encourages and wishes to promote that clients and service providers discuss and attempt to resolve privacy issues in the most direct and informal manner. However, if a client chooses to file a formal complaint, the following procedure will be used.

Process for Complaint

1. The client will complete the HIPAA Privacy Complaint form, which describes the acts or omissions the client believes to have occurred. The complaint form will include
 - a. The date on which the act or omission is believed to have occurred;
 - b. A description of the PHI affected and how it was affected;
 - c. The name(s) of anyone who may have been improperly provided with the PHI.
2. The complaint will be forwarded to the program director or designee when the client has completed the complaint form.
3. If the program director cannot resolve the complaint within 5 working days after his/her receipt or believes that the outcome of the complaint requires examination of and/or changes to existing policies, the complaint will be forwarded to the complaint resolution committee.
4. The complaint resolution committee, consisting of the program director, the associate director, and the privacy officer, and other workforce members as needed, will review and act on the complaint in a timely manner (not more than 5 working days from their receipt of the complaint). If greater time is necessary to review and investigate the complaint, the committee will notify the client of the delay and inform him/her of the expected time frame for the completion of the review.
5. If the affected PHI was created and maintained by a business associate, the complaint will be forwarded to the business associate as outlined in the business associate agreement. Complaints forwarded to business associates will be logged and a notice of action sent to the client making the complaint.
6. The complaint resolution committee will determine if there is cause to believe that a violation of Privacy Compliance Policies has occurred and the course of action to be taken.
 - a. If no violation has occurred, the complaint will be considered closed and a written notice will be provided to the client.
 - b. If cause exists to believe that a violation has occurred, the complaint resolution committee will be responsible for determining if
 - i. Performance or training needs to be improved;
 - ii. A recommendation to revise or create a new Privacy Compliance Policy(s) should be made. In this case, the recommendation will be forwarded to the HIPAA core team for action.

- c. If workforce member discipline must be taken, FCC's Privacy Compliance Policy 22 regarding sanctions will be followed.
7. If the complaint resolution committee finds that no cause exists to believe a violation has occurred and the client is not satisfied, then the client may seek resolution from the board of directors.
 - a. Through completion of the complaint form, the client will request that the complaint resolution committee forward the complaint to the board of directors.
 - b. The board will review and act on the complaint in a timely manner, not more than 30 days from receipt of the complaint form.
 - c. The board will determine one of the following:
 - i. That the original determination of the complaint resolution committee is accurate;
 - ii. That remediation should occur through increased training or that a recommendation be made for possible disciplinary action;
 - iii. That a recommendation for Privacy Compliance Policy review be initiated through the HIPAA core team;
 - iv. That a recommendation be made for the establishment of a new Privacy Compliance Policy.

Complaints to Outside Entities

Family Counseling Center and the outside entities listed below prefer that, if such a complaint is filed, it occur only after all options in the FCC complaint procedures have been exhausted. FCC will cooperate with those entities in any reviews or investigations. Please refer to Notice of Privacy Practices for information about how to contact outside entities.

1. Clients who receive funding from Missouri Department of Mental Health retain a right to submit a complaint to that department.
2. Any person who believes that FCC is not complying with the Privacy Rule or Federal Confidentiality Regulations may file a complaint with the Secretary of Health and Human Services. The following requirements govern such a complaint:
 - a. The complaint must be filed in writing, either on paper or electronically;
 - b. The complaint must name the entity that is the subject of the complaint and describe acts or omissions believed to be in violation of regulations;
 - c. The complaint must be filed within 180 days of when the complainant knew, or should have known, of the act or omission, unless the time limit is waived by the Secretary for good cause shown.

The Secretary may investigate complaints, which may include review of policies, procedures, or practices of FCC and of the circumstances regarding the alleged acts or omissions.

Retention

1. The original complaint form will be placed in the client's clinical record.
2. The complaint resolution committee is responsible for logging
 - a. The person or entity making the complaint;
 - b. The date the complaint was received;
 - c. A list of PHI affected;
 - d. The status of the complaint;
 - e. A list of business associates or facilities affected;
 - f. The action(s) taken.
3. Complaints will be retained for a minimum of seven (7) years.

No Retaliation

There shall be not retaliation against any client or against a workforce member for assisting a client to file a HIPAA privacy complaint.

Policy 16: Research

Policy

Protected health information used or created for research is subject to the Privacy Rule. Protected health information used or created for research cannot be used or disclosed without authorization, except in limited circumstances.

Procedure

Research Not Subject to Privacy Rule

In the following circumstances, research is *not* subject to Privacy Rule:

1. Research in which health information has been de-identified according to Privacy Rule;
2. Research that neither accesses nor creates PHI from the covered entity.

Privacy Board

FCC's Privacy Board will make decisions about the research that uses clients' PHI. The board

1. Includes members of varying backgrounds and appropriate professional competency to review the effect of research protocols on privacy rights and related interests;
2. Includes at least one member who is not affiliated with FCC or the entity sponsoring or conducting the research, and is not related to anyone affiliated with these entities;
3. Does not have any member participating in a review of a project in which he/she has a conflicting interest.

Requirements for Research

FCC will obtain from the researcher(s) documentation that

1. PHI used/disclosed is sought solely for the purpose of research or to prepare a research protocol (or similar preparatory purpose);
2. PHI sought is necessary for research purposes;
3. No PHI will be removed from FCC premises;
4. If the research subject is deceased, the researcher will provide documentation of the subject's death, if requested by FCC;
5. PHI will be kept confidential. This includes securing storage and adhering to regulations regarding re-disclosure.

Uses/Disclosures of PHI for Research Purposes for Which an Authorization Is Required

Unless otherwise indicated in this policy, authorization is required for use or disclosure of PHI for research purposes. Such authorization must follow the regulations outlined in Privacy Compliance Policy 4.

Use/Disclosure of PHI for Research Purposes for Which an Authorization Is Not Required

In the following circumstances, authorization or the opportunity to agree or object is not required:

1. Privacy board approval of a waiver of authorization. Such waiver must follow the guidelines pursuant to 164.512 below:
 - a. Identification and date of action;
 - b. Waiver criteria;
 - c. Brief description of the PHI for which use or access has been determined to be necessary by the privacy board;
 - d. A statement that the waiver of authorization has been reviewed and approved;
 - e. Signature of the privacy board's chair or designee.
2. Reviews preparatory to research. The researcher must attest that:

- a. The information is being sought solely to prepare a research protocol or for similar purposes preparatory to research;
 - b. No PHI will be removed from FCC by the researcher;
3. Research on decedent. The researcher must attest that:
 - a. The information being sought is solely for research on decedents;
 - b. The information being sought is necessary for research purposes;
 - c. FCC has a right to require documentation of the death of the individuals.
4. Limited data set. FCC, or its business associates, may create a limited data set that eliminates direct identifying information but still contains information that could potentially identify a client.
 - a. Use or disclosure of the information contained in a limited data set is conditioned upon the receipt of a data use agreement. Under these circumstances, waiver of authorization by the privacy board is not required.
 - b. A limited data set must adhere to the minimum necessary rule.
 - c. Disclosures made in a limited data set do not have to be included in FCC's accounting of disclosure to a client.

Access of Clients to PHI Related to Research

A client's right to access PHI created or obtained in the course of research may be suspended while the research is in progress, provided the client

1. Agreed to the denial of access when consenting to participate in the research; and
2. Has been informed that his/her right of access will be reinstated upon completion of the research.

Accounting of Disclosures of PHI Related to Research

Clients have a right to receive an accounting of disclosures of PHI, as outlined in Privacy Compliance Policy 14. Certain exceptions or modifications apply.

1. An accounting of disclosures is not required pursuant to an authorization or disclosure in a limited data set;
2. If the research project involves more than 50 records, FCC may provide a client with a list of research protocols for which the client's PHI might have been disclosed. The list must include
 - a. The name of the study;
 - b. A description of the study's purpose;
 - c. The type of information sought;
 - d. The timeframe of the disclosure.

If requested, FCC will assist the client in contacting the researcher to whom his/her PHI was disclosed.

Policy 17: De-Identification of Protected Health Information

Policy:

This policy assists in understanding what constitutes protected health information and methods to de-identify such information. (e.g., remove the client's name and other identifiers and personal data) so as to protect a client's confidentiality with respect to specific health information.

This policy covers any protected health information possessed by Family Counseling Center in whatever form and from whatever source. This policy determines how Family Counseling Center may de-identify protected health information for purposes of using information contained within protected health information without compromising the privacy of the individual to whom the protected health information pertains. Information obtained from de-identified protected health information may be used or disclosed by Family Counseling Center to perform any otherwise legal business purpose.

Procedure

FCC may use or disclose PHI only as permitted by its Privacy Compliance Policies, pursuant to the Privacy Rule and Federal Confidentiality Regulations.

PHI does not include health information that neither identifies an individual nor creates a reasonable basis to believe that the information can be used to identify that individual. It is therefore possible to modify PHI so that it is de-identified.

De-Identification Process

According to the Privacy Rule, PHI de-identification can only be achieved by a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information de-identified. Because most FCC workforce members do not possess this knowledge or experience, all requests for the de-identification of PHI should be directed to the Chief Financial Officer.

The person applying the de-identification process, as outlined in the Privacy Rule, must address the factors identified in 164.514(b). He/she must conclude that the risk is very small that the resultant information can be used alone, or in combination with other reasonably available information, to identify the individual to whom the PHI pertains. Such person must further document that the de-identification process employed and the results obtained from that process support the risk determination described above. Only after this process and conclusions are finalized and documented can the de-identified information be used by FCC for the intended purposes.

Re-Identification Process

FCC may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by FCC, provided that:

1. The code or other means of record identification is not derived from or related to information about the client and is not otherwise capable of being translated so as to identify the individual; and
2. FCC does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification.

Policy 18: Information Systems

Policy: This policy addresses the need to identify information systems that contain protected health information wherever reasonable. This should include the location (or unique system identifier), the form of the data (electronic or paper), the uses(s), and a description of the types of protected health information contained.

Procedure

An inventory of systems that contain PHI will be maintained by the privacy officer and by the security officer. The privacy officer and the security officer will be responsible for identifying new or modified paper or electronic systems and updating the inventory system.

When new systems are inaugurated, the user or users are responsible to notify the privacy officer and the security officer that the system is in production and PHI is present. Conversely, when a system that contains PHI is decommissioned, the user or users will notify the privacy officer and the security officer so that the inventory system can be amended accordingly.

Designated workforce members will adhere to Privacy Compliance Policies 1, 3, and 11 with regard to appropriate locations for all paper-based records containing PHI and for guidelines for the creation, storage, release, transport, copying and destruction of paper-based records.

In instances where an individual member of the workforce gains or creates departmentally sanctioned, exclusive possession and control of PHI as a part of his or her assigned duties, that person is responsible to notify the privacy officer and the security officer of the existence of such information. Further he/she will be responsible for all administrative duties in terms of security, data access, privacy, data backup, disaster recovery and accountability. If the workforce member does not have the technical expertise or facilities to adequately protect the PHI, he/she must arrange for technical assistance either through ITS, or other competent resources approved by ITS, to assure confidentiality of the PHI. (See IT Acceptable Use Policy for additional information regarding electronic records).

Examples of such exclusive possession and control could be:

1. PHI contained within departmentally and/or privacy board sanctioned discrete databases created by and for the member of the workforce, in the performance of their assigned duties;
2. PHI contained within written logs or notes maintained by the member of the workforce, in the performance of his or her assigned duties;
3. PHI contained within any electronic device, such as voice recorders, personal digital assistants, pc's and notebook computers, recordable media such as USB drives, cd's, etc.;
4. PHI transported using any medium such as e-mail, fax, or physical relocation.

Policy 19: Business Associates

Policy

All business associates that require or have access to client protected health information or that are involved in the exchange, transmission, or use of protected health information must agree in writing to protect protected health information in accordance with federal and state law and Family Counseling Center policy. All contracts with outside entities that have access to protected health information will contain required regulatory language.

Definitions and Qualifications: A business associate is defined as any entity that:

1. On behalf of FCC, or any organized health-care arrangement of which FCC is a part, performs, or assists in the performance of, a function or service that involves the use or disclosure of identifiable health information or any other function or activity regulated by the Privacy Rule; or
2. Examples of categories of FCC business associates include, but are not limited to, third party professionals (e.g., attorneys and accountants), consultants (e.g., information technology consultants), service providers (e.g., answering services), laboratories, and shared service arrangements.

A business associate is *not*:

1. A member of FCC's workforce, including volunteers;
2. An entity that performs services as part of an organized health-care arrangement;
3. An entity that is a conduit for information (e.g., the U. S. Postal Service or its electronic equivalent); and
4. A financial institution that processes consumer payments for health care.

Procedure

1. The associate director will review (or appoint another individual with appropriate authority to review) any proposed contracts with potential business associates and/or review proposed contracts with potential business associates to ensure that required regulatory language is included in any agreements prior to signature if the business associate has access to PHI.
2. Representatives of business associates must sign a contract that contains the required regulatory language before access to PHI is granted.
3. Each business associate contract or agreement must be signed by a representative of FCC authorized to grant access to PHI before access to PHI being granted.
4. Completed business associate contracts must be maintained by FCC in a centralized location by the executive director and/or other authorized workforce members.
5. The contract with the business associate must contain the following:
 - a. A clause that the business associate must agree not to use or disclose PHI of a client except as otherwise provided in the agreement;
 - b. A clause that requires a business associate to receive assurances from third parties prior to making any authorized disclosures to those third parties;
 - c. A clause that requires business associates to have safeguards in place to prevent the unauthorized use or disclosure of PHI and allows FCC to review those safeguards;
 - d. A clause that requires business associates to enter into agreements with third parties regarding the protection of PHI prior to making any authorized disclosures to those third parties;
 - e. A clause that requires access to PHI that the business associate may maintain on behalf of FCC, and, if necessary, describes the process to amend such records at the request of FCC or client;

- f. A clause that requires business associates to retain information regarding uses and disclosures for the past seven years and allow FCC and the U.S. Department of Health and Human Services access to such records;
 - g. A clause that allows FCC to terminate any contract with business associate if business associate fails to follow the privacy requirements.
6. If any FCC workforce member has cause to believe that a business associate has breached any of the business associate's obligations to protect PHI, the workforce member is required to report such belief to the privacy officer and the associate director or the executive director.
7. If a breach of business associate's obligations to protect PHI is suspected, the privacy officer, in conjunction with the associate director or the executive director, should immediately begin an investigation of that business associate's practices, which shall include, at a minimum:
 - a. A review of business associate's records, tracking uses and disclosures of FCC's PHI;
 - b. A review of business associate's privacy practices, including but not limited to, safeguards implemented to prevent the unauthorized use or disclosure of PHI;
 - c. Interviews with appropriate business associate employees; and
 - d. If necessary, involvement of legal counsel to conduct interviews, etc.
8. If the privacy officer and the associate director or the executive director believe that the business associate failed to protect PHI as required in its contract with FCC or in any addenda thereto, they may choose to consult with legal counsel prior to taking any further action.
9. If appropriate given the risk associated with allowing access to PHI to a particular business associate, language will be included in the business associate's contract requiring the business associate to obtain insurance for the unauthorized use or disclosure of PHI.
10. If appropriate given the risk associated with allowing access to PHI to a particular business associate, language will be included in the business associate's contract requiring the business associate to indemnify FCC or any losses incurred due to the business associate's unauthorized use or disclosure of PHI.
11. Implement administrative, physical and technical safe guards that reasonably and appropriately protect the confidentiality, integrity and accountability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity.
12. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safe guards to protect it.

Policy 20: Workforce Member Personnel Files

Scope of Policy:

This policy covers medical information about workforce members. It does not address all of the contents or procedures surrounding Family Counseling Center workforce members' personnel files. See Family Counseling Center Policies and Procedures manual, PE-32, for more information.

Policy: Family Counseling Center's personnel files will keep workforce members' protected health information, as well as other designated information, confidential.

Procedures:

Access to Workforce Members' Personnel Files

1. Access to workforce members' personnel files is limited to designated personnel.
2. Access will be authorized by the Executive Director and the human resource coordinator.
3. In certain situations, individuals such as auditors or federal investigators may have access to workforce members personnel files without their authorization.

Storage and Contents of Workforce Members' Personnel Files

1. Personnel files will be maintained in locked files or within a locked room to ensure privacy and security.
2. The contents of personnel files will be maintained in accordance with the current state and federal law.

Workforce Members' Medical Files

Files containing medical information about workforce members will be kept separate from the rest of their personnel file. This information includes

1. Requirements for doctor's verification of illness;
2. Physicians' statements;
3. Worker's Compensation issues;
4. Initial and subsequent health clearance;
5. Medical clearance to return to work, clinical evaluations, ability to perform essential functions statements;
6. Employee injury reports.

The information maintained in the medical files will not be considered to be part of the workforce member's individual personnel file. This information will be accessed only on a need-to-know basis.

Policy 21: Training Workforce Members

Policy

Family Counseling Center will train, and document the training of, all workforce members on policies and procedures relating to protected health information as necessary and appropriate to their work functions.

Any workforce member whose functions are affected by a material change in policies or procedures required by regulations will be trained within a reasonable time after material changes become effective.

Procedure

1. The privacy officer and other designated staff are responsible for scheduling training sessions for all existing FCC workforce. FCC workforce will be trained as to FCC's Policies and Procedures related to client privacy (Privacy Compliance Policies).
2. New workforce member orientation programs will contain information regarding FCC's Policies and Procedures related to client privacy (Privacy Compliance Policies). New workforce members will be trained on these policies within 10 working days of their start date.
3. Documentation that a member of the workforce has received information and initial training about FCC's Policies and Procedures on client privacy will be placed in that member's personnel file.
4. Any modifications or additions to FCC's Policies and Procedures related to client privacy will be presented to all workforce members through communications from program directors within two weeks of the modification or addition.
5. Designated workforce members will participate in reviews of FCC's Policies and Procedures related to client privacy annually, and documentation of their participation will be placed in their personnel files.
6. Workforce members who violate policies and procedures related to client privacy will be subject to disciplinary action, up to and including termination.

Policy 22: Sanctions for Breaches or Potential Breaches of Client Privacy

Policy

Client and workforce member information will be regarded as confidential and will be available only to authorized users for approved purposes. Access to confidential information is permitted for direct client care and approved administrative/supervisory functions.

Confidential information obtained either during assigned duties or by accident will not be released to any person or institution except in accordance with Family Counseling Center policy. No Family Counseling Center workforce member or vendor will seek access to confidential information out of curiosity, for malicious purposes, or for financial gain. Discussion or consultation involving a client's care or a workforce member's confidential information should be conducted in private. Individuals not directly involved in the client's care should not be present without the client's permission. Family Counseling Center will have and apply appropriate sanctions against members of its workforce who fail to comply with Family Counseling Center's privacy policies and procedures. Family Counseling Center will document the sanctions that are applied, if any.

New employees will be given Privacy Compliance training and monitored by their supervisor.

Procedure

All breaches or patterns of potential breaches will be reviewed by HIPAA officers and any other designees for performance improvement. These incidents will be reviewed by examining possible physical causes, human causes, and/or organization causes. Physical causes are the tangible causes of failure, human causes trigger a physical cause of failure (errors of commission or omission). Organizational causes originate in the operational system in which the people function.

Level of Breach

Breaches in client confidentiality have been divided into the following four levels with the corresponding disciplinary action for each level of breach. Supervisors/program directors will follow the procedure outlined below; however, if a supervisor /program director believes that special circumstances apply, he/she will consult with the privacy officer to determine appropriate action.

Disciplinary actions will be administered in a progressive manner. Disciplinary sanctions at each level will be reported to the applicable professional licensing board as appropriate.

Level 1: Potential Breach

A Potential Breach is defined as a situation where a lapse in security resulted in the risk of acquisition, access, use or disclosure of unsecured PHI/ePHI but no known actual breach resulted. For example, interior facility doors left unsecured, conversations in public areas, unencrypted emails, etc., for which there is no evidence of acquisition, access, use or disclosure of unsecured PHI/ePHI.

Level 2: Unintentional or Careless Breach: This level of breach occurs when a member of the FCC workforce unintentionally or carelessly accesses, reviews, or reveals client information to him/herself or others without a legitimate need to know the client information. Examples include, but are not limited to, workforce members discuss client information in a public area; workforce members leave a copy of client PHI in a public area; workforce members leave a computer unattended in an accessible area with a client's chart unsecured.

Disciplinary Sanctions for Level 1 and Level 2 Breaches

FCC workforce members will be given reminders for breaches that are judged unintentional or careless by the appointed HIPAA Agent/supervisor. If the breach causes potential or actual harm to a client, the workforce member's name, the date of the breach, and a description of the breach will be placed in the site's HIPAA Corrections Manual.

Documentation in the Corrections Manual does not necessarily constitute a "write up." Agents may randomly engage in site checks if he/she notices a pattern in breaches.

The privacy officer will be available to meet regularly with designated HIPAA agents and will also review the Corrections Manual periodically to assess for patterns. The privacy officer may also engage in random site checks if deemed necessary.

The severity of the sanction for a Level 1 or 2 breach is contingent upon:

- i. The seriousness of the breach. For example, sanctions for a workforce member who forget to shut his/her door periodically may be less severe than a workforce member who leaves a client's clinical record in the waiting area.
- ii. The number of times a workforce member commits the breach. For example, if a workforce member engages in the same violation multiple times, sanctions would likely be more stringent.
- iii. The amount of time that has lapsed between breaches. For example, consideration will be given for workforce members who have much time in between breaches.
- iv. Special circumstances. Supervisors, in conjunction with the privacy officer, have the right to determine if workforce member breaches have occurred due to special circumstances. For example, consideration may be given for a workforce member who is under an undo amount of duress, or a breach occurred due to problems in FCC procedures and is not due to the workforce member's carelessness.

The level of sanction can range from an oral warning up to probation, unpaid leave, and even termination. Workforce members may be asked to repeat the privacy training module as well.

Level 3: Curiosity or Concern (no personal gain): This level of breach occurs when a workforce member intentionally accesses or discusses client information for purposes other than the care of the client or other authorized purposes but for reasons unrelated to personal gain. Examples include, but are not limited to, a workforce member looks up client birth dates, address of friends or relatives; a workforce member accesses and reviews a record of a client out of concern or curiosity; a workforce member reviews a public personality's PHI.

Disciplinary Sanctions for Level 3 Breaches

Step 1

The breach will be reviewed and the workforce member will be put on probation with a plan of corrective action or termination. . Documentation will be placed in the workforce member's personnel file and in the HIPAA Corrections Manual.

Step 2

A second breach at this level will result in a workforce member's termination. Documentation will be placed in the workforce member's personnel file and in the HIPAA Corrections Manual. This step should be undertaken after the program director consults with the associate director and the privacy officer.

Level 4: Personal Gain or Malice: This level of breach occurs when a workforce member accesses, reviews, or discusses client information for personal gain or with malicious intent. Examples include, but are not limited to, a workforce member reviews a client's record to use information in a personal relationship; a workforce member compiles a mailing list for personal use or to be sold.

Disciplinary Sanctions for Level 4 Breaches

A breach at this level will result in a workforce member's termination. Documentation will be placed in the workforce member's personnel file and in the HIPAA Corrections manual. This step should be undertaken after the program director consults with the associate director and the privacy officer.

Appeal Process

A workforce member who has been recommended for disciplinary sanctions more severe than a reprimand ("write-up") has a right to appeal the recommendation, either in writing or in person, to the associate director. This request should be made within seven days of the program director's recommendation. Dismissal may be appealed to the executive director and the board of directors, as outlined in FCC's Policy and Procedures manual, PE-36-38.