Policy Number:
25
Effective: March 19, 2007
Revised: October 16, 2017, November 12, 2020

Subject: HIPAA Compliance

POLICY:

Camden County Developmental Disability Resources (CCDDR) shall have a policy in order to be compliant with the Health Insurance Portability and Accountability Act of 1996.

Definitions

Protective Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity, health plan, or clearing house as defined under the Health Insurance Portability And Accountability Act (HIPAA 45 CFR part 160 and 164).

CCDDR Privacy Officer: CCDDR's Executive Director and/or designee assigned by the Executive Director.

I. Notice of Privacy Practices

A. At the date of the first delivery of, appearance for service at the CCDDR facility, or application for services (even those services received electronically with CCDDR), the client or their legal guardian or parent (if a minor) should be presented with the Department of Mental Health (DMH) Notice of Privacy Practices. This is considered the initial contact between the client and CCDDR. The sending of an application packet is not considered the initial contact. When the client is presented with the Notice of Privacy Practices, CCDDR will make every effort to obtain written acknowledgment of receipt for the Notice of Privacy Practices.

1. Documentation of acknowledgment on the current Notice of Privacy Practices' acknowledgement sheet that such a Notice has been presented to a client (or their legal guardian or parent, if a minor) for review must be signed and placed in the client's record. The full Notice of Privacy Practices is then given to the client.
2. If CCDDR does not obtain the acknowledgment, then CCDDR will 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.
3. In emergency treatment situations, the Notice of Privacy Practices and a good faith attempt to have the client sign the Notice should be initiated at admission or prior to

dismissal, whichever is sooner. If personal contact is not possible, the Notice of Privacy Practices can be mailed for client signature.

B. A copy of the Notice of Privacy Practices is given to each client at their annual plan meeting. This provides clients the opportunity to discuss privacy practices with their Support Coordinator.

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

D. CCDDR's Privacy Officer or designee will be responsible for ensuring that CCDDR employees are trained regarding the Notice of Privacy Practices.

E. Client questions related to the Notice of Privacy Practices should be directed to the CCDDR Privacy Officer or designee.

F. The CCDDR Privacy Officer or designee will 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 Support Coordinators, staff members, and providers may share medical information with each other about DMH clients served in common for the purpose of general treatment, payment, or health care operations without the consent of the client, parent, or guardian. CCDDR may not use or disclose PHI without a valid authorization completed by the client, parent, guardian, or applicable personal representative with limited exceptions. The CCDDR Privacy Officer or designee will obtain written information regarding the identity of the requestor as well as the date, nature, purpose of the request, and the authority the requestor has to request such information. If other staff receive a completed authorization form for the release of PHI, they will direct it to the CCDDR Privacy Officer or designee for review.

B. Any disclosures that occur will 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 client authorizes the disclosure
- Disclosures required by law

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

- To a public health authority (i.e. required reporting to the Missouri Department of Health and Senior Services)
- To report child abuse/neglect situations, and other situations involving exploitation, abuse, neglect or domestic violence (if disclosure is allowed by law)

- To the Food and Drug Administration
- To a health oversight agency for activities authorized by law (i.e. audits, invitations, inspections, licensure)
- To judicial or administrative proceedings (a subpoena from a court is not necessarily enough)
- 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, RSMo])
- To avert a serious threat to health or safety
- Governmental functions (such as national security and veterans' information)
- To other agencies administering public benefits
- To medical examiners, coroners, and funeral directors
- For organ and tissue donation
- For authorized research purposes
- If there is an emergency or if CCDDR is required by law to discuss certain information
- To assist in communication barriers in obtaining a consent from a client
- Appointment reminders
- Treatment alternatives and health related benefits and services
- Emergency or disaster events for individuals involved in disaster relief
- Protective Services for the President and others
- Workers Compensation
- Public Health Risk, which includes prevention or control of disease; injury; disability; and/or report birth, deaths, abuse, neglect, and exploitation
- Correctional facility inmates

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

E. If it is CCDDR requesting the client complete the authorization, CCDDR must provide the client with a copy of the signed authorization.

III. <u>Accounting of PHI Disclosures</u>

A. All written and verbal communication requests on PHI need to be tracked. 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:

- Disclosures made for treatment, payment, and healthcare operation purposes
- Disclosures made to the client.
- Disclosures made for facility directory purposes, if utilized
- Disclosures made for national security or intelligence purposes
- Disclosures made to correctional institutions or law enforcement officials

- Disclosure made 6 years prior to the date the accounting was requested
- 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 or designee should this situation arise.

B. The CCDDR Privacy Officer or designee shall assure that a plan is in place which tracks disclosure of both written and verbal PHI.

C. CCDDR may assist clients filling out the Request for Accounting of Disclosures:

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 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 client (or legal guardian) must make a written Request for Accounting of Disclosures to the CCDDR Privacy Officer or designee. The request shall be on the CCDDR form. Staff may assist the client 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 the Request for Accounting of Disclosure. If CCDDR has disclosed information to a business associate regarding the client requesting the accounting, then CCDDR, through its Privacy Officer or designee, must request an accounting of disclosures of the client'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 client must be informed in writing:

   - The reason for the delay
   - The date the accounting will be provided

   Such notification to the client 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 client in the client's confidential file.

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

A. The client or personal representative must sign a valid authorization for the disclosure of confidential PHI 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 or designee including the following:

- The name of the requesting party or parties
- Any documentation, statements, or representations from the person requesting the PHI of the requestor's authority to request such information (i.e., legal representative of client, law enforcement official, etc.)

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

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

- Presentation of agency identification, credentials, or other proof of government status (a badge, identification card, etc.)
- 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.)
- 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
- A court order

E. The CCDDR Privacy Officer or designee 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 CCDDR Privacy Officer or designee shall verify facsimile numbers of any faxed requests. The main number of the sending agency shall be called, and the fax number verified.

G. The CCDDR Privacy Officer or designee shall verify e-mail addresses by calling requestors. 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. All e-mails containing PHI MUST be encrypted.

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

I. The CCDDR Privacy Officer or designee must review the forwarded information and determine if the documents satisfactorily verify the identity of the requestor and also demonstrate the requestor has authority to request the information under state and federal law.

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

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

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

V. Disclosure of Minimum Necessary Amount of PHI

A. CCDDR will make reasonable efforts to ensure that the minimum necessary PHI is disclosed, used, or requested. Exceptions to the minimum necessary requirement include:

- Disclosures to the individual who is the subject of the information
- Disclosures made pursuant to an authorization
- Disclosures to or requests by healthcare providers for treatment purposes
- Disclosures required for compliance with the standardized HIPAA transactions
- Disclosures made to Health & Human Services/Office of Civil Rights (HHS/OCR) pursuant to a privacy investigation
- 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 the user's duties. These efforts will include the CCDDR Privacy Officer or designee monitoring staff use and disclosure of PHI.

D. For situations where PHI use and disclosure or PHI requests occur on a routine and recurring basis, the CCDDR Privacy Officer or designee 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 a legitimate or legal authorization), staff will address questions to the CCDDR Privacy Officer or designee to assure that PHI is limited to what 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. Client/Guardian Procedural Safeguards for Improper Use or Disclosure of PHI

DMH and CCDDR encourage clients and service providers to discuss and attempt to resolve issues at the local level.

The following steps constitute the HIPAA complaint process:

A. Fill out the CCDDR Complaint Form

B. Forward a copy of the complaint form to the CCDDR Privacy Officer or designee if the alleged violation took place at CCDDR facility or program.
C. All Privacy Complaints received by the CCDDR Privacy Officer or designee will be date-stamped upon arrival:

- The CCDDR Privacy Officer or designee will review and act on the complaint in a timely manner and not more than 30 days from receipt of the complaint – if additional time is necessary to review and investigate the complaint, the CCDDR Privacy Officer or designee shall, within 30 days, notify the client of the delay, and inform the grievant of the expected timeframe for completion of the review
- The CCDDR Privacy Officer or designee shall determine what PHI is affected by the complaint and if the PHI was provided to other covered entities and business associates
- 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 client making the complaint

D. The CCDDR Privacy Officer or designee will determine if there is cause to believe 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 client, guardian, and/or legal representative.
2. If cause exists to believe a violation has occurred, the CCDDR Privacy Officer or designee 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
    - A recommendation should be made to the Board of Directors to establish a new Privacy Policy or change the existing CCDDR policy.

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

E. If the complaint resolution finds that no cause exists to believe a violation occurred, then the client or client's legal representative may seek resolution to the CCDDR Board of Directors directly (if it is a CCDDR based complaint).

1. The client or client's legal representative, through completion of the Complaint Form, will request that the CCDDR Privacy Officer or designee 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.

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

- The original determination of the CCDDR Privacy Officer or designee is accurate
- Remediation should occur through increased training or a recommendation be made for possible disciplinary action
- A recommendation for CCDDR policy review be initiated
- A recommendation be made for the establishment of a new CCDDR policy

G. The original complaint form shall be placed in the client's confidential file.

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

- Person or entity making the complaint
- Date complaint was received
- A list of the PHI affected
- Status of a complaint
- A list of business associates or facilities affected
- Actions taken

I. There shall be no retaliation against any client or against a workforce member for assisting a client to file a CCDDR complaint regarding CCDDR management of PHI or a report of breach of privacy and security of PHI.

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

A. CCDDR shall identify all information systems (defined as an organized collection of information) that contain PHI.

B. That inventory shall be maintained by the CCDDR Privacy Officer or designee. Any new, modified, or defunct systems will be added to or removed from the inventory by the Privacy Officer or designee.

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 client care or payment decision making, including (but not limited to):

- Medical and billing records about clients maintained by or for CCDDR
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for CCDDR

- Any records or information used, in whole or in part, by or for CCDDR to make decisions about clients

D. Information not part of the Designated Records Set is defined as follows:

1. 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 client or any work therapy employment files; integrated risk assessment including serious incident history, index crime report, annual synopsis of endangering behaviors, recent predictive behaviors, request for passes and privileges, forensic release request, law enforcement reports, victim notification information; or REJIS, MULES, or NCIC report. However, these types of information may be accessible by parents or guardians. In addition, for forensic case evaluations (defined in section 552 or 557, RSMo), 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.
2. For forensic cases, any forensic evaluation or any correspondence relating to the forensic commitment is not part of the designated records set.
3. For persons referred, considered for referral, or committed (pursuant to section 632.525 RSMo), risk assessments, probable cause evaluations, court-ordered evaluations, and annual reports are not part of the designated records set.
4. Working files, either paper or electronic, are not considered part of the designated records set. Examples of this information may include, but are not limited to, copies of the current personal plan, IEP, guardianship information, MOCABI or Vineland, client budgets, correspondence (including e-mail), face or cover sheet (including demographic information), behavior support plan, discharge summary, any necessary monthly or quarterly reports, authorizations, conditional release plan, etc.
5. Psychotherapy notes are not included in the designated records set and are to be kept separate from the medical record.

E. When an individual or department have been given sanctioned, exclusive possession and control of PHI as part of their assigned duties, the individual or department 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 or department does not have the technical expertise or equipment to adequately protect the PHI, the individual or department must arrange for technical assistance either through the Information Systems or Health Information Management Departments to assure the confidentiality of the PHI. Any field staff must refer to DMH DOR 9.080.

F. The designated record set will be created, stored, released, transported, copies and destroyed based on DMH DOR 8.110 Record Retention and Destruction. Failure to comply or assure compliance with the DOR could result in disciplinary action, up to and including dismissal. The CCDDR Privacy Officer or designee will collect information

from the Local Privacy Officer or designee annually to monitor compliance with the DMH DOR.

VIII. Access to Computerized/Electronic PHI

A. Pursuant to the Electronic Communications Privacy Act of 1986, 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:

- A legitimate business need exists that cannot be satisfied by other means
- The involved employee is unavailable, and timing is critical to a business activity
- There is reasonable cause to suspect criminal activity or policy violations
- 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 or designee beforehand. All users shall be required to protect confidential data, and only the minimum necessary data shall be accessed.

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

F. No CCDDR client 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 unless authorized by the client. Any proposed client/client access shall include documentation of the client reviewing and agreeing to a confidentiality statement. Documentation will include the types of systems and files accessed.

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

H. Users are required to abide by the following guidelines when using CCDDR email and internet systems:

1. The internet and email 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. Email may be used to disseminate business-related newsletters, press releases, or other documents to groups of people.
4. Email and the internet may be used for discussion groups on job-related topics.
5. Do NOT use personal email.

I. Email and/or the internet may not be used for:

- Any illegal, private, or unethical purpose
- Downloading software of any kind without prior approval of management
- Participating in personal social media, internet chat rooms, instant messaging, or other similar medias
- Playing games
- Conducting any political activity

J. All CCDDR employees, clients, and volunteers must receive the required HIPAA privacy training.

K. CCDDR workforce members receiving or maintaining 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.

L. CCDDR will utilize password management:

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

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

- Physical access control to CCDDR hardware
- Purging CCDDR data on any type of media before it is discarded
- 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 IT manager/consultant.

F. The CCDDR workforce shall not load software, from any source, on to their assigned workstation without prior authorization from the Executive Director. This software includes, but is not limited to, software from the internet, a CD, or other external device or media. Software must be approved by the Executive Director prior to being loaded on workstations.

X. Client/Guardian Right to Amend PHI

A. A client, parent of a minor, and personal representative or legal guardian, as relevant to the client's representation, who believes information in the client's 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 client 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 client provides the name of a new private physician or other professional whom the client 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 to Amend 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 client.

C. All requests for amendment of PHI must be forwarded to the CCDDR Privacy Officer or designee, who will route the original request to the author of the PHI or the individual's supervisor. If the author choses to add a comment to the request form, a second copy of the form will be given to the client with the author's comments.

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

E. 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 the reasons for the delay and the date the request will be concluded.

F. If a client with a guardian requests an amendment, a letter is to be sent to the guardian stating that the client is requesting an amendment, and further requesting that the guardian complete the request for amendment form.

G. 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 client that the amendment is accepted.
3. Obtain the authorization of the client to notify all relevant persons or entities with whom the amendment needs to be shared.
4. Within 60 days, make reasonable efforts to provide the amendment to the persons identified by the client, 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 client.
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.

H. CCDDR may deny the request for amendment to PHI if:

1. The information was not created by CCDDR. However, if the client 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 client would be permitted to inspect and copy (for specifics on client's access to PHI, see DMH DOR 8.030).
4. The information is accurate and complete.

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

- The basis for the denial
- The client's right to submit a written statement disagreeing with the denial and how the client may file such a statement

- The name, title, address, and telephone number of the person to whom a statement of disagreement should be addressed
- The steps to file a complaint with the Department of Health and Senior Services.
- A statement that if the client does not submit a statement of disagreement, the client may request that CCDDR provide the request for amendment and the denial with any future disclosures of PHI
- A copy must also be provided to the guardian, if applicable; to parent(s), if applicable; or to Department of Social Services if that agency has legal and physical custody of the juvenile

J. Clients 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 will be submitted in writing to the CCDDR Executive Director.
2. CCDDR may prepare a written rebuttal to the statement of disagreement and must provide the client 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.

K. If the client 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.

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

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

XI. Request to Restrict PHI

A. Clients shall indicate their request for restriction on the use or disclosure of their PHI using the "Request for Restrictions on the Use and/or Disclosure of Protected Health Information" form.

B. The requested restrictions must be provided in writing as well as signed and dated by the client or legal representative.

C. The CCDDR Privacy Officer or designee must receive the written request. The Privacy Officer or designee, in consultation with the Executive Director or DMH Privacy Officer or designee, will determine whether it will be approved using the following procedure:

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

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

1. The client agrees to or requests the termination in writing.
2. The client orally agrees to the termination and the oral agreement is documented.
3. CCDDR informs the client 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 or designee.
5. If the restriction was identified on the face sheet of the client's confidential file, that identification shall be removed by the Privacy Officer or designee.

E. If CCDDR has agreed to the restriction, but the client 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. Failure of staff to comply or assure compliance may result in disciplinary action, including dismissal.

XII. Client Right to Access or Receive a Copy of PHI

A. A client who has or is receiving services from CCDDR, parent of a minor, and legal representative or legal guardian as relevant to their representation, must request in writing for access to inspect or receive copies of PHI, 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 to Access or Receive a Copy of Protected Health" form shall be provided to facilitate the request. CCDDR personnel may assist in initiating the process requesting access to PHI.

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

D. If it is acceptable after discussion with the client, CCDDR may provide a summary of the PHI to the client. If the summary is acceptable, CCDDR shall determine the appropriate staff to provide that explanation to the client. The client's agreement to a summary shall be documented in writing in the record as a check in the appropriate box in the "Request To Access or Receive a Copy of PHI" form. The form shall be filed in the client'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 PHI may be denied without a right to review as follows:

- 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
- If the client is participating in research related treatment and has agreed to the denial of access to records for the duration of the study
- If access is otherwise precluded by law
- 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 client worker, then the information shall be removed before any review of the record
- 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 PHI 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 client or another person.
2. CCDDR may deny the client access to PHI if the information requested makes reference to someone other than the client 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 client if CCDDR has a reasonable belief that the client has been or may be subjected to domestic violence, abuse, or neglect by such person; 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 client to treat that person as the client'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 client, or other valid representative making the request for access, stating in plain language the basis for the denial.

1. If the client 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 client may obtain access, CCDDR must inform the client where to direct the request for access.

I. A client, parent of a minor, or guardian of a client 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 or designee, 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 client's record.

    a. The reviewer must determine if access meets an exception.
    b. If the reviewer determines that the initial denial was appropriate, the client 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 or designee 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 client or legal representative with access, in whole or in part, to PHI, CCDDR must comply with the specifications as outlined in federal regulations to the extent of CCDDR's 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:

    - The client agrees in advance to the summary or explanation in place of the record
    - The client agrees in advance to any fees imposed for the summary or explanation

4. If the requested information is maintained electronically and the client 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 client 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 client and CCDDR.

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

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

M. The PHI of a deceased client 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 or designee shall ask for a copy of the Probate Court Order.

XIII. Workforce Compliance

A. CCDDR workforce members shall be granted access to 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 PHI 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. Client PHI can be taken outside the office building with specific authorization from the Privacy Officer or designee upon receipt of a court order which subpoenas the records or if a record is being transported to the DMH Regional Office due to discharge or transfer of a client.

C. If PHI in any form is lost or stolen, the Privacy Officer or designee 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 or designee 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. 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 HIPAA Confidentiality Statement. A copy of the signed confidentiality statement shall be maintained in the personnel file of CCDDR staff or volunteers.

F. 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 are given a packet regarding HIPAA rules at new hire orientation. After HIPAA information has been reviewed by CCDDR employees, a test is given on the information covered in packet and results of the tests are discussed with the individual. Additional HIPAA training is covered in mandatory courses required by DMH.

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 DMH privacy policies or procedures as determined by the DMH's Privacy Officer or designee.
3. Periodic mandatory security training shall be scheduled as determined by the DMH'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 also be required to 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 excluding mandatory courses required by DMH. 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 or designee shall identify groups 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 HIPAA Training shall be recorded by the CCDDR Privacy Officer or designee.

XV. 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, digital device/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, informing CCDDR personnel if they are CCDDR records, and/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 services are expected. Upon leaving the hotel, employees shall take these items with them, 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, briefcases, 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 encrypted storage device or to the network when at all possible to avoid loss of valuable PHI.

I. If PHI in any form is lost or stolen, the CCDDR Privacy Officer or designee should be notified as soon as practical, not to exceed two (2) 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 facilities 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. Call the receiving location to verify transmission was successful.

L. Any CCDDR identifying information shall not be in plain view such as agency logo on a notebook, 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, which 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 client 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. Conversations where PHI is discussed must be held at a volume level that cannot be overheard and away from individuals without authorized access to the PHI.

REFERENCES:

- Health Insurance Portability and Accountability Act Of 1996/Public Law 104-191, Department of Mental Health DORs.