Policy Number:
25
Effective: March 19, 2007
Revised:

Subject: HIPAA Compliance

POLICY:

It is the policy of Camden Co. Developmental Disability Resources to be in compliance with the Health Insurance Portability and Accountability Act of 1996.

PROCEDURES:

I. Notice Of Privacy Practices

A. At the date of the first delivery of, or appearance for, services with Camden County Developmental Disability Resources (CCDDR), application for services, or upon referral from the Rolla Regional Center for services, the consumer (or their legal guardian or parent, if a minor) should be presented with the Notice of Privacy Practices.

1. Documentation of acknowledgment (defined for CCDDR's purposes as the consumer's signature or mark on a cover sheet to the current Notice of Privacy Practices) that such a Notice has been presented to a consumer (or their legal guardian or parent, if a minor) for review must be placed in the consumer's record. The cover sheet to the Notice of Privacy Practices is to be removed from the Notice and filed in the consumer's confidential file. The full Notice of Privacy Practices is then given to the consumer.

2. If CCDDR does not obtain the acknowledgment, then it shall document its good faith efforts to obtain the acknowledgment, and document the reason(s) why the acknowledgment was not obtained on the acknowledgment cover sheet to the Notice of Privacy Practices.

B. A copy of the Notice of Privacy Practices shall be posted in a highly visible and prominent location at CCDDR, where it is reasonable to expect individuals will be able to locate and read the Notice.

C. Whenever the Notice of Privacy Practices is revised, the revised Notice must be made available upon request by a consumer.

D. CCDDR's Privacy Officer will be responsible for developing and updating, as necessary, the Notice of Privacy Practices. When a material change is made, CCDDR must make

that revised Notice available upon request, and the revised Notice must be posted at the CCDDR facility.

E. The Privacy Officer will be responsible for ensuring that CCDDR employees/volunteers are trained regarding the Notice of Privacy Practices in accordance with CCDDR's policy related to employee HIPAA mandatory training.

F. Consumer questions related to the Notice of Privacy Practices should be directed to the CCDDR Privacy Officer.

G. The CCDDR Privacy Officer shall maintain a historical record of all versions of the Notice of Privacy Practices, and the applicable dates for each.

II. Use & Disclosure Of Protected Health Information (PHI) and Authorization To Release PHI

A. CCDDR may not use or disclose protected health information without a valid authorization completed by the consumer, or applicable personal representative, with limited exceptions. The CCDDR Privacy Officer 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. If other staff receives a completed authorization form for the release of PHI, they shall direct it to the CCDDR Privacy Officer for review.

B. Any disclosures that occur shall be limited to the minimum amount of information necessary to meet the purpose of the use or disclosure. Exceptions to the minimum necessary requirement are as follows:

- When the consumer authorizes the disclosure;
- Disclosures required by law.

C. CCDDR must obtain an authorization for any use or disclosure of psychotherapy notes except:

- to carry out treatment, payment or health care operations;
- for CCDDR to use in defending itself in litigation or other proceedings brought by the consumer.

D. PHI may only be disclosed without authorization in the following situations:

1. To a public health authority (i.e. required reporting to the Missouri Department of Health and Senior Services);
2. To report child abuse/neglect situations, and other situations involving abuse, neglect or domestic violence (if disclosure is allowed by law);
3. To the Food and Drug Administration;
4. To a health oversight agency;
5. To judicial or administrative proceedings (a subpoena from a court is not enough);

6. To law enforcement (but only in certain circumstances, including when they present a grand jury subpoena; information concerning forensic clients; to locate a missing person, suspect, or fugitive; or at the discretion of the head of the facility when the information is requested to assist law enforcement in their investigation [see Section 630.140, Revised Statutes of Missouri]);
7. To avert a serious threat to health or safety;
8. Governmental functions (such as national security; veterans' information);
9. To other agencies administering public benefits;
10. To medical examiners and coroners;
11. To funeral directors;
12. For organ donation purposes;
13. For some research purposes; or
14. As required by law.

E. Any questions as to whether a use or disclosure is permitted or required by law should be directed to the CCDDR Privacy Officer.

F. If it is CCDDR that requests that the consumer complete the authorization, CCDDR must provide the consumer with a copy of the signed authorization.

III. Accounting of Protected Health Information Disclosures

A. All disclosures of PHI need to be accounted for upon the request of the individual. This is not limited to hard copy information but any manner of communication that discloses information, including verbal release. However, the following list of exceptions to this requirement does not require tracking or need to be accounted for upon the request of the individual:

1. Disclosures made for treatment, payment, and healthcare operation purposes as set out in 45 CFR §164.502;
2. Disclosures made to the consumer. (45 CFR §164.502);
3. Disclosures made for facility directory purposes, if utilized (45 CFR §164.510);
4. Disclosures made for national security or intelligence purposes. (45 CFR §164.512 (k)(5));
5. Disclosures made to correctional institutions or law enforcement officials. (45 CFR §164.512(k)(5));
6. Disclosure made prior to the date of compliance with the privacy standards
7. There are further exceptions for disclosures to health oversight agencies (see section 164.528(a)(2)(I) et seq.). Please contact the CCDDR Privacy Officer should this situation arise.

B. The CCDDR Privacy Officer shall assure that a mechanism is in place which tracks disclosure of both written and verbal protected health information. One format shall be utilized.

C. CCDDR will include the following Required Content in the Accounting of Disclosures:

1. The name and social security number of the consumer 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 consumer what the purpose was for the disclosure, or provide the consumer with a copy of the authorization, or provide the consumer with a copy of the written request for disclosure.

D. If multiple disclosures are made to the same entity or person for the same reason, it is not necessary to document each disclosure. CCDDR 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.

E. The consumer (or legal guardian) must make a written request for an accounting of disclosures to the CCDDR Privacy Officer. The request shall be on the CCDDR Form. Staff may assist the consumer in completing the form if requested to do so.

F. CCDDR shall have 60 days after receipt of the request for such an accounting to act on that request for an accounting of disclosure. If CCDDR has disclosed information to a business associate regarding the consumer requesting the accounting, then CCDDR through its Privacy Officer or designee must request an accounting of disclosures of that consumer's information from that business associate, who has 20 calendar days to provide the accounting. CCDDR may request one 30-day extension, which is allowed, but the consumer must be informed in writing:

1. Of the delay,
2. The reason for the delay,
3. The date the accounting will be provided, and
4. Such notification to the consumer or person requesting the accounting of disclosures of any delay must take place within the 60-day timeframe.

G. CCDDR will provide all accounting of disclosures free of charge

H. CCDDR must retain a copy of the written accounting that is provided to the consumer in the consumer's confidential file.

IV. <u>Verification Of Requestor Identity & Authority</u>

A. The consumer or personal representative must sign a valid authorization for the disclosure of confidential protected health information before such PHI can be released, except in accordance with existing HIPAA requirements.

B. All requests for disclosure shall be forwarded to the CCDDR Privacy Officer including the following:

1. The name of the requesting party or parties and
2. Any documentation, statements or representations from the person requesting the PHI of his/her authority to request such information (i.e., legal representative of consumer, law enforcement official, etc.).

C. The consumer must present identification prior to receipt of any records regarding themselves.

D. The Privacy Officer may rely on the following information to demonstrate identity:

1. Presentation of agency identification, credentials or other proof of government status (a badge, identification card, etc.);
2. A written request on agency letterhead or an oral statement if a written statement would not be possible (a natural disaster, other emergency situations, etc.);
3. 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; or
4. A court order.

E. The Privacy Officer shall verify identity of any phone requests from all individuals, including law enforcement officers and others who have an official need for PHI by using a callback phone number before releasing information.

F. The Privacy Officer shall verify facsimile number of any faxed requests. The main number of the sending agency shall be called, and the fax number verified.

G. The CCDDR Privacy Officer shall verify e-mail address by calling requestor. The general number for the sending agency shall be called, and then a request shall be made to be transferred to the specific individual who made the contact.

H. The Privacy Officer is responsible for copying verification information or obtaining badge number, etc., and for maintaining it in the consumer's health information file.

I. The Privacy Officer must review the forwarded information and determine if he or she is satisfied that the documents verify the identity of the requestor and also demonstrate that the requestor has authority to request the information under state and federal law.

J. The Privacy Officer may disclose information to the requestor if all requirements for use and disclosure are met.

K. The Privacy Officer shall contact agencies or other entities for further verification of identity or authority to receive PHI, if necessary.

L. The Privacy Officer may deny access to information, if verification of identity or authority is not accomplished.

M. The CCDDR Privacy Officer shall assure that a mechanism is in place which tracks disclosure of both written and verbal protected health information.

V. Disclosure Of Minimum Necessary Amount Of Protected Health Information

A. CCDDR and its workforce will make reasonable efforts to ensure that the minimum necessary protected health information (PHI) is disclosed, used, or requested. Exceptions to the minimum necessary requirement include:

1. Disclosures to the individual who is the subject of the information;
2. Disclosures made pursuant to an authorization;
3. Disclosures to or requests by healthcare providers for treatment purposes;
4. Disclosures required for compliance with the standardized HIPAA transactions;
5. Disclosures made to Health & Human Services/Office of Civil Rights (HHS/OCR) pursuant to a privacy investigation; or
6. Disclosures otherwise required by the HIPAA regulations or other law.

B. Each user of PHI will be subject to the provisions of CCDDR policies relating to staff access to PHI.

C. Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties. These efforts will include the Privacy Officer monitoring staff use and disclosure of PHI.

D. For situations where PHI use, disclosure or request for PHI occurs on a routine and recurring bases, the Privacy Officer will issue directives as to what information constitutes the minimum necessary amount of PHI needed to achieve the purpose of the use, disclosure or request.

E. For non-routine disclosures (other than pursuant to an authorization), staff should address questions to the CCDDR Privacy Officer to assure that PHI is limited to that which is reasonably necessary to accomplish the purpose for which disclosure is sought. Examples of non-routine disclosures include providing PHI to accrediting bodies; insurance carriers, research entities, funeral homes, etc.

VI. Consumer/Guardian Procedural Safeguards For Improper Use Or Disclosure Of Protected Health Information

The following steps constitute the HIPAA complaint process:

A. Utilize CCDDR HIPAA Privacy Complaint form.

B. Forward a copy of the complaint form to the CCDDR Privacy Officer if the alleged violation took place at CCDDR facility or program.

C. The HIPAA Privacy Complaint must describe the acts or omissions the consumer believes to have occurred.

D. The HIPAA Privacy Complaint must include the following information:

1. the date on which the act or omission occurred;
2. a description of the PHI affected and how it was affected; and
3. the name(s) of anyone who may have improperly been provided with the PHI.

E. All Privacy Complaints received by the Privacy Officer or designee will be date-stamped upon arrival.

1. The Privacy Officer will review and act on the complaint in a timely manner and not more than 30 days from receipt of the complaint. If greater time is necessary to review and investigate the complaint, the Privacy Officer shall, within 30 days, notify the consumer of the delay, and inform the grievant of the expected timeframe for completion of the review.
2. The Privacy Officer shall determine what PHI is affected by the complaint and if the PHI was provided to other covered entities and business associates.
3. 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 the action sent to the consumer making the complaint.

F. The Privacy Officer shall determine if there is cause to believe that a violation of CCDDR privacy policies occurred, and the course of action to be taken.

1. If no violation has occurred, the complaint and finding will be date-stamped, the complaint will be considered closed, and a written notice of this shall be provided to the consumer.

2. If cause exists to believe that a violation has occurred, the Privacy Officer shall be responsible for determining if:

- Performance or training need to be improved;
- A recommendation for a change to the CCDDR policy should be forwarded to the Board of Directors; or
- A recommendation should be made to the Board of Directors to establish a new Privacy policy (if a CCDDR complaint).

3. The Privacy Officer shall notify the Board of Directors of the action needed.
4. If employee discipline must be taken, it must follow the CCDDR policy on sanctions.

G. If the complaint resolution finds that no cause exists to believe a violation occurred, then the consumer or his/her personal representative may seek resolution to the CCDDR Board of Directors directly (if it is a CCDDR based complaint).

1. The consumer, through completion of the Complaint Form, will request that the CCDDR Privacy Officer forward the complaint to the CCDDR Board of Directors.
2. The Board of Directors will review and act on the complaint in a timely manner and not more than 30 days from receipt of the complaint form.

H. The Board of Directors shall determine one of the following:

1. That the original determination of the CCDDR Privacy Officer is accurate;
2. That remediation should occur through increased training, or that a recommendation is made for possible disciplinary action;
3. That a recommendation for CCDDR policy review be initiated;
4. That a recommendation be made for the establishment of a new CCDDR policy.

I. The original complaint form shall be placed in the consumer's confidential file.

J. The CCDDR Privacy Officer's primary responsibilities in the HIPAA Complaint process include logging and retaining complaints in a retrievable manner for a minimum or six years, and identifying:

1. Person or entity making the complaint;
2. Date complaint was received;
3. A list of what PHI was affected;
4. Status of complaint;
5. A list of business associates or facilities affected; and
6. Actions taken.

K. There shall be no retaliation against any consumer, or against a workforce member for assisting a consumer to file a HIPAA Privacy Complaint.

VII. <u>Designated Records Set</u>

A. CCDDR shall identify all information systems (defined as an organized collection of information) that contain Protected Medical/Health Information.

B. That inventory shall be maintained by the CCDDR Privacy Officer. Any new or modified systems shall be added to the inventory by the appropriate Privacy Officer.

C. For the purpose of the implementation of 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 CCDDR for consumer care or payment decision making including but not limited to:

1. Medical record and billing records about consumers maintained by or for CCDDR;
2. Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for CCDDR; and

3. Any records or information used, in whole or in part, by or for CCDDR to make decisions about consumers.

D. Information that is not part of the Designated Records Set is defined as follows: any documents that are used for census information, quality assurance or quality improvement, peer review, sentinel event, Centers for Medicare and Medicaid purposes, utilization review, abuse/neglect investigations, incident/injury reports, state auditors, or various electronic databases, etc., which are not used to make decisions regarding an individual consumer, shall not be considered as part of the designated records set. However, please note that these types of information may be accessible by parents or guardians. In addition, for forensic cases (defined as Chapter 552 or 557, RSMo, evaluations), the pretrial commitment order, the pretrial evaluation, or any correspondence relating to the pretrial is not part of the designated records set. Neither is the victim notification information.

1. Working files, either paper or electronic, are also not considered part of the designated records set.
2. Psychotherapy notes are not included in the designated records set (psychotherapy notes are defined in 45 CFR Section 164.501, and are to be kept separate from the medical record).

E. When an individual has been given sanctioned, exclusive possession and control of PHI as part of their assigned duties, they shall be responsible for all administrative duties of a data trustee in terms of security, data access, privacy, data backup, disaster recovery and accountability. When the individual does not have the technical expertise or equipment to adequately protect the PHI, they must arrange for technical assistance to assure the confidentiality of the PHI.

VIII. Access To Computerized/Electronic PHI

A. Management's Right to Access Information:

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), CCDDR management shall have complete access to all E-mail and Internet activities. No electronic communications sent or received are considered private to the employee. Management has the right to monitor messages and Internet use as necessary to assure efficient and appropriate use of the technology.

B. Each of the electronic communications technologies may create electronic records that are easily saved, copied, forwarded, retrieved, monitored, reviewed, and used for litigation. All electronic records are the property of the CCDDR and can be accessed and used by management when:

1. A legitimate business need exists that cannot be satisfied by other means; or
2. The involved employee is unavailable and timing is critical to a business activity; or
3. There is reasonable cause to suspect criminal activity or policy violations; or

4. Law, regulation, or third-party agreement requires such monitoring.

C. These disclosures of electronic records may be made without prior notice to the staff members who sent or received the communications. Staff members should not assume that any electronic communications are private.

D. User Access to Electronic CCDDR Data: To gain access to any CCDDR protected healthcare information, CCDDR workforce members are required to consult with the CCDDR Privacy Officer beforehand. All users shall be required to protect confidential data, and only the minimum necessary data shall be accessed.

E. CCDDR shall maintain a Business Continuity/Disaster Recovery Plan, approved by the Security Officer to assure continued operations in the event of an emergency.

F. No CCDDR client/consumer or volunteer shall have access to another person's PHI or any other CCDDR client demographic system, or be allowed to input information to local systems that may be used to feed or modify those systems or unless authorized by the consumer. Any proposed client/consumer access shall include documentation of the client/consumer reviewing and agreeing to a confidentiality statement. Documentation shall include the types of systems and files accessed.

G. Such client/consumer access shall be approved by the CCDDR Director, or designee with notification and documentation provided to the Security Officer.

H. Access to Electronic Media & Internet and Electronic Mail: Users are required to abide by the following guidelines when using CCDDR electronic mail systems:

1. The Internet and E-mail are intended to be used primarily for business purposes.
2. The Internet may be used to access external databases and files to obtain reference information or to conduct research.
3. E-mail may be used to disseminate business-related newsletters, press releases, or other documents to groups of people.
4. E-mail and the Internet may be used for discussion groups on job-related topics.
5. Personal use of E-mail must be limited and must not interfere with the performance of work duties.

Electronic mail and/or the Internet may not be used for:

- Any illegal or unethical purpose;
- Private purposes such as advertising products or services, business transactions, or for private business activities;
- Operating a business, sending chain letters, or soliciting money for any purpose;
- Transmitting, downloading or viewing material that is obscene, pornographic, threatening or harassing, or information that may be perceived to be obscene, threatening or harassing to another individual;
- Disseminating, copying, or printing copyrighted materials (including articles, software, music and movies) in violation of copyright laws;

- Subscribing to mailing lists and broadcast services that do not relate to the business of CCDDR;
- Downloading software of any kind without prior approval of management;
- Participating in Internet chat rooms or instant messaging, including but not limited to AOL Instant Messenger and Internet Relay Chat (IRC);
- Playing games; or
- Conducting any political activity.

I. Training on Access: All CCDDR employees, client/consumers and volunteers must receive the required HIPAA privacy training.

J. Required Confidentiality Agreement:
CCDDR workforce members that receive or maintain PHI shall be required to agree to the security of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement. A copy of the signed confidentiality statement shall be maintained in the personnel file of CCDDR staff.

K. Password Management:

1. Passwords shall not be shared.
2. Passwords shall be changed immediately if user is aware that someone else knows it.
3. Users shall not change their passwords while others are present.
4. Passwords shall have no connection to the user. i.e. user name, children's name, etc.

IX. Physical Security/Maintenance Of Electronic & Computerized PHI

A. Users shall be automatically logged off their workstations after a maximum period of 15 minutes of inactivity.

B. Designated CCDDR staff shall ensure that all media has been thoroughly cleansed of any client data before the media is surplussed or disposed of.

C. Access to media containing client data shall be controlled by:

1. Physical access control to CCDDR hardware;
2. Purging CCDDR data on any type of media before it is surplussed or discarded;
3. Storage of data on media that is backed up.

D. The CCDDR Security Officer shall maintain an up to date Standards List which prescribes appropriate procedures and practices for data security purposes.

E. Virus protection for the CCDDR network shall be maintained by the CCDDR Security Officer, pursuant to the CCDDR virus protection procedures.

1. Email Servers. All CCDDR email servers shall be protected using the email-specific anti-virus software listed on the Standards List.

2. Workstations, laptops, PDAs

    a. All workstations, laptops, PDAs or any other device that connect to an CCDDR network shall be protected using the anti-virus software for that device listed on the Standards List.
    b. Equipment that has not been purchased by CCDDR shall not be allowed to connect to any CCDDR network.

F. Anti-virus software will check for virus signature updates at least weekly from the software manufacturer.

G. Anti-virus software shall be kept up-to-date by the CCDDR Security Officer at the current software release or no more than one release below the most current release version.

H. CCDDR workforce shall not load software, from any source, onto their assigned workstation without prior authorization from Director. This software includes but is not limited to software from the Internet, a CD, or a floppy diskette. Software shall be loaded on workstations only by the Director.

I. CCDDR workstations shall be situated by Security Officer to prevent more than incidental observation of work product.

X. Consumer/Guardian Right To Amend PHI

A. A consumer, parent of a minor, and personal representative or legal guardian as relevant to their representation, who believe information in their health records is incomplete or incorrect may request an amendment or correction of the information as outlined below:

1. For minor discrepancies, i.e. typos, misspelled name, wrong date, etc., the consumer may approach the author of the entry, point out the error, and ask the author to correct it.
    a. If the entry author agrees, the entry can be corrected according to best documentation practices by drawing a single line through the error, adding a note explaining the error (such as “wrong date” or “typo”), date and initial it, and make the correction as close as possible to the original entry in the record.
    b. Any information added to a Person Centered Plan in the regular course of business is not considered an amendment. An example would be when a consumer provides the name of a new private physician whom he/she sees in the community.

2. All other requests for amendment to PHI shall be in writing and provide a reason to support the amendment. Specifically, any request should be supported by documentation of any incorrect information or incomplete information.

B. The "Request for Amendment to Protected Health Information" form shall be provided to facilitate the request. CCDDR may assist in initiating the process requesting amendment to PHI and a copy shall be provided to the consumer.

C. All requests for amendment of PHI must be forwarded to the CCDDR Privacy Officer, who will route the original request to the author of the PHI.

D. If the author chooses to add a comment to the request form, a second copy of the form will be given to the consumer with the author's comments.

E. This request shall be processed in a timely consistent manner according to established timeframes but not more than 60 days after receipt of the request.

F. If the request for amendment cannot be processed within the 60 days, the timeframe may be extended no more than an additional 30 days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

G. If a consumer with a guardian requests an amendment, a letter is to be sent to the guardian stating that the consumer is requesting an amendment, and further requesting that the guardian complete the Request for Amendment form.

H. If the request is granted, CCDDR shall:

1. Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment, and then document the change in the same section of the record as the original information.
2. Inform the consumer that the amendment is accepted.
3. Obtain the authorization of the consumer to notify all relevant persons or entities with whom the amendment needs to be shared.
4. Within a reasonable time frame, make reasonable efforts to provide the amendment to the persons identified by the consumer, and any persons, including business associates, that CCDDR knows has been provided the PHI that is the subject of the amendment and who may have relied on or could foreseeably rely on the information to the detriment of the consumer. A reasonable time frame is defined as attempts to complete this process within 60 days of the date of the amendment to the record.
5. If the amendment affects a service for which billing or a charge has already been submitted, then the billing must be reviewed to see if it should be amended or changed as well to reflect the new information.

I. CCDDR may deny the request for amendment to PHI if the health information that is the subject of the request if:

1. The information was not created by CCDDR. However, if the consumer can provide reasonable proof that the person or entity that created the information is no longer available to make the amendment, and the request is not denied on other grounds, CCDDR must amend the information.

2. The information is not part of the medical information kept by or for CCDDR.
3. The information is not part of the information that the consumer would be permitted to inspect and copy
4. The information is accurate and complete.

J. If CCDDR denies the requested amendment, it must provide the consumer with a timely, written denial, written in plain language that contains:

1. The basis for the denial;
2. The consumer's right to submit a written statement disagreeing with the denial and how the consumer may file such a statement;
3. The name, title, address, and telephone number of the person to whom a statement of disagreement should be addressed;
4. The steps to file a complaint with the Secretary of HHS;
5. A statement that if the consumer does not submit a statement of disagreement, the consumer may request that CCDDR provide the Request for Amendment and the denial with any future disclosures of PHI.
6. A copy must also be provided to the guardian, if applicable; to parent(s), if applicable; or to DFS if that agency has legal and physical custody of the juvenile.

K. Consumers shall be permitted to submit to CCDDR a written statement disagreeing with the denial of all or part of a requested amendment and the basis for the disagreement. This statement of disagreement shall be limited to one page.

1. The statement of disagreement shall be submitted in writing to the CCDDR Director.
2. CCDDR may prepare a written rebuttal to the statement of disagreement and must provide the consumer with a copy of the rebuttal.
3. CCDDR must identify the record of PHI that is the subject of the disputed amendment and append or link the request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the CCDDR rebuttal statement if any.

L. If the consumer has submitted a statement of disagreement, CCDDR must include the documents or an accurate summary of the information, with any subsequent disclosure of the PHI to which the disagreement relates.

M. If the consumer has not submitted a written statement of disagreement, CCDDR must include the consumer's request for amendment and its denial, or an accurate summary of the information, with any subsequent disclosure of PHI only if the consumer has requested it.

N. If CCDDR receives information from another source of an amendment of a consumer's PHI, the PHI from that sending facility must be amended in written or electronic form.

XI. Request To Restrict PHI

A. Consumers shall indicate their request for restriction on the use or disclosure of their PHI using the "Request to Restrict Information" form.

B. The requested restrictions must be provided in writing, signed and dated by the consumer or personal representative.

C. The CCDDR Privacy Officer must receive the written request. The Privacy Officer shall determine whether it will be approved using the following procedure:

1. If approved, CCDDR must implement the restriction.
2. The CCDDR Privacy Officer will identify the restriction on the face sheet of the consumer's confidential file.
3. CCDDR's agreement or refusal of the request shall be documented on the request form, signed and dated by the Privacy Officer.
4. The original will be filed for permanent retention
5. A copy of the approved or denied form will be provided to the consumer.

D. CCDDR may terminate the agreement to a restriction if:

1. The consumer agrees to or requests the termination in writing.
2. The consumer orally agrees to the termination and the oral agreement is documented.
3. CCDDR informs the consumer that it is terminating its agreement to a restriction and that such termination is only effective with respect to PHI created or received after it has so informed the individual.
4. When any of the above criteria are met, the restriction will be removed, and the form will be dated and signed by the Privacy Officer.
5. If the restriction was identified on the face sheet of the consumer's confidential file, that identification shall be removed by the Privacy Officer.

E. If CCDDR has agreed to the restriction, but the consumer who requested the restriction is in need of emergency treatment, and the restricted PHI is needed to provide the emergency treatment, CCDDR may disclose that PHI to a health care provider to provide such treatment.

F. If such PHI is disclosed in an emergency situation, CCDDR must require that the health care provider to whom the information was disclosed not further use or disclose that PHI.

XII. Consumer Right To Access PHI

A. A consumer who has or is receiving services from CCDDR, parent of a minor, and personal representative or legal guardian as relevant to their representation, must request in writing for access to inspect, or receive copies of, Protected Health Information except in those instances covered by Federal Regulation and outlined in the Notice of Privacy

Practices acknowledged at admission, and must further specify the exact information requested for access.

B. The "Request for Consumer Access to Their Protected Health Information" form shall be provided to facilitate the request. CCDDR personnel may assist in initiating the process requesting access to Protected Health Information.

C. All requests by consumers and their legal representatives for PHI must be forwarded to the Privacy Officer for action.

D. If it is acceptable after discussion with the consumer, CCDDR may provide a summary of the PHI to the consumer. If the summary is acceptable, CCDDR shall determine the appropriate staff to provide that explanation to the consumer. The consumer's agreement to a summary shall be documented in writing in the record as a check in the appropriate box in the "Request for Consumer Access to Their Protected Health Information" form. The form shall be filed in the consumer's confidential file.

E. This request shall be processed in the format requested i.e. microfiche, computer disk, etc, if possible, and in a timely consistent manner according to established timeframes but not more than 30 days after receipt of the request. If the record cannot be accessed within the 30 days, the timeframe may be extended once for no more than an additional 30 days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

F. Requests for Access to Protected Health Information may be denied without a right to review as follows:

1. If the information conforms to one of the following categories: psychotherapy notes; information compiled for use in a civil, criminal or administrative action or proceeding; or information that would be prohibited from use or disclosure under the Certified Laboratory Information Act (CLIA) laws and regulations;
2. If the consumer is participating in research related treatment and has agreed to the denial of access to records for the duration of the study;
3. If access is otherwise precluded by law;
4. If the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. All Victim Notification and Duty To Warn forms, as well as any other documentation that contains demographics of victims or potential victims shall be removed before any review of the record by anyone not employed by CCDDR, and if the CCDDR employee is a consumer worker, then the information shall be removed before any review of the record; or
5. If CCDDR has been provided a copy of a court order from a court of competent jurisdiction which limits the release or use of PHI.

G. Requests for Access to Protected Health Information may be denied provided the individual is given a right to have the denial reviewed as follows:

1. A licensed health care professional based on an assessment of the particular circumstances, determines that the access requested is reasonably likely to endanger the life or physical safety of the consumer or another person.
2. CCDDR may deny the consumer access to PHI if the information requested makes reference to someone other than the consumer and a licensed health care professional has determined that the access requested is reasonably likely to cause serious harm to that other person.
3. CCDDR may deny a request to receive a copy or inspect PHI by a personal representative of the consumer if CCDDR has a reasonable belief that the consumer has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and CCDDR, exercising professional judgment, decides that it is not in the best interest of the consumer to treat that person as the consumer's personal representative.

H. Upon denial of any request for access to PHI, in whole or in part, a written letter shall be sent to the consumer, or other valid representative making the request for access, stating in plain language the basis for the denial.

1. If the consumer has a right to a review of the denial, the letter shall contain a statement of how to make an appeal of the denial including the name, title, address, and telephone number of the person to whom an appeal should be addressed.
2. This letter shall also address the steps to file a complaint with the Secretary of HHS.
3. If the information requested is not maintained by CCDDR, but it is known where the consumer may obtain access, CCDDR must inform the consumer where to direct the request for access.

I. A consumer, parent of a minor, or guardian of a consumer has the right to appeal the decision to withhold portions or all of the record for safety or confidentiality reasons as follows:

1. The appeal shall be submitted in writing to the CCDDR Privacy Officer, who will designate a licensed health care professional.
2. The designated licensed health care professional who did not participate in the original decision to deny access shall review the record and the request for access to the consumer's record.
    a. The reviewer must determine if access meets an exception.
    b. If the reviewer determines that the initial denial was appropriate, the consumer must be notified in writing, using plain language that the review resulted in another denial of access. The notice must include the reasons for denial and must describe the process to make a complaint to the Secretary of HHS.
    c. If the denial was not appropriate, the licensed health care professional who acts as the reviewer shall refer the request to the CCDDR Privacy Officer for action.
3. If access is denied to any portion of the PHI, access must still be granted to those portions of the PHI that are not restricted.
4. CCDDR is bound by the decision of the reviewer.

J. If CCDDR provides a consumer or legal representative with access, in whole or in part, to protected health information, CCDDR must comply with the specifications as outlined in federal regulations to the extent of CCDDR' capabilities and as identified in the Notice of Privacy Practices.

1. Requested information must be provided in designated record sets.
2. If the requested information is maintained in more than one designated record set or in more than one location, CCDDR only needs to produce the information one time in response to the request.
3. CCDDR may provide a summary or explanation of the requested PHI if:
   a. The consumer agrees in advance to the summary or explanation in place of the record.
   b. The consumer agrees in advance to any fees imposed for the summary or explanation.
4. If the requested information is maintained electronically and the consumer requests an electronic or faxed copy, CCDDR must accommodate the request if possible and should explain the risk to security of the information when transmitted as requested.
5. If the information is downloaded to a computer disk, the consumer should be advised in advance of any charges for the disk and for mailing the disk. CCDDR shall establish a reasonable cost for the duplication of this information on a disk.
6. If the information is not available in the format requested, CCDDR must produce a hard copy document or other format agreed upon by the consumer and CCDDR.

K. CCDDR shall provide the access requested in a timely manner and arrange for a mutually convenient time and place for the consumer to inspect the PHI or obtain copies, unless access by another method has been requested by the consumer and agreed to by the CCDDR. Any requests for accommodations shall be sent or given in writing to the Privacy Officer.

L. The fee charged will be in compliance with the current Missouri State Statute (See Section 191.227, RSMO), and federal law.

M. The PHI of a deceased consumer may only be released via a Probate Court order from the County Circuit Court where the deceased resided or from another Probate Court in the State of Missouri.

N. Upon request to obtain information, the Privacy Officer shall ask for a copy of the Probate Court Order.

XIII. Workforce Compliance

A. CCDDR workforce members shall be granted access to protected health information (PHI), whether written, electronic or verbal in nature, in accordance with state and federal law (HIPAA, P.L. 104-191); (42 CFR Part 2 et seq.); and other relevant CCDDR policies. Such access shall be limited to the minimum necessary amount of protected health

information to accomplish the purpose of any requested use or disclosure of PHI, e.g. to the amount of PHI the employee or workforce member needs to know in order to accomplish their job or task. In addition, communications between workforce members which involve PHI shall also be considered confidential and should not take place in public areas. If it is absolutely necessary to conduct such conversations in public areas, reasonable steps shall be taken to assure the confidentiality of the PHI.

B. Consumer PHI should never be removed from CCDDR office without specific authorization from the Privacy Officer. CCDDR shall establish a procedure for how workforce members are to physically access PHI in confidential records (i.e. how to sign records in and out and under what conditions, etc.).

C. If PHI in any form is lost or stolen, the Privacy Officer should be notified as soon as practical, but no later than two (2) business days after the loss is discovered, in order for the Privacy Officer to initiate the mitigation process.

D. The CCDDR workforce members shall be informed of their obligations with respect to PHI in accordance with CCDDR by mandatory participation in HIPAA Privacy Training.

E. Required Confidentiality Agreement: The CCDDR workforce members that receive or maintain PHI shall be required to agree to the protection of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement. A copy of the signed confidentiality statement shall be maintained in the personnel file of CCDDR staff or volunteers.

F. Visitors: Visitors to CCDDR are not required to sign the confidentiality agreement. However, a copy of the confidentiality agreement shall be located next to the Visitor Sign-in materials and available for review by each visitor.

XIV. Mandatory Training

A. All employees of CCDDR, as well as volunteers, students and contract employees of CCDDR on a regular course of business shall attend training on the privacy and security provisions of HIPAA. This training shall follow a specific curriculum established by the DMH HIPAA Core Team, on file in the CCDDR office.

1. Trainings shall be conducted at the CCDDR facility or designated location.
2. Additional mandatory privacy training shall be scheduled whenever there is a material change in the Department of Mental Health's (DMH) privacy policies or procedures as determined by the Department's Privacy Officer.
3. Periodic mandatory security training shall be scheduled as determined by the Department's Security Officer.

B. CCDDR employees shall receive training as part of their initial employee orientation. The content for the HIPAA new employee orientation shall be the same as listed in paragraph A. However, any interactive exercises, or supplemental videos, will not be required content for new employee orientation. HIPAA new employee orientation must take place within 30 days of the date of hire.

C. Volunteers, students and contract employees for CCDDR on a regular course of business shall receive training as a part of their initial CCDDR orientation (also known as the new employee orientation course). The content for the HIPAA initial CCDDR orientation shall be the same as listed in paragraph A to this policy. However, any interactive exercises, or supplemental videos, will not be required content for initial CCDDR orientation. Such training must be done within 30 days of the initial date that the person presents for service.

D. The CCDDR Privacy Officer shall identify group(s) or individuals who, due to the nature of their job function within CCDDR, will require in-depth training related to HIPAA and CCDDR's policies, and then provide that specialized training.

E. Documentation of Mandatory Training: Documentation of Mandatory HIPAA Training shall be recorded by the CCDDR Privacy Officer.

XIV. Field Practices

A. PHI that is unattended shall be secured in a manner to protect such information from persons without authorized access to this PHI.

B. Vehicles containing any PHI shall be kept locked while unoccupied. PHI shall be kept locked in the trunk of the vehicle, when possible. In the event of extreme temperature situations, an electronic device (laptop, personal digital assistant etc.) containing PHI shall be maintained in the temperature controlled cab in a case while the vehicle is occupied.

C. In the event of a vehicle accident any CCDDR employee who suspects there is PHI in the vehicle shall 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).

D. Upon an employee leaving an area where they have materials containing PHI, e.g. to use the restroom, the employee shall take the materials with them or ensure that the area is protected from viewing by those without authorization by locking the area, or informing CCDDR personnel if they are CCDDR records, or using some other reasonable intervention.

E. Electronic devices containing PHI and other forms of PHI shall not be left in a hotel room for the day when cleaning service is expected. Upon leaving the hotel, employees shall take these items with them or ensure they are locked in the valuables area at the front desk or locked in a safe in the room if one is available. Should this not be possible, each document that is contained on the laptop shall be password protected on an individual basis.

F. Employees shall travel in the field taking only PHI necessary to carry out their duties.

G. Any documentation or equipment such as laptops, pagers, briefcases, palm pilots, etc. that may contain PHI shall be secured from access by those without authorization to the PHI. This includes all locations including an employee's home. Again, each document that is contained on the laptop shall be password protected on an individual basis.

H. Data contained on all laptops, etc., should be backed-up to a disk or to the network when at all possible to avoid loss of valuable consumer protected health information.

I. If PHI in any form is lost or stolen, the CCDDR Privacy Officer should be notified as soon as practical, not to exceed two business days, in order to initiate the mitigation process.

J. PHI that is potentially within view of others, even if CCDDR staff is present, shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI:

    1. All PHI within a vehicle shall be maintained so as to protect from plain view through the windows of the vehicle.
    2. Any electronic device containing PHI shall not have the screen placed in view of others and if left unattended briefly, a screen saver with password shall be employed consistent with CCDDR's security requirements.
    3. All documentation containing PHI shall be maintained out of the view of unauthorized persons.
    4. While working with PHI, the employee shall keep the documentation within line of sight or within arm's reach.
    5. This documentation shall be viewed in the most private settings available.
    6. Only PHI documentation necessary for the task at hand shall be in view.
    7. Briefcases containing PHI shall remain closed when not in use.
    8. When having PHI material copied, the employee shall ensure that this material is only viewed by authorized persons.
    9. When the employee is finished with reviewing CCDDR records containing PHI, the records shall be returned promptly to their appropriate storage area.

K. Employees shall send and receive faxed materials containing PHI to and from CCDDR facility only, unless such facility is not readily available and timely transmission of records is necessary for safety needs. If in non-CCDDR locations:

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

L. Any CCDDR identifying information shall not be in plain view such as agency logo on a notebook or briefcase, etc.

M. When using sign language interpreters where PHI may be transmitted, the most private setting available out of view of others shall be used.

N. PHI that is verbally transmitted to others shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI.

O. Conversations where PHI is discussed shall occur in the most private settings. There shall be as much distance as possible between any individuals without authorized access to the PHI.

1. Conversations where PHI is discussed shall occur with the employee using a volume level which cannot be overheard by those without authorized access to the PHI. This includes telephone conversations. If there is no way to prevent being overheard, a specific code shall be used to identify an individual such as chart number, or consumer initials.
2. The employee shall make every effort to keep the volume level of all participants' low enough so as to not be overheard.
3. Conversations shall involve using only the first name of an individual whenever possible.

P. Wireless/cellular and cordless telephones shall be used for communicating PHI only if necessary.

1. Home cordless telephones can be monitored up to one mile away. The employee shall switch to their regular landline telephone (if available) or digital cellular telephone for increased security if they receive a call on a cordless telephone. Employees shall not communicate PHI on a cordless telephone, unless using a code specified previously.
2. There is currently no device to monitor digital cellular telephone calls, so PHI discussions are currently acceptable. The employee shall not communicate PHI on analog cellular telephones.

Q. PHI that may be shared with others in the course of an employee carrying out duties shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI.

REFERENCES:

- Health Insurance Portability And Accountability Act Of 1996/Public Law 104-191