

HIPAA
Privacy/Confidentiality/Security Policy
Delaware County Board of Developmental Disabilities

DCBDD Review Date: August 18, 2011
DCBDD Resolution # 11-08-08
Effective Date: August 19, 2011
Reviewing Department: Director of Transition Support Administration/Privacy Officer

Philosophy

Confidentiality is the basis for all personal relationships, as well as for the respect due personal privacy. It involves intimacy, trust, confidence, and is the key to any and all therapeutic relationships.

A breach in confidentiality occurs when, enrollee information is passed along to another individuals without the Designated Authority's knowledge and consent, information can be used against the enrollee's welfare or services, information draws undue attention to the disability, rather than normalization capabilities. The goal of all enrollee discussions or information seeking must be to serve the enrollee.

Overview

Delaware County Board of Developmental Disabilities (DCBDD) will conform to all applicable requirements set forth in the Health Insurance Portability and Accountability Act, HIPAA, of 1996, including Electronic Health Care Transactions, Privacy, Confidentiality, and Health Data and Security of Health Data. DCBDD will maintain appropriate policies, procedures, regulations and rules to prevent, detect, contain and correct violations. DCBDD will apply appropriate sanctions against employees who fail to comply with the aforementioned policies and procedures adopted by the Board per its employee disciplinary policy up to and including termination.

Purpose

To safeguard each individual participant's right to privacy and confidentiality in the receipt of services from the Board.

To establish a policy and subsequent procedures for compliance with applicable HIPAA security standards.

To maintain the confidentiality, integrity, and availability of all electronic protected health information (EPHI).

Protect against any reasonably anticipated threats or hazards of the security or integrity of EPHI.

Protect against any reasonably anticipated uses or disclosures of such information that is not permitted or required.

Maintain compliance by the employees of the DCBDD.

Application

The provisions of this directive shall apply to all Board members, employees, volunteers/interns, contract services employees of all departments of the Board

Definitions

A. **Board** means the Delaware County Board of Developmental Disabilities and its designated administration and staff.

B. **Designated Authority** means the person who has legal authority to make decisions on behalf of the individual. For children under the age of 18 the parent or other legal guardian will be the Designated Authority. If the parents are separated or divorced, Designated Authority is the parent with legal custody of the individual with a disability. Designated Authority may also include an individual's guardian, custodian, or parent surrogate. As defined in ORC 3323.05 (B) and Administrative Code 3301-51-02 (F). At age eighteen, the participant must act in his or her own behalf, unless he/she has a court-appointed guardian. This term does not include the state, if an individual is a ward of the state.

C. **Destruction** means physical destruction of a record or removal of personal identifiers from information so that the information is no longer personally identifiable. Transferring information to microfilm or electronically scanned format shall not be considered destruction.

D. **Directory Information** includes the following information relating to a participant: Participant's name, address, telephone number, date and place of department or service, participation in officially recognized activities and sports, weight and height or membership of athletic teams, dates of attendance, and awards received.

E. **Disclosure** means permitting access to or the release or transfer, or other means of communication of records of the participant or the personally identifiable information contained therein, orally or in writing, or by electronic means, or by any other means to any party.

F. **Education/Habilitation Records** mean those records that are directly related to a participant and are maintained by the Board or by a party acting for the agency. The term does not include those records which are excluded under 34 Code of Federal Regulations (CFR), Reg. 909.3.

G. **Enrollee** means the eligible individual for whom the Board has created and maintains a record.

H. **Personally Identifiable Data includes:**

1. The name of the enrollee, the enrollee's family members
2. The address of the enrollee
3. A personal identifier, such as the enrollee's date of birth, social security number, or Medicare number
4. A list of personal characteristics or other information which would make it

possible to identify the enrollee with reasonable certainty

I. **Individual Plan** means Individualized Family Support Plan (IFSP), Individual Education Plan (IEP), Individual Support Agreement or Plan (ISA or ISP) or any other service plan for an individual.

J. **Record** means any information or data recorded in any medium, including, but not limited to: photographs, handwritten, print, tapes, film, microfilm, microfiche and automated data bank.

Security

Procedures

A. Administrative Safeguards

DCBDD will maintain appropriate procedures, regulations, and rules to prevent, detect, contain, and correct security violations.

1. Risk Analysis

DCBDD will conduct an annual accurate and thorough assessment of the potential risk and vulnerabilities of the confidentiality, integrity, and availability of EPHI including hardware, software, and network devices to ensure the security of EPHI.

2. Risk Management

DCBDD maintains security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level through the utilization of Anti-virus software at the server and workstation level, Anti SPAM hardware and services, firewalls, protocol filters and VPN connectivity into the network.

3. Sanction Policy

DCBDD will apply appropriate sanctions against employees who fail to comply with the security policies and procedures adopted by the Board up to and including termination of employment.

4. Information system activity review

DCBDD will regularly review records of information system activity, including but not limited to audit logs, access reports and security incident tracking reports.

5. Security incident procedures

Security incidents will be reported to the Superintendent of DCBDD and appropriate training and discipline will be given.

6. Assigned Security Responsibility

The Director of Information Systems of the DCBDD is the security officer who is responsible for the development and implementation of the policies, procedures, and regulations required to address the purpose of this policy and procedures.

7. Response and reporting

DCBDD will identify and respond to suspected or known security incidents; mitigate, to the extent possible, harmful effects of security incidents that are known and document security incidents and their outcomes.

8. Contingency Plan

DCBDD will maintain EPHI at an offsite data storage center (i.e. InfoLink) for responding to an emergency or other occurrence such as fire, vandalism, system failure, and natural disaster that damages systems that contain EPHI.

9. Data backup plan

DCBDD will create and maintain retrievable exact copies of EPHI each workday.

10. Disaster recovery plan

DCBDD will maintain retrievable copies of EPHI to restore any loss of data.

11. Emergency mode operation plan

DCBDD will maintain the continuation of critical business operations for protection of the security of EPHI while operating in emergency mode. In case of an emergency, appropriate staff will be notified of the emergency and an offsite computer center will be utilized if necessary.

12. Evaluation

DCBDD will perform an annual technical and non-technical evaluation, based upon the HIPAA regulation and subsequently, in response to environmental or operational changes affecting the security of EPHI.

B. Physical Safeguards

1. Workstation Use

DCBDD will maintain the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI through use of usernames, passwords, screen savers and session time limits.

2. Workstation Security

DCBDD will maintain physical safeguards, including lock doors for all workstations that access EPHI, in order to restrict access to authorized users only.

3. Device and Media Controls

DCBDD will monitor the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility. Any movement of hardware and electronic media that contains EPHI must be consistent with the proper protection of EPHI.

4. Disposal

DCBDD will remove or have removed all EPHI before the final disposition and/or the hardware or electronic media on which it is stored.

5. Media Re-use

DCBDD will remove all EPHI from electronic media before the media are made available for re-use.

C. Technical Safeguards

1. Access Control

DCBDD will allow access only to those persons or software programs that have been granted access rights to electronic information systems that maintain EPHI.

2. Unique User Identification

DCBDD will assign a unique name and/or number for identifying and tracking user identity.

3. Emergency Access Procedure

DCBDD will allow (and implement as needed) only as necessary access to EPHI during an emergency.

4. Audit Controls

DCBDD will record and examine activity in information systems that contain or use EPHI, including hardware, software, and/or procedural mechanisms whenever practical.

Confidentiality/Privacy

A. Confidentiality

1. All information contained in an enrollee's records, including information contained in an automated data bank, shall be considered confidential. The content of these records is never the subject for discussion, except as an official member of a habilitation team.

2. DCBDD may permit a business associate to create, receive, maintain or transmit EPHI on DCBDD's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information and a Business Associate Agreement is on file.

B. Responsible person for ensuring confidentiality of records

1. Each program department director or his/her designee shall act as the confidentiality officer of their particular department to ensure the confidentiality of information of each enrollee receiving services from that department.

2. It is the responsibility of the confidentiality officer to see that each enrollee is adequately represented by his/her natural parent(s), parent(s) having legal custody, legal guardian(s) or custodian(s), surrogate parent(s).

3. An enrollee of legal age (18) with no court-appointed legal guardian has the right to act in his/her own behalf in all matters related to confidentiality and records access, consent, maintenance, and destruction. Throughout the remainder of this policy, "Designated Authority" refers to the enrollee, himself/herself, when acting in his/her own behalf as well as the legal guardian of a person.

C. Access Rights

1. The Designated Authority has the right to inspect and review any agency record related to his or her enrollee that is enrolled in any department of the Board; a court-appointed guardian has the same right, with respect to the records of his/her appointee. The agency shall request a copy of the official document stating the parent does not have the authority, under applicable state law, governing such matters as guardianship, separation, and divorce, if the parent's right to access has been restricted or denied.
2. Any program department shall comply with the Designated Authority's requests for access to confidential material without unnecessary delay. Requests occurring before an Individual Planning meeting or a hearing related to identification, evaluation or placement of the enrollee shall have immediate response. In the case of an enrollee placed by the LEA, the response time shall be no more than forty-five days after the request has been made.
3. The Board may charge a fee for copies of records
4. The types of records maintained and available in each department shall include as applicable but are not limited to the following:
 - a. Admission and referral records
 - b. Verification of age
 - c. Emergency contact sheet
 - d. Enrollment for evaluation information
 - i. Interdisciplinary team report
 - ii. Psychological report
 - iii. Medical report
 - iv. Substantial developmental disability determination, if applicable
 - v. Background information
 - vi. Evidence of public school graduation or a certificate of completion or valid public school placement data for program eligibility, if applicable
 - e. Medical reports
 - f. Comprehensive evaluation reports
 - g. Specialist reports
 - h. Special job accommodations
 - i. Current Individual's Plan
 - j. Evidence of Individual Plan reviews and revisions
 - k. Incident reports – maintained in a separate file by the MUI Investigative Agent
 - l. Medication reports
 - m. Internal and external service referrals and reports
 - n. Attendance records
 - o. Individual production and payroll records
 - p. Materials no longer needed for current programming
 - q. The name of the service and support administrator who is the single point of accountability for the individual (Archive)
 - r. Quality Assurance Reviews

- s. Information identifying guardianship, trusteeship or protectorship

D. Records Access

1. An individual's record is removed from a department's jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute, children's services. Enrollee records shall not be removed from the premises for any other reason.
2. Each department shall develop a list of the types and locations of records collected, maintained, or used by them, and shall provide this list to Designated Authority on request.
3. Each department director or designee shall implement procedures to keep a record of parties obtaining or given access to records collected, maintained, or used (except access by the Designated Authority or authorized employees of the department or other educational agency). Record of access/disclosure shall be kept on parties reviewing the files and of parties to whom information is sent, including written documentation of:
 - a. Name of the party
 - b. Date access was given
 - c. Purpose for which the party is authorized to use the data
 - d. Signature authorizing release
4. If any agency record includes information on more than one enrollee, the enrollee or Designated Authority of those enrollees shall have the right to inspect and review only the information relating to their son/daughter or to be informed of that specific information.

E. Amendment of Record at Enrollee or Designated Authority's Request

1. The Designated Authority who believes that information in records collected, maintained, or used under this part is inaccurate or misleading or violates the privacy or other rights of the enrollee may request the department which maintains the information to amend the information.
2. The department director shall direct the request to the Board management team, which shall decide whether or not to amend the information within 30 days after the director, has received the request.
3. If a decision is made not to amend the information in accordance with the request, the director of the department to which the request was directed shall inform the Designated Authority of the refusal and advise the Designated Authority of the right to a records hearing to challenge information in education/habilitation records, to ensure that it is not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the enrollee.
4. A record's hearing shall be scheduled at the Designated Authority's request and will adhere to the following:
 - a. The records hearing shall be held within 30 days after the department director has received the request and the Designated Authority shall be given notice of the date, place, and time, at least 10 days in advance of the hearing.

- b. The records hearing may be conducted by any party, as designated by the Superintendent, including an official of the agency, or another agency who does not have a direct interest in the outcome of the hearing.
- c. The Designated Authority shall be afforded a full and fair opportunity to present evidence relevant to the issues and may be assisted or represented by individuals of his or her choice, at his/her own expense, including an attorney. The hearing representative shall make his/her decision in writing to the Superintendent within 10 days after the conclusion of the hearing. The decision shall be based solely upon the evidence presented at the hearing and shall include a summary of the evidence and the reasons for the decision.

F. Results of Records Hearing

1. If, as a result of the records hearing, it is decided that this information is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the participant, the department director shall amend the information accordingly, and so inform the Designated Authority, in writing.
2. If, as a result of the records hearing, it is decided that the information is not accurate, is misleading, or otherwise in violation of the privacy or other rights of the enrollee, the department director shall inform the Designated Authority of the right to place in the records the agency maintains on the enrollee a statement commenting on the information or setting forth any reasons for disagreeing with the decision of the agency.
3. DCBDD shall maintain any explanation placed in the records of the enrollee under this paragraph as part of the records of the enrollee, as long as the record or contested portion is maintained. If the records of the enrollee or the contested portion are disclosed to any party, the explanation must also be disclosed to the party.

G. Safeguards

1. All Board personnel collecting, maintaining, using, or otherwise having access to personally identifiable data shall be informed of the confidentiality policies and procedures of the agency and are responsible for implementing them.
2. Each department director shall be assigned the responsibility for assuring the confidentiality of any personally identifiable data.
3. Each department shall maintain, for public inspection, a current listing of the names and positions of those employees within the department who may have access to the personally identifiable data.

H. Disclosure of Records Information

1. Except as provided in Section H.3. of this policy, no person shall disclose the identity of an individual who requests programs or services under this chapter or release a record or report regarding an eligible person that is maintained by the Board or an entity under contract with the Board unless one of the following circumstances exists:
 - a. The Designated Authority makes a written request to the Board for, or approves in

writing, disclosure of the individual's identity or release of the record or report regarding the eligible person.

b. Disclosure of the identity of the enrollee is needed for approval of a direct services contract under 5126.032 or 5126.033 of the Revised Code. The Board shall release only the individual's name and general nature of the services to be provided.

c. Disclosure of the identity of the enrollee is needed to ascertain that the Board's waiting lists for programs and services are being maintained in accordance to 5126.042 of the Revised Code and the rules adopted under that section. The Board shall release only the individual's name, the general nature of the programs or services to be provided to the individual, the individual's rank on each waiting list that includes the individual, and any circumstances under which the individual was given priority when placed on a waiting list.

2. DCBDD or entity under contract that discloses an individual's identity or releases a record or report made regarding an eligible person shall maintain a record of when and to whom the disclosure or release was made.

3. At the request of the Designated Authority, DCBDD or entity under contract with DCBDD shall provide the person who made the request access to records or reports of the eligible person. Upon written request, the Board or entity under contract shall provide copies of the records and reports to the Designated Authority. The Board or entity under contract with the Board may charge a reasonable fee to cover the costs of copying. The fee may be waived in cases of hardship.

4. DCBDD shall provide access to any waiting list or record or report regarding an eligible person maintained by DCBDD to any state agency responsible for monitoring and reviewing programs and services provided or arranged by the Board, any state agency involved in the coordination of services for an eligible person, and any agency under contract with the Ohio Department of Mental Retardation and Developmental Disabilities for the provision of protective services pursuant to Section 5123.56 of the Revised Code.

5. When an eligible person who requests programs or services dies, DCBDD or entity under contract with DCBDD shall, upon written request, provide to both of the following persons any reports and records in the board or entity's possession concerning the eligible person:

a. If the report or records are necessary to administer the estate of the person who is the subject of the reports or records, to the executor or administrator of the person's estate.

b. To the guardian of the person who is the subject of the reports or records or, if the individual had no guardian at the time of death, to a person in the first applicable of the following categories first applicable of the following categories:

1. The person's spouse
2. The person's children
3. The person's parent
4. The person's brother or sister

5. The person's uncle or aunt
 6. The person's closest relative by blood or adoption
 7. The person's closest relative by marriage
- c. The Board or entity shall provide the reports and records as requested not later than thirty (30) days after receipt of the request.

I. Transfer of Information

1. When an eligible information relocates to another county within the state of Ohio and is no longer receiving services from DCBDD, or entity under contract with DCBDD, upon written request from the Designated Authority or other County Board of DD, shall transfer pertinent information contained in the enrollee's record in order to expedite enrollment with the County Board of DD that will be providing services and programs. The information shall include as applicable but is not limited to the following:
- a. Eligibility Reports
 - b. Intake information
 - c. Therapy evaluations
 - d. Psychological evaluations
2. Information requested from DODD will be released as requested.

J. Destruction of Information

DCBDD shall notify the Designated Authority prior to destroying any record or report regarding the eligible person. Transferring information to microfilm or electronically scanned format shall not be considered destruction.

K. Social Networks

Privacy does not exist in the world of social media. Please note that DCBDD cannot control the actions of others with whom individuals may choose to share their information. Content contributed to social media sites could encourage detrimental comments; however DCBDD board members, employees, volunteer/interns, contract service employees of all departments of DCBDD must uphold all applicable requirements to maintain confidentiality.

Privacy Promise

It is the goal of DCBDD to maintain the trust and confidence of all individuals receiving services and programs from DCBDD by keeping their personal information confidential.

Contact Us

If you would like further information about our Confidentiality/Security Policy, are concerned with how personal information was collected, maintained, or used in a way that is misleading or violate the privacy or other rights of the eligible individual by contacting:

Complaint or Privacy Officer

7991 Columbus Pike
Lewis Center, Ohio 43035
(740) 201-3600

Complaints

We will investigate all complaints alleging a violation of the terms of this notice and will not retaliate against anyone filing a complaint. If DCBDD determines a complaint is justified, DCBDD will take appropriate measures including, if necessary, amending our policies and procedures.

You may also file a complaint with either:

The Secretary of the U.S. Department of Health and Human Services
200 Independence Ave. SW
Washington, DC 20201
1-877-696-6775

OR

The office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Ave. SW
HHH Building, Room 509 F
Washington, DC 20201
1-800-368-1019
ocrmail@hhs.gov