

Policy 2400 Confidentiality and Privacy
HIPAA, FERPA, IDEA and Ohio Revised Code Compliance

Table of Contents

2400 CONFIDENTIALITY & PRIVACY POLICIES _____ **3**

2400.01 POLICIES FOR ALL STAFF _____ **3**

 2400.01.01 Confidentiality, Privacy and Computer Security Definitions _____ **3**

 2400.01.02 Confidentiality – General Rules _____ **9**

 2400.01.03 Minimum Necessary Policy _____ **10**

 2400.01.04 Confidentiality Safeguards (Oral & Written) _____ **12**

 2400.01.05 Speaking with the Family and Friends of an Individual Receiving Services _____ **14**

 2400.01.06 Authorizations _____ **15**

 2400.01.07 Verification _____ **17**

 2400.01.08 Minors, Personal Representatives and Deceased Individuals _____ **18**

 2400.01.09 Duty to Report Violations and Security Incidents _____ **20**

 2400.01.10 Disclosures that do Not Require an Authorization _____ **21**

2400.02 INDIVIDUAL RIGHTS _____ **25**

 2400.02.01 Individual’s Right to Access Records _____ **25**

 2400.02.02 Individual’s Right to Request Amendment of Records _____ **27**

 2400.02.03 Individual’s Right to Receive an Accounting of Disclosures _____ **29**

 2400.02.04 Individual’s Right to Request Additional Restrictions _____ **31**

 2400.02.05 Individual’s Right to Request Confidential Communications _____ **32**

 2400.02.06 Individual’s Right to Notice of Privacy Practices _____ **33**

2400.03 CONFIDENTIALITY POLICIES FOR SUPERVISORS _____ **34**

 2400.03.01 Business Associate Contracts _____ **34**

 2400.03.02 Non-intimidation and Non-retaliation _____ **35**

 2400.03.03 HIPAA Assignments and Documentation _____ **36**

 2400.03.04 Privacy Complaints _____ **38**

 2400.03.05 Policy Updating and Staff Training _____ **39**

APPENDICES _____ **40**

Appendix A: Identifying Business Associates _____ **40**

Appendix B: Sample HIPAA Business Associate Agreement _____ **42**

Appendix C: Sample Privacy & Security Officer Job Descriptions _____ **45**

Appendix D: Minimum Necessary – Workforce, Disclosures and Requests _____ **47**

Workforce Access to PHI and Safeguards _____ **47**

Procedures for Routine Disclosures of PHI _____ **48**

Procedures for Routine Requests of PHI _____ **48**

Appendix E – Change Log and Formatting Notes _____ **49**

Clermont County Board of Developmental Disabilities (CCBDD) – Authorization Form _____ **50**

Notice of Privacy Practices _____ **51**

CCBDD Disclosure Log _____ **54**

2400 CONFIDENTIALITY & PRIVACY POLICIES

2400.01 POLICIES FOR ALL STAFF

2400.01.01 Confidentiality, Privacy and Computer Security Definitions

POLICY

The following definitions shall apply to Policies 2400 and 2500.

AUDIENCE

All Staff

AUTHORITY

The definitions below are adapted from the federal HIPAA regulations, FERPA regulations, the Ohio Revised Code, and Ohio Administrative Code. In some cases, a definition in a regulation is adjusted to facilitate these policies. For example, the definition of PHI, in these policies, is adapted to include both the information protected by the HIPAA regulations and the information protected by the FERPA regulations.

NORMS

Throughout Policies 2400 (Confidentiality and Privacy Policies) and 2500 (Computer Security) the terms *may*, *must*, *shall* and *should* are used. The following is a guide for interpreting these terms:

- 1) **May** – means a task is suggested, but not required, or that an individual or entity is empowered, but not required, to perform the specified task.
- 2) **Must** – means the individual or entity is required to perform the specified task. See also “Shall”.
- 3) **Shall** – means the individual or entity is required to perform the specified task. See also “Must”.
- 4) **Should** – means the individual or entity is recommended to perform the specified task, even though the task may not be required. When “should” is used, the item is a best-practice recommendation although not absolutely mandated.

DEFINITIONS

- 5) **Access** – means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (Taken from HIPAA regulations.)
- 6) **Administrative safeguards** – are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
- 7) **Agency** – means CCBDD
- 8) **Applicable Requirements** – Applicable requirements mean applicable federal and Ohio law and the contracts between the CCBDD and other persons or entities which conform to federal and Ohio Law.
- 9) **Authentication** – means the corroboration that a person is the one claimed.
- 10) **Availability** – means the property that data or information is accessible and useable upon demand by an authorized person.
- 11) **Breach** – the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information.
Breach *excludes*:
 - A) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.
 - B) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered

entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.

- C) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except for the three exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:

- A) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - B) The unauthorized person who used the PHI or to whom the disclosure was made;
 - C) Whether the PHI was actually acquired or viewed; and
 - D) The extent to which the risk to the PHI has been mitigated.
- 12) **Business Associate (BA)** – A Business Associate, basically, is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The complete definition is included in [Appendix A - Identifying Business Associates](#).
- 13) **Confidentiality** – means the property that data or information is not made available or disclosed to unauthorized persons or processes.
- 14) **Covered Entity** – Covered entity means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA transaction rules.
- 15) **Designated Record Set** – Designated record set means:
 A group of records maintained by or for a covered entity that is:
 B) The medical records and billing records about Individuals maintained by or for a covered health care provider;
 C) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
 D) Used, in whole or in part, by or for the covered entity to make decisions about Individuals.
 For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- 16) **Directory Information** -- as defined in FERPA, means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate; full-time or part-time), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended.
- 17) **Disclosure** – Disclosure means the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the entity holding the information.
- 18) **DODD** – the Ohio Department of Developmental Disabilities
- 19) **Early Intervention Records**. – means all records regarding a child that are required to be collected, maintained, or used under Part C of the Act and the regulations in this part. These are essentially equivalent to FERPA Education Records
- 20) **Education** – Education means activities associated with operating the school including instruction, IHP/IEP preparation, administration, behavioral intervention, extra-curricular activities and other normal school functions. Education shall also include activities associated with early intervention programming.
- 21) **Education Records** – As defined in the FERPA regulations, means records that are:
 A) Directly related to a student; and
 B) Maintained by an educational agency or institution or by a party acting for the agency or institution.
 The term does **not** include:
 A) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.

- B) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
- C) Either of the following:
 - i) Records relating to an Individual who is employed by an educational agency or institution, that:
 - 1) Are made and maintained in the normal course of business;
 - 2) Relate exclusively to the Individual in that Individual's capacity as an employee; and
 - 3) Are not available for use for any other purpose.
 - ii) Records relating to an Individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (C)(i) of this definition.
- D) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
 - i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
 - ii) Made, maintained, or used only in connection with treatment of the student; and
 - iii) Disclosed only to persons providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution.
- E) Records created or received by an educational agency or institution after an Individual is no longer a student in attendance and that are not directly related to the Individual's attendance as a student.
- F) Grades on peer-graded papers before they are collected and recorded by a teacher.
- 22) **Employee** – Employee means any person employed by the Agency, volunteers, board members and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.
- 23) **Encryption** – means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 24) **Facility** – means the physical premises and the interior and exterior of a building(s).
- 25) **FERPA** – FERPA means the Family Educational Rights and Privacy Act, which are federal regulations that govern the privacy of records maintained by schools, as well as the rights of parents and students to access those records. These regulations are codified in [CFR Title 34 Part 99](#).
- 26) **Guardian of the Person** – Guardian of the Person means a person appointed by the Probate Court to provide consent for and make decisions for the ward
- 27) **Health care** – means care, services, or supplies related to the health of an Individual. Health care includes, but is not limited to, the following:
 - A) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and
 - B) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
- 28) **Health Care Clearinghouse** – A Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system or community health information system that does either of the following functions:
 - A) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
 - B) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
- 29) **Health care operations** – means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
 - A) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
 - B) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and

- provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- C) Except as prohibited under §45 CFR § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §45 CFR § 164.514(g) are met, if applicable;
 - D) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
 - E) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
 - F) Business management and general administrative activities of the entity, including, but not limited to:
 - i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
 - ii) Resolution of internal grievances;
 - iii) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
 - iv) Consistent with the applicable requirements of [§45 C.F.R. Part 164.514](#), creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.
- 30) **Health Oversight Agency** – Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
- 31) **Health Plan** – Health plan means an individual or group plan that provides, or pays the cost of medical care. A partial list of entities that are health plans (edited based on relevance to DD Boards) includes the following, singly or in combination:
- A) The Medicaid program under title XIX of the Act, [42 U.S.C. § 1396](#), et seq.
 - B) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.
 - C) A group health plan, that is, an employee welfare benefit plan (as defined in section 3(1) of the Employment Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1), including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents, that:
 - i) Has 50 or more participants; or
 - ii) Is administered by an entity other than the employer that established and maintains the plan.
 - D) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
- 32) **HIPAA** – HIPAA means the Health Insurance Portability and Accountability Act of 1996, codified in [42 USC §§ 1320 - 1320d-9](#) and at 42 CFR Parts 160, 162 and 45 CFR § 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.
- 33) **IDEA** – Individuals with Disabilities Education Act. Part C details rights and safeguards for infants aged 0-2 involved with Early Intervention programs, and Part B details rights and safeguards for children aged 3-18.
- 34) **Incidental Disclosure** – An unintentional disclosure of PHI, that occurs as a result of a use or disclosure otherwise permitted by the HIPAA Privacy Rule. An Incidental Disclosure is NOT a violation of the Privacy Rule. However, in order for incidental disclosures to not be a violation, the covered entity must be in compliance with the requirement for implementation of the minimum necessary principle, and also in compliance with the requirement to implement physical, technical, and administrative safeguards to limit incidental disclosures.

- 35) **Individual, Individual receiving services or Individual served** – Means a person who receives services from the Agency. Note that parents or minors, guardians and other “personal representatives” may exercise any right or privilege available to an Individual served.
- 36) **Individually Identifiable Health Information** – is information that is a subset of health information, including demographic information collected from an Individual, and:
- A) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - B) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
 - i) That identifies the Individual; or
 - ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.
- 37) **Information system** – means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
- 38) **Integrity** – means the property that data or information have not been altered or destroyed in an unauthorized manner.
- 39) **Malicious software** – means software, for example, a virus, designed to damage or disrupt a system.
- 40) **MOU** – MOU means a Memorandum of Understanding between governmental entities, which incorporates elements of a business associate contract in accordance with HIPAA rules.
- 41) **Parent** – Parent means either parent. If the parents are separated or divorced, "parent" means the parent with legal custody of the child. "Parent" also includes a child's guardian, custodian, or parent surrogate. At age eighteen, the participant must act in their own behalf, unless they had a court-appointed guardian
- 42) **Password** – means confidential authentication information composed of a string of characters.
- 43) **Payment** – means, in the context of a County Board of DD:
- A) Both:
 - i) Activities by the Agency required to determine if a person is eligible for services, and
 - ii) Activities of the Agency either to reimburse contracted providers for services rendered to Individuals served or seeking reimbursement, for example from Medicaid or DODD, for services rendered to an Individual served.
 - B) The activities in paragraph (A) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:
 - i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
 - ii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
 - iii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
 - iv) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.
- 44) **Personal Representative** – Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco parentis has assented to an agreement of confidentiality between the CCBDD and the minor.
- 45) **Physical safeguards** – are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- 46) **Protected Health Information, or PHI** – means individually identifiable information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Records of Individuals deceased for more than 50 years are not PHI. For the purposes of this manual, and the Agency's compliance program, PHI shall also include “Education Records” as defined by FERPA. This creates a consistent set of policies for both types of confidential information.

- 47) **Provider** – Provider means a person or entity, which is licensed or certified to provide services, including but not limited to health care services, to persons with DD, in accordance with applicable requirements. A Covered Provider is a Health Care Provider who transmits any health information in electronic form.
- 48) **Public Health Authority** – Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
- 49) **Security or Security measures** – encompass all of the administrative, physical, and technical safeguards in an information system.
- 50) **Security incident** – means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- 51) **Social Engineering** – means “an outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information they need to gain access to the system” or “getting needed information (for example, a password) from a person rather than breaking into a system” . . . social engineering is generally a hacker’s clever manipulation of the natural human tendency to trust. The hacker’s goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
- 52) **Subcontractor** – means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- 53) **Technical safeguards** – means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
- 54) **Treatment** – means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
- 55) **TPO** – TPO means treatment, payment or health care operations under HIPAA rules. For the purposes of this policy manual, TPO shall also include “Education” as defined above.
- 56) **Unsecured protected health information** – protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology in guidance specified by the Secretary of the Department of HHS in guidance issued under section 13402(h)2 of Public Law 111-5.
- 57) **Use** – Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
- 58) **User** – means a person or entity with authorized access.
- 59) **Violation, or violate** – means, as the context may require, failure to comply with a provision of either the HIPAA Privacy or Security rules, or a provision of state law relating to privacy, confidentiality or computer security.
- 60) **Workforce Member** – Workforce Member means the same as Employee. See definition above.
- 61) **Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

2400.01.02 Confidentiality – General Rules

POLICY

All information in an enrollee's records, including electronic information, is confidential. Further, all conversations involving individually identifiable information is confidential.

The CCBDD shall conform to all requirements for privacy and confidentiality set forth by the State of Ohio, the federal HIPAA, FERPA and IDEA regulations, and any other applicable law. Safeguards will be implemented for the use, disclosure, collection, storage, retention and destruction of individually identifiable information. The CCBDD shall not use or disclose individually identifiable information except in accordance with applicable requirements.

AUDIENCE

All Staff

AUTHORITY

[45 CFR Part 160](#) and [45 CFR § 164](#) (current as of 3/27/2013)

[45 CFR § 164.504\(g\)](#) for entities with multiple functions

[ORC § 5126.044](#) Ohio law on confidentiality (effective 9/22/2000)

[OAC § 5123:2-1-02\(M\)](#) General DD Board confidentiality requirements (1/1/2015)

[45 CFR § 164.502\(a\)\(1\)\(iii\)](#) incidental uses and disclosures

[OAC § 3301-51-04](#) Confidentiality (effective 7/1/2014), for schools

[34 CFR 99](#) FERPA (current as of 1/2012)

[34 CFR 300](#) and 301 Part B IDEA (Individuals with Disabilities Education Act, ages 3-21)

[34 CFR 303 Part C](#) IDEA (Individuals with Disabilities Education Act, ages 0-2)

[34 CFR 303.402](#) - 416 Early Intervention Confidentiality and Family Rights Provisions

[34 CFR 300.610](#) - [627](#) Children with Disabilities Confidentiality and Parent Rights Provisions

PROCEDURES

- 1) Staff of the CCBDD may use or [disclose PHI](#) only as follows:
 - A) For education, treatment, payment and health care operations, including to contracted Business Associates. This information is to be used by employees for Agency purposes for serving Individuals. In an exception, explicit parent authorization is required for any Medicaid billing for children.
 - B) In accordance with a release or authorization of the Individual in accordance with policy and procedure set forth in [Policy 2400.01.06 Authorizations](#).
 - C) As permitted in [Policy 2400.01.05 Speaking with the Family or Friends of an Individual Receiving Services](#).
 - D) As permitted by in [Policy 2400.01.10 Disclosures that do Not Require an Authorization](#).
- 2) For all of the above, the minimum amount of information should be disclosed, and specific procedures followed as detailed in [2400.01.03 Minimum Necessary Policy](#).
- 3) All employees are responsible for safeguarding the information regarding Individuals served by CCBDD, as detailed in
 - A) [Policy 2400.01.04 Confidentiality Safeguards \(Oral & Written\)](#)
 - B) [Policy 2500.04.01 Computer Usage](#)
 - C) [Policy 2500.04.02 Social Media Use](#)
 - D) [Policy 2500.04.03 Portable Computing Devices](#)
 - E) [Policy 2500.04.04 Employee Work at Home](#)
- 4) Rights of Individuals served by CCBDD may be exercised by parents, guardians and personal representatives as detailed in [Policy 2400.01.08 Minors, Personal Representatives and Deceased Individuals](#).
- 5) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in [Policy 2400.01.09 Duty to Report Violations and Security Incidents](#).
- 6) Supervisors, managers and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.

2400.01.03 Minimum Necessary Policy

POLICY

The use and disclosure of PHI must be limited to the minimum necessary to satisfy the request or to complete the task, except in situations specifically identified by the HIPAA rules. The Privacy Officer shall implement safeguards and protocols to implement this policy. All employees shall follow those protocols.

AUDIENCE

All Staff

AUTHORITY

[45 CFR § 164.502\(b\)\(1\)](#) minimum necessary standard
 34 CFR 300.623(d) IDEA Part B
 34 CFR 303.415(d) IDEA Part C
 34 CFR 99.31(a)(1)(i)(A) FERPA
 OAC 3301-51-04(N)(4) OAC Confidentiality Safeguards

PROCEDURES

FOR THE PRIVACY OFFICER

- 1) **Implementation Approach.** The Privacy Officer will implement the minimum necessary requirement with the steps detailed below. Measures to limit workforce access, and procedures for both routine disclosures and requests for PHI will be created and documented as detailed below:
 - A) **Limiting Workforce Access to PHI:** Access to the PHI will be granted based on the employee's role and determined by the Director and Privacy Officer of CCBDD. CCBDD will identify:
 - i) Those persons or classes of persons, who require access to PHI to carry out their duties, in the workforce, including interns and trainees, will be listed according to job classification with the minimal necessary PHI required for successful job performance to serve the Individuals, and
 - ii) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
 - iii) Safeguards will be developed and documented to restrict workforce access to the minimum necessary, especially as detailed in [Policy 2500.01.04 Facility Security and Access Control](#).
 - iv) The Privacy Officer will document the results of this analysis in [Appendix D – Minimum Necessary – Workforce, Disclosures and Requests](#). This report will be available for public inspection.
 - B) **Procedures for Routine Disclosures and Requests.** The HIPAA Privacy Officer will identify all routine disclosures made by Agency employees, for which the minimum necessary requirement applies, and create procedures to implement these. The same shall be done for routine requests for PHI. [Note that minimum necessary does not apply for disclosures or requests related to “treatment”; consequently no procedures must be created in these situations.] These results shall be documented in [Appendix D – Minimum Necessary – Workforce, Disclosures and Requests](#).
 - C) **Implementation.** The Privacy Officer shall take the steps to implement the results of the analysis above, including configuring access control on software, staff training for routine requests and disclosures, and any other measures necessary.

FOR ALL EMPLOYEES

- 1) **Minimum Necessary Requirement.**
 - A) **Basic Requirement.** When using or disclosing PHI, or when requesting PHI from another entity, employees must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
 - B) **Exceptions.** The minimum necessary requirement does NOT apply to:
 - i) Disclosures to or requests by a health care provider for treatment
 - ii) Uses or disclosures made to the Individual served, including but not limited to any requests for their records or requests for an accounting of disclosure
 - iii) Uses of disclosures made pursuant to an Authorization
 - iv) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations

- 2) **Routine Requests or Disclosures.** Staff shall be familiar with and follow procedures detailed in [Appendix D – Minimum Necessary – Workforce, Disclosures and Requests](#) when making requests for PHI or disclosures.
- 3) **Procedures for Non-Routine Disclosures or Requests**
 - A) **For non-routine disclosures,** when subject to the minimum necessary provision, the person making the disclosure will apply the minimum necessary principle. He or she may seek the guidance, if necessary, of the Privacy Officer (or his/her designee).
 - B) **For non-routine requests,** the requesting party will utilize the minimum necessary principle, seeking the guidance, if necessary, of the Privacy Officer (or his/her designee).
 - C) **Good Faith Reliance** – CCBDD staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:
 - i) The disclosure is made to a **public official**, permitted to receive information, and the public official represents that the request is for the minimum necessary information;
 - ii) The request is from another **covered entity**;
 - iii) The request is from a **professional** at CCBDD, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary

2400.01.04 Confidentiality Safeguards (Oral & Written)

POLICY

CCBDD shall utilize appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

AUTHORITY

[45 CFR § 164.530\(c\)](#) – Administrative, Technical, and Physical Safeguards

[34 CFR 99.31\(a\)\(1\)\(ii\)](#) Safeguards

[ORC § 5126.044](#) Ohio law on confidentiality

[OAC § 5123:2-1-02\(M\)](#) DD Board Records

PROCEDURES

1) General Procedures

- A) Employees shall be familiar with [Appendix D Facility Security and Access Plan](#) in the [Policy 2500 Computer Security](#) regarding staff, Individuals receiving services, parent and other visitor access to the facility.
- B) Visitors shall be required to sign-in and wear a visitor badge while on the premises. Employees shall escort visitors throughout the premises.

2) Oral Privacy

- A) Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings, and using appropriate volume when speaking to prevent others from overhearing conversations.
- B) Employees shall refrain from holding conversations in common areas where Individuals receiving services or visitors can overhear PHI.
- C) Discussions concerning Individuals should be done in a private area and discussions must be limited to “need to know” information for purposes of providing the best services.
- D) Overheard conversations are not to be shared or repeated.
- E) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.

3) Safeguards for Written PHI

A) Control of the Original Paper Records

- i) The HIPAA Privacy Officer shall be responsible for administering the security controls for paper record storage.
- ii) Case and School records shall be kept locked and secured. Employees requiring access to these records shall have a key and/or combination for the storage room or cabinet.
- iii) Paper files shall be put away promptly when not being used.
- iv) Original paper records shall not be removed from the building without the authorization of the superintendent, Privacy Officer or designee.
- v) Individual records shall be retained per [Policy 803 Records Retention and Destruction](#).

B) Other use and storage of paper records

- i) Employees should minimize the use of hardcopy PHI.
- ii) Personal appointment books with names of Individuals being served should be safeguarded while away from the office. It is best to avoid putting last names in appointment books if possible.
- iii) Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer.

C) Faxing Procedure

- i) When faxing a document with PHI, use a cover sheet which indicates that information is confidential, protected under state and federal laws, and not to be re-disclosed.
- ii) Care should be taken to address and transmit fax to the proper recipient.
- iii) Faxed documents should not be left at a common fax machine.

D) Printing and Copying PHI

- i) Printers and copiers used for printing of PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
- ii) PHI printed to a shared printer should be promptly removed.

- iii) The Security Officer shall monitor all printer and photocopier acquisitions. In the event that this equipment includes internal storage devices, which retain images of photocopies made, the asset shall be managed by the IT department, especially upon disposal to ensure destruction of any PHI contained in its storage.
- E) **Transportation/outside use of documents with PHI**
 - i) Caseworkers and other employees who remove documents from the facility, to conduct fieldwork, for example, are responsible for safeguarding these documents.
 - ii) When leaving documents unattended in a personal vehicle, the vehicle should be locked. Preferably, the documents and/or their container should not be visible.
 - iii) If any documents with PHI are lost or stolen, the incident should be immediately reported to a supervisor.
- F) **Visibility of records and other PHI.** All employees using records for Individuals and other paperwork with PHI shall arrange these items so that PHI is not readily visible to other Individuals receiving services/visitors, especially in high traffic areas such as reception area.
- G) **Shredding.** Unneeded paper documents containing PHI shall be destroyed by shredding.
- H) **Clean Desk Policy.** All employees shall clean their desks of PHI whenever leaving their work area for a time, especially at end-of-day.
- 4) **Compliance Audits/Facility Review.** At least annually, the HIPAA Privacy Officer or designee may audit staff compliance with these guidelines. The audit shall consist of a walk-through of the facility, with observations recorded, such as placement of desks, location of computer equipment, any papers with PHI that would be visible to a visitor, etc. The results shall be discussed with the appropriate employee, and any appropriate actions taken.
- 5) **Enforcement.** All supervisors are responsible for enforcing this policy. Employees who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.
- 6) **Annual Review.** These safeguards shall be reviewed and updated annually.

2400.01.05 Speaking with the Family and Friends of an Individual Receiving Services

POLICY

CCBDD personnel are permitted to verbally disclose protected health information to family, friends, caregivers and other persons involved with the care of an Individual being served, in specific situations, after giving the Individual receiving services the opportunity to either agree to or object to the disclosure.

AUDIENCE

All Staff

AUTHORITY

[45 CFR § 164.510\(b\)](#)

PROCEDURES

- 1) **If the Individual is present**
 - A) **Permitted disclosure to family or friend present.** If a family member, or friend of the Individual is present while services are being rendered, an employee serving the Individual may disclose PHI after one of the following:
 - i) verbally seeking permission for the disclosure, and the Individual agrees; or
 - ii) giving the Individual the opportunity to object to the disclosure, and the Individual does not express an objection; or
 - iii) the staff member reasonably infers from the circumstances, based on the exercise of professional judgment, that the Individual does not object to the disclosure.
- 2) **If the Individual is not present**
 - A) **Communications about the Individual's care**
 - i) In the event of a phone call or other discussion with a family member or one involved with the care of the Individual being served by CCBDD, where the Individual is not present, the employee may use their professional judgment to determine if the disclosure is in the best interests of the Individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Individual's care.
 - B) **Notifications**
 - i) An employee may disclose PHI to notify a family member, a personal representative of the Individual, or another person responsible for the care of the Individual of the Individual's location or general condition.

2400.01.06 Authorizations

POLICY

All disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization. CCBDD will use an authorization form that conforms with Ohio Laws, and the federal FERPA, IDEA and HIPAA regulations.

AUDIENCE

All Staff

AUTHORITY

[45 CFR § 164.508](#) – HIPAA requirements for authorizations

[ORC § 5126.044](#) – Ohio Statute on confidentiality of records

[OAC § 5123:2-1-02\(M\)](#) – Ohio Rule on confidentiality of records

[34 CFR 99.30](#) – FERPA requirements for prior consents to disclose information

[34 CFR 99.32](#) – FERPA recordkeeping requirements concerning requests and disclosures

LEGAL NOTES

- FERPA applies for records created for education; HIPAA applies to all other records. The term used in the FERPA regulations is “consent”. The HIPAA term “authorization” is used in these policies.

PROCEDURES

- 1) **Valid Authorization.** Unless otherwise authorized by CCBDD policy and/or state or federal law, release of an Individual's records requires specific authorization by the Individual being served or his/her legal representative. A [standard authorization form](#) is included as an Appendix. If authorizations are received on other forms, note that a valid authorization must include the following:
 - A) Full Name of the Individual.
 - B) A specific description of the information to be released. For example, a range of dates, or category of record.
 - C) The purpose or need for the disclosure.
 - D) The name of the person or agency disclosing the information.
 - E) Names of the person(s), or agency to whom the disclosure is to be made.
 - F) The date, event, or condition upon which the authorization expires (which can be no longer than 180 days from the date of signing).
 - G) Statement of the Individual’s right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke.
 - H) Statement that CCBDD may not condition treatment on whether the Individual signs the authorization.
 - I) A statement informing the Individual of the potential that information disclosed could be redisclosed if the recipient is not subject to federal or state confidentiality restrictions.
 - J) Signature and date of the Individual or personal representative.
 - K) If the authorization is signed by a guardian or personal representative, a description of that person's relationship to the Individual and authority to sign the authorization.
 - L) Written in plain language.
- 2) **Invalid Authorization.** A PHI authorization is considered invalid if authorization has the following defects:
 - A) Authorization is incomplete.
 - B) Authorization is not dated or time has elapsed.
 - C) Authorization does not contain required elements as explained above.
 - D) CCBDD is aware authorization has been revoked.
 - E) CCBDD is aware information is false.
 - F) Authorizations to release PHI is combined with other documents.
- 3) **For authorizations presented in person for immediate release,** the staff member shall verify the identity of the recipient according to [Policy 2400.01.07 Verification](#), after which the information may be released.
- 4) **Proper Completion of Authorization Form by Staff.** The staff person handling the request should complete the following steps, and annotate the bottom of the [Authorization Form](#):
 - A) The employee should write their name on the completed authorization form.

- B) The original signed authorization shall be saved in the Individual's master record, and a copy must be given to the Individual.
- C) A record of the release shall be maintained in the Individual's record, using the [Disclosure Log](#) included as an Appendix, detailing the following information:
 - i) The date of the disclosure.
 - ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
 - iii) A brief description of the PHI disclosed.
 - iv) A brief statement of the purpose of the disclosure.
 - v) If the disclosure was due to a health or safety emergency, a description of the significant threat to health or safety.
- 5) **Retention Period for Written or Electronic Copy of Authorization.** The CCBDD must retain the written or electronic copy of the authorization for a period of six (6) years from the later of the date of execution or the last effective date.
- 6) **Revocation of Authorization.** Upon instructions of revocation of authorization, CCBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.
- 7) Note that information from other service providers contained in the Individual's record may be released with the Individual's written authorization.

2400.01.07 Verification

POLICY

CCBDD will take reasonable steps to verify the identity and the authority of the person requesting protected health information (PHI) of an Individual.

AUDIENCE

All Staff

AUTHORITY

[34 CFR 99.31](#)(c) Verification

[45 CFR § 164.514](#)(h) Verification

PROCEDURES

REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY

- 1) **Verifying Identity and Authority.** In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI, CCBDD personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing PHI:
 - A) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI.
 - B) Presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person.
 - C) A written statement on appropriate government letterhead that the person is acting under the government's authority.
 - D) Other evidence of documentation from an agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
 - E) A written statement of the legal authority under which the information is requested.
 - F) If a written statement would be impracticable, an oral statement of such legal authority.
 - G) A request that is made pursuant to a court order and subpoena or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority.
- 2) The following issues should be addressed before releasing PHI once a request is received:
 - A) Is the requestor who she/he claims to be?
 - B) Does the requestor have the authority to request PHI. If the request involves a court order, subpoena, or other legal request, follow the procedures outlined in the [Policy 2400.01.10 Disclosures that do Not Require an Authorization](#).

REQUESTS FROM AN INDIVIDUAL RECEIVING SERVICES, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE

- 1) A properly completed, valid Authorization per the specifications in [Policy 2400.01.06 Authorizations](#) is sufficient verification of the identity and authority of the person requesting information.
- 2) For requests for information other than formal record releases, staff must first verify both the identity and the authority of the person prior to releasing PHI:
 - A) If the person is known to the staff person, this is sufficient verification of identity.
 - B) Identity can be verified by questioning the person regarding their knowledge of information in the record of the Individual being served, such as birth date, social security number, etc., which only an authorized person would typically know.
 - C) For requests from someone other than the Individual or the parent of a minor, the person's authority to obtain information must also be verified. For example, a healthcare Power of Attorney and/or statement from the Individual that the requestor is a HIPAA Personal Representative would demonstrate proper authority. See also [Policy 2400.01.05 Speaking with Family and Friends of an Individual Receiving Services](#) for situations where it may be permissible to give information to a family member.

2400.01.08 Minors, Personal Representatives and Deceased Individuals

POLICY

Staff must follow applicable legal requirements to maintain confidentiality and to permit the legal release of protected health information (PHI) to minors and personal representatives, and for the release of PHI of deceased Individuals.

AUTHORITY

[ORC 5126.044](#) Confidentiality

[ORC 3319.321\(4\)](#) Confidentiality and Parental Rights of Access to Student Records

[ORC 3109.051\(H\)](#) Parenting Time – companionship rights

[ORC 1337.13](#) Authority of attorney under durable power of attorney for health care

[45 CFR § 164.502\(g\)\(1\)](#) Personal representatives

[45 CFR § 164.502\(g\)\(2\)](#) Adults and emancipated minors

[45 CFR § 164.502\(g\)\(3\)](#) Unemancipated minors

[45 CFR § 164.502\(f\)](#) Deceased Individuals

[45 CFR § 164.510\(b\)\(5\)](#) Uses and disclosures when the individual is deceased

NOTES

Federal HIPAA law changes issued 1/25/2013 relax confidentiality requirements upon death of an Individual. These include 45 CFR § 164.502(f) which eliminates all protections of information 50 years after the death of an Individual, and 45 CFR § 164.510(b)(5) which allow for disclosures to people involved with the care of the Individual prior to death for information that is relevant to the person's involvement. While HIPAA rules preempt contrary state law, state laws which offer greater privacy safeguards, more rights of access to information, or less coercion shall prevail. No changes have been made to these policies to implement the relaxed HIPAA provisions; consult with your prosecutor regarding whether to change these policies.

PROCEDURES

- 1) **Rights of legally Consenting Minors.** Individuals being served, who are minors, and who are legally allowed to consent to treatment under Ohio Law may exercise all rights regarding access to, requests for amendment to, and release of their PHI pursuant to a written authorization.
- 2) **Rights of an Individual's Personal Representative.** CCBDD recognizes an Individual's personal representative as a person authorized to exercise rights of access and/or inspection of PHI, rights to request amendment of PHI, and the right to sign the CCBDD [Authorization Form](#) which permits release of PHI.
- 3) **Recognized Personal Representative.** CCBDD recognizes the following persons to be personal representatives:
 - A) The parent of a child younger than 18 years old
 - B) The non-custodial parent of a child younger than 18 years old ([ORC 3319.321](#) and [ORC 3109.051\(H\)](#)), unless the custodial parent presents CCBDD a court order restricting the non-custodial parent's access. In the event that CCBDD is presented with such a court order, CCBDD shall adhere to the terms of that order.
 - C) A person who is recognized through durable power of attorney to have authority to act on the behalf of the Individual ([ORC § 1337.13](#))
 - D) The legal guardian of the Individual
 - E) Any other person authorized by law except in Abuse, Neglect, and/or Endangerment situations, or where CCBDD has received a court order or other documentation limiting privileges of a non-custodial parent as provided below.
 - i) Abuse, Neglect, and/or Endangerment Situations. Notwithstanding a state law of any requirement of this paragraph to the contrary, CCBDD may elect not to recognize a person as a personal representative of an Individual. In order for CCBDD to choose not to recognize a person as a personal representative, CCBDD must decide that it is not in the best interest of the Individual to treat the person as the Individual's personal representative and must believe that one of the following conditions exist:
 - 1) The Individual has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative.
 - 2) Treating such person as the personal representative could endanger the Individual.

- ii) Receipt of a court order limiting privileges of a non-custodial parent. In the event that CCBDD receives from the custodial parent a court order limiting the privileges of the non-custodial parent to act in the capacity of the child's personal representative, CCBDD shall adhere to the restrictions in the court order.

4) Deceased Individuals

- A) **Disclosure of PHI After Death.** PHI generated during the life of an Individual is protected from disclosure after death unless disclosure is for treatment or payment, quality assurance or other auditing or program review functions. CCBDD and its employees cannot release PHI regarding a deceased Individual unless a valid personal representative has been established and has requested the PHI through the proper authorization process.
- B) **Disclosure of PHI to Administer Estate.** Upon request, PHI shall be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate ([ORC § 5126.044](#)).
- C) **Disclosure to Guardian or next-of-kin:** Upon request, the Agency shall release records regarding an Individual served to the guardian at time of death. Absent a guardian, records may be released to the next of kin:
 - i) The Individual's Spouse (if married)
 - ii) The Individual's children
 - iii) The Individual's parents
 - iv) The Individual's brothers or sisters
 - v) The Individual's uncles or aunts;
 - vi) The Individual's closest relative by blood or adoption
 - vii) The Individual's closest relative by marriage

An entire category must be exhausted (i.e., no people in the category exist or are still alive) before moving to the next category ([ORC § 5126.044](#)).

2400.01.09 Duty to Report Violations and Security Incidents

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

Confidentiality of PHI, and the computer security required to protect information regarding Individuals receiving services is taken very seriously at CCBDD. Employees are required to follow all rules in these policies. Any employee who becomes aware of a violation of either confidentiality or computer security rules is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

AUTHORITY

HIPAA Privacy Rules, [45 CFR § 164](#)

[45 CFR § 164.530\(e\)\(1\)](#) – Sanctions

PROCEDURES

- 1) **Employees Duty to Report Violation.** Any employee observing a violation of any of the Confidentiality and Computer Security policies is to report the violation to his/her supervisor. Failure to report a violation is in itself a disciplinable offense.
- 2) **Investigation.** The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, Individuals receiving services, or others, and/or review of computer or paper audit trails.
- 3) **Procedure for Data Breach.** For potential data [breaches](#), the Privacy and/or Security Officer will follow any procedures detailed in [Policy 2500.01.08 Breach Reporting](#).
- 4) **Procedure for Privacy Violation.** For Privacy Violations, the Privacy Officer will follow procedures in [Policy 2500.01.12 Mitigation](#).
- 5) **Filing of Written Report by Privacy and/or Security Officer.** A written incident report will be written by the Privacy and/or Security Officer. It will be filed in:
 - A) the Privacy Officer's Privacy Violations file; and
 - B) the employee's personnel file.
- 6) **Employee Discipline**, if appropriate, will be taken and documented in accordance with [Policy 308 Discipline](#).
- 7) **Post-Incident Review.** A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in policy, additional training, or other appropriate action.

2400.01.10 Disclosures that do Not Require an Authorization

POLICY

CCBDD employees may use and disclose PHI in specific situations authorized by state and federal statute. In these cases, the Individual's authorization is not required. Staff will carefully follow specific requirements for these unusual and infrequent disclosures. These disclosures include the following:

- When required by law.
- For public health purposes such as reporting communicable diseases, work-related illnesses, or other diseases and injuries permitted by law; reporting births and deaths, and reporting reactions to drugs and problems with medical devices.
- To protect victims of abuse, neglect, or domestic violence.
- For health oversight activities such as investigations, audits, and inspections.
- To accrediting organizations.
- For judicial and administrative proceedings.
- For law enforcement purposes.
- To coroners, medical examiners, and funeral directors.
- For organ, eye or tissue donation.
- To reduce or prevent a serious threat to public health and safety.
- For Specialized government functions.
- In connection with "whistleblowing".
- For workers' compensation or other similar programs if applicable.

AUTHORITY

[45 CFR § 45 CFR § 164.512](#)

[34 CFR 99.31](#)

[34 CFR 99.36](#)

[ORC § 2151.421](#)(A) Reports of Child Abuse

[ORC § 2305.51](#) Disclosures to prevent harm to 3rd parties

[ORC § 2317.02](#)(B) Privilege for physicians, school guidance counselors, licensed social workers and licensed counselors

[ORC § 4732.19](#) Privilege for psychologists

[ORC § 5123.19](#) Licensure activities of DODD

[ORC § 5123.60](#) OLRs

[ORC § 5123.61](#)(C)(1) Duty to report abuse/neglect of persons with DD

[ORC § 5126.044](#) Confidentiality for DD Boards

[ORC § 5126.055](#) LMAA functions of DD Boards

[ORC § 5126.31](#) Case Review and Investigation

[OAC § 5123:2-17-02](#)(B) Incidents adversely affecting health/safety

[OAC § 5123:2-17-02](#)(D) Reporting MUIs

[OAC § 5123:2-3-04](#) Monitoring of licensed facilities

Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena

[ORC § 4113.52](#) Reporting Violations of law by employer or fellow employee

[34 CFR Part 99 Subpart D](#) May an Educational Agency Disclose Education Records

20 U.S.C. 7165(b) Section 4155(b) No Child Left Behind Act – Transfer of Disciplinary Records

OAC 3301-51-04(Q) Disciplinary Information

LEGAL NOTES

- [ORC § 5126.044](#) does not authorize any of the excepted disclosures detailed in HIPAA and FERPA. Other Ohio regulations reference disclosures otherwise allowed by federal and state law. HIPAA preempts contrary state law, except where state law offers greater privacy protections, greater rights of access to an Individual's records, or is less coercive. Consult your county prosecutor for review and approval of this policy.
- HIPAA and FERPA/IDEA maintain overlapping but different lists of disclosures permitted without authorization or parental consent. We use the term "Education Records" below to refer to FERPA/IDEA permitted disclosures, and "PHI" regarding HIPAA permitted disclosures.

PROCEDURES

CCBDD employees will follow the indicated procedures for the various special circumstances detailed below:

- 1) **Recordkeeping.** For all of the disclosures authorized below, the employee handling the disclosure will document the details of the disclosure on the [Disclosure Log](#) which will be maintained in the adult or school record. Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.
- 2) **When required by law**
 - A) To officials at another school that an Individual served by the Agency intends to enroll in, or is already enrolled in, for the purposes of Individual's enrollment or transfer. Any such disclosures must include records of any disciplinary actions.
 - B) The CCBDD may use or disclose PHI or Education Records to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
 - C) For compliance with mandatory disclosures related to sex offenders
- 3) **For public health purposes** PHI may be used or disclosed to:
 - A) A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions.
 - B) A public health or other government authority authorized by law to receive reports of child abuse or neglect.
 - C) A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance.
 - D) A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.
 - E) To the extent that the CCBDD receives PHI disclosed under this section in its role as LMAA, the CCBDD may use the PHI to carry out its duties.
- 4) **To protect victims of abuse, neglect, domestic violence or other crime**
 - A) **Reports of child abuse**
 - i) Reports of child abuse shall be made in accordance with Ohio law.
 - ii) The CCBDD may disclose PHI related to the report of abuse to the extent required by applicable law. Such reports shall be made to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
 - B) **Reports of abuse and neglect other than reports of child abuse or neglect.**
 - i) The CCBDD may disclose PHI about an Individual believed to be a victim of abuse, neglect, or domestic violence to a governmental authority authorized to receive such reports if:
 - 1) the Individual agrees; or
 - 2) the CCBDD believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm.

If the Individual lacks the capacity to agree, disclosure may be made if not intended for use against the Individual and delaying disclosure would materially hinder law enforcement activity.
 - ii) The CCBDD staff member making the disclosure must promptly inform the Individual whose PHI has been released unless:
 - 1) doing so would place the Individual at risk of serious harm; or
 - 2) the CCBDD would be informing a personal representative, and the CCBDD reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the Individual as determined by the CCBDD, in the exercise of professional judgment.
- 5) **For health or education oversight activities such as investigations, audits, and inspections**
 - A) PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.
 - B) Specifically excluded from this category are investigations of an Individual that are not related to receipt of

- health care, or the qualification for, receipt of, or claim for public benefits.
- C) To the extent that the CCBDD receives PHI disclosed under this section in its role as LMAA, the CCBDD may use the PHI to carry out its duties.
- D) Education Records may be disclosed to the Comptroller General of the US, Attorney General of the US, Secretary of Education and/or State of Ohio Education authorities subject to the requirements of 34 CFR 99.35 or to state officials involved with juvenile justice in accordance with 34 CF 99.38.
- 6) **To accrediting organizations**
- A) Information in Education Records may be disclosed to accrediting organizations without parental consent. For any disclosure of PHI, a HIPAA Business Associate agreement should be in place with the accrediting organization.
- 7) **For judicial and administrative proceedings**
- NOTE:** These policies do not detail all situations such as grand juries and other infrequent legal proceedings. Consult with legal counsel prior to disclosure for any unusual situations! Also note that HIPAA and FERPA requirements are similar but different in some situations.
- A) The CCBDD must always comply with a **court order**, but only in accordance with the express terms of the order.
- B) For a **subpoena, discovery request or other lawful process**: the CCBDD may comply with such legal requests only if:
- i) The CCBDD makes reasonable effort to notify the parent involved and/or receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the Individual who is the subject of the requested PHI has been given notice of the request; or
 - ii) The CCBDD receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.
- The CCBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements of HIPAA or FERPA.
- 8) **For law enforcement purposes**
- A) **Conditions Allowing for Disclosure of PHI to Law Enforcement.** PHI may be disclosed for the following law enforcement purposes and under the specified conditions:
- i) Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; or commission of a felony, subject to any exceptions set forth in applicable law.
 - ii) Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.
 - iii) The CCBDD may disclose to a law enforcement official protected health information that the CCBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the CCBDD.
- B) **Reporting Commission and Nature of Crime.** PHI may be disclosed to law enforcement personnel to report the commission and nature of a crime; The location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime. When responding to requests about the location of a suspect, fugitive, material witness, or missing person, the following PHI may be released:
- i) Name and address
 - ii) Date and place of birth
 - iii) Social security number
 - iv) ABO blood type and RH factor
 - v) Type of injury
 - vi) Date and time of treatment
 - vii) Date and time of death, if applicable,
 - viii) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos
- C) **Compliance/Enforcement of privacy regulations:** PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.
- 9) **To coroners, medical examiners, and funeral directors**
- A) PHI may be disclosed to coroners, medical examiners and funeral directors, as necessary for carrying out their duties.

- 10) **Organ, eye or tissue donation**
- A) PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.
- 11) **To reduce or prevent a serious threat to public health and safety and/or safety of person(s)**
- A) The CCBDD may disclose PHI or Education Records as follows, to the extent permitted by applicable law and ethical standards:
- i) **Good Faith.** PHI may be used or disclosed if the entity believes in good faith:
 - 1) that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat; or
 - 2) the disclosure is to law enforcement authorities to identify or apprehend an Individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.
 - B) **Disclosure of Individual's Admitted Participation in a Violent Crime.** Disclosures of admitted participation in a violent crime are limited to the Individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.
 - C) **Disclosure of Individual's Admitted Participation in a Violent Crime Learned in the Course of Treatment.** Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the Individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.
- 12) **Specialized government functions**
- A) **National Security and Intelligence:** PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, Counterintelligence, and other activities authorized by the National Security Act.
- B) **Protective Services:** PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
- C) **Correctional Institution or Law Enforcement Official.** The CCBDD may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other Individual protected health information about such inmate or Individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:
- i) The provision of health care to such Individuals;
 - ii) The health and safety of such Individual or other inmates;
 - iii) The health and safety of the officers or employees of or others at the correctional institution;
 - iv) The health and safety of such persons and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
 - v) Law enforcement on the premises of the correctional institution; and
 - vi) The administration and maintenance of the safety, security, and good order of the correctional institution.
- The provisions of this section do not apply after the Individual is released from custody.
- D) **Public Benefits:** PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.
- 13) **In connection with "whistleblowing".** In connection with "whistleblowing", or reporting of a violation of law or ethics, an employee of CCBDD may disclose PHI to his/her attorney, and to other parties specified in Ohio Revised Code § 4113.52, while following the procedures outlined in that statute. See also [Policy 324 Protection of Whistleblowers](#).
- 14) **For workers' compensation or other similar programs if applicable.**
- A) PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

2400.02 INDIVIDUAL RIGHTS

2400.02.01 Individual's Right to Access Records

Adopted: 7/1/2013

Revised Date:

Effective:

POLICY

Individuals served by CCBDD, and their personal representatives, have the right to access and/or inspect the PHI and/or Education Records contained in the designated record set, subject to any limitations imposed by law.

AUDIENCE

Privacy Officer, Supervisors

AUTHORITY

[45 CFR § 164.524\(e\)](#) individual's right to access PHI

[45 CFR § 164.524\(b\)](#) Time limits on response to access

[45 CFR § 164.524\(c\)](#) Form of access

[34 CFR 99.4](#) Rights of Parents

[34 CFR 300.613\(c\)](#) IDEA Rights of parents

[ORC § 1347.08\(A\)\(2\)](#) individual's right to access records

[OAC § 3301-51-04](#) Confidentiality, for Education of Students with Special Needs

[OAC § 5123:2-1-02\(M\)](#) County Board Administration – Records

LEGAL NOTES

- State laws, HIPAA, and FERPA all provide that Individuals receiving services have access to their records.
- State law, OAC 5123:2-1-02 was amended 1/1/2015 to harmonize with HIPAA and FERPA

PROCEDURES

1) Who May Access Records

- A) An Individual served by the Agency above the age of 18, the parent/guardian of a child, the guardian of an adult not able to act on their own behalf, or any "personal representative" of an Individual served may access the records. See [Policy 2400.01.08 Minors, Personal Representatives and Deceased Individuals](#).
- B) **3rd Party Review.** An Individual or parent may include any 3rd party of their choosing, including an attorney, to review the records.
- C) **Presumption of Parental Right to Access Records.** CCBDD may presume that either parent of a minor may have access unless presented with documentation that the parent does not have authority under applicable state law governing such matters as guardianship, separation, or divorce.

2) Procedure, form and method of access

- A) **Requests for Access.** Requests for access to records shall be directed to the Privacy Officer or his/her designee.
- B) **Verification Procedure.** The Privacy Officer shall follow the Verification Procedure to verify the identity of the requestor. For any grant of access to someone other than the parent, the authority of the requestor to access the information shall also be verified. This might include documentation of guardianship or documentation that the person was appointed a "Personal Representative" under HIPAA.
- C) **Forms of Access Requested by the Individual.** The CCBDD shall provide the Individual with access to their records in any of the following ways requested by the Individual:
 - i) **By inspection.** CCBDD shall provide a private room for the Individual to review the records under the supervision of a CCBDD staff member who will ensure that the record is not altered.
 - ii) **Photocopy.** CCBDD shall provide a photocopy of the entire record or portion of the record requested.
 - iii) **Electronic format.** CCBDD shall provide an electronic copy of the information requested if this is feasible; if not, the Security Officer or his/her designee shall negotiate an electronic format and transmission method acceptable to both parties and fulfill the request.

- 1) If the Individual requests the information via email and only unsecured email is available, the Individual shall be notified that this method is subject to electronic eavesdropping. If the Individual is willing to accept the risks, the info shall be sent via email.
- 2) The Agency shall honor requests for commonly used media, such as USB Flash drives.
- D) **Record of Parties Accessing Records.** The Privacy Officer or his/her designee shall maintain a record of parties accessing records (except the access by the Individual or their parent) including the name of the party, the date access was given, and the purpose of access. These shall be maintained on the [Disclosure Log](#) illustrated in the Appendix.
- 3) **Other services/rights of Individuals, parents, and guardians**
 - A) **Explanation and Interpretation of Records.** CCBDD will respond to reasonable requests for explanation and interpretation of the records.
 - B) **List of Types and Locations of Records Maintained by CCBDD.** Upon request, CCBDD must provide Individuals, parents and guardians a list of the types and locations of records maintained or used by CCBDD.
 - C) **Known Records Not Maintained by CCBDD.** If the CCBDD does not maintain the PHI that is the subject of the Individual's request for access, and the CCBDD knows where the requested information is maintained, the CCBDD must inform the Individual where to direct the request for access.
- 4) **Transfer of rights at Age of Majority**
 - A) Rights of parents under these policies and under FERPA and IDEA transfer to the Individual served once that Individual reaches age 18 years. Once a child reaches age 17 years, the child must be informed of this transfer, and the IEP must include a statement that the child has been informed regarding the transfer of rights.
- 5) **Time for response to request for access**
 - A) Access shall be granted without unnecessary delay. In particular, requests should be honored prior to any scheduled IEP meeting, hearing, or administrative procedure. Requests in all cases shall be honored within 5 business days.
- 6) **Fees for copying/electronic media**
 - A) CCBDD at present has no fees for photocopies, postage or electronic media used to provide records.

2400.02.02 Individual's Right to Request Amendment of Records

Adopted: 7/1/2013

Revised Date:

Effective:

POLICY

Individuals receiving services have the right to request that CCBDD amend PHI in the designated record set, or Education Records, that they believe are erroneous. CCBDD will use procedures compliant with HIPAA, FERPA and/or IDEA in processing any requests for correction.

AUDIENCE

Privacy Officer, Supervisors

AUTHORITY

[45 CFR § 164.526\(f\)](#) Individual's right to request amendment

[OAC § 3301-51-04](#) Confidentiality, for Education of Students with Special Needs

[ORC § 1347.09](#) Disputing of Records

[34 CFR 99.20](#) FERPA – Requesting amendment of records

[34 CFR 99.21](#) FERPA – Rights to a Record Hearing

[34 CFR 99.22](#) FERPA – Requirements for a Records Hearing

LEGAL NOTES

These policies are designed to simultaneously comply with Federal HIPAA and FERPA regulations as well as Ohio regulations. All these regulations are similar; where they differ, policies are written to follow the regulations that provide the greatest degree of privilege and right of appeal to the Individual.

PROCEDURES

REQUESTS FOR AMENDMENTS

- 1) **Amending Statements Believed to be Inaccurate, Misleading or in Violation of Individual's Rights.** An Individual, parent, guardian, or other person acting as a HIPAA personal representative may request amendment of PHI about the Individual (and exercise rights for hearing and statements of disagreement), which they believe is inaccurate, misleading, or violates the rights of the Individual, and is held by the CCBDD or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
- 2) **Responsibility of Privacy Officer.** The Privacy Officer of the CCBDD is responsible for receiving requests for amendment, processing the requests, arranging for any hearings, and completing required documentation.
- 3) **Time to Act on a Request for Amendment.** The CCBDD will act on a request for amendment without unnecessary delay and no later than 60 days after the date of the request.
- 4) **Accepted Request for Amendments.** If the CCBDD accepts the requested amendment, in whole or in part, CCBDD must make the appropriate amendment, and inform the Individual and other persons or entities who have had access to the information.
- 5) **Denied Request for Amendments.** Otherwise, if the CCBDD believes the existing record is correct as is, it may deny the amendment:
 - A) **Written Notice.** If an amendment is denied, the CCBDD will give written notice in plain language which includes the following:
 - i) The basis for the denial;
 - ii) The Individual's right to submit a written statement disagreeing with the denial and how the Individual may file such a statement;
 - iii) A statement that, if the Individual does not submit a statement of disagreement, the Individual may request that the CCBDD provide the Individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
 - iv) The Individual's right for a hearing to challenge the information.
 - B) **Statement of Disagreement.** If the Individual submits a statement of disagreement, the Privacy Officer

will insert this statement into the appropriate portion of the record. Otherwise, the Privacy officer will insert into the record that the Individual requested an amendment and the CCBDD's denial.

- C) **Written Rebuttal.** The CCBDD may prepare a written rebuttal to the Individual's statement of disagreement. Whenever such a rebuttal is prepared, the CCBDD must provide a copy to the Individual who submitted the statement of disagreement.
- D) **Permanent Record.** The inserted statement of disagreement and any rebuttal become a part of the permanent record and must be included with all future disclosures of the covered records.
- 6) **Individual's Request for Copy of Changed Record.** At the Individual's request, CCBDD will send a copy of the changed record to any party requested by the Individual (per [ORC 1347.09](#)).
- 7) **Separate Transmission of Information in EDI Format.** If the disclosure which was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, the CCBDD may separately transmit the information to the recipient of the transaction in a standard EDI format.

RECORDS HEARINGS

CCBDD must offer a Records Hearing to any Individual who is denied a requested amendment of their records.

1) Hearing Procedures

- A) The HIPAA Privacy Officer will arrange the Records Hearing.
- B) The Privacy Officer must schedule the hearing within a reasonable time upon receiving a request.
- C) CCBDD shall give the Individual notice of date, time and place reasonably in advance of the hearing.
- D) To conduct the hearing, the Privacy Officer may appoint any person, including an official of CCBDD, who does not have a direct interest in its outcome.
- E) During the hearing, the parent shall have a full and fair opportunity to present evidence relevant to their objection. The Individual or parent may obtain assistance of any person(s), including an attorney hired at their own expense, to assist them.
- F) The decision shall be based solely on the evidence presented.
- G) The decision shall be documented in writing, within a reasonable time of the hearing, and shall include a summary of the evidence presented and the reasons for the decision.

2) Results of Hearing

- A) If, as a result of the hearing, CCBDD decides that the information in its records is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the Individual, it must amend the information accordingly and inform the Individual in writing.
- B) If, as a result of the hearing, CCBDD decides that the information is not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the Individual, it must inform the Individual of their right to place in the record a statement commenting on the information or setting forth any reasons for disagreeing with the decision of CCBDD.
- C) Any information placed in the record as a result of this hearing, CCBDD must maintain this statement as part of its permanent record, and include it with any subsequent disclosure.

2400.02.03 Individual's Right to Receive an Accounting of Disclosures

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD will provide, upon request, an "Accounting of Disclosures," in accordance with HIPAA Regulations, to Individuals who receive services from the Agency.

AUDIENCE

Privacy Officer, Supervisors

AUTHORITY

[45 CFR § 164.528](#)

[45 CFR § 164.528](#)(d) Individual's right to an accounting of disclosures of PHI

[34 CFR 99.32](#) FERPA Recordkeeping requirements concerning requests and disclosures

PROCEDURES

- 1) **Proper Records.** The Privacy Officer shall be responsible for insuring that proper records are kept to allow for proper and complete responses to any requests for accountings of disclosures. See also procedures listed in [Policy 2400.01.10 Disclosures that do Not Require an Authorization](#) and [Policy 2400.01.06 Authorizations](#) which detail the use of the [Disclosure Log](#).
- 2) **Individual's Right to Request Accounting of Disclosures of PHI.** Generally, an Individual has the right to request an accounting of disclosures of their PHI by CCBDD and its business associates during a time period of up to six years prior to the date of the Individual's request. Most disclosures are **not** required to be included in the accounting. The types of disclosures which are **not** required to be accounted for are:
 - A) For the purposes of treatment, payment and health care operations ([45 CFR § 164.502](#));
 - B) To the Individual receiving services, or to a parent, guardian or personal representative, of the Individual's own PHI ([45 CFR § 164.502](#));
 - C) Incidental disclosures, as detailed in ([45 CFR § 164.502](#));
 - D) Pursuant to an authorization ([45 CFR § 164.508](#));
 - E) To persons involved in the Individual's care or other notification purposes ([45 CFR § 164.510](#));
 - F) For national security and intelligence purposes, as detailed in ([45 CFR § 164.512](#))(k)(2);
 - G) Disclosures to prisons and other law enforcement agencies regarding an Individual who is in custody, as detailed in ([45 CFR § 164.512](#))(k)(5).
- 3) **Employee Documentation of Disclosures.** Any employee who makes a disclosure other than listed above shall document the disclosure in the Individual File, with all information described in step 6B below. More specifically, the following types of disclosures must be documented:
 - A) To public health authorities
 - B) Birth and death reporting
 - C) To law enforcement regarding crime on premises
 - D) To law enforcement in emergencies where crime is suspected
 - E) For cadaveric organ, eye, tissue donation purposes
 - F) For judicial and administrative proceedings
 - G) For research with an IRB waiver
 - H) To military command authorities
 - I) For Workers Comp purposes
 - J) To correctional institutions except as detailed in 2G above
 - K) About decedents to medical examiners, funeral directors, coroners
 - L) For public health activities
 - M) About victims of abuse
 - N) Regarding child abuse or neglect
 - O) To the FDA

- P) To a person who may have been exposed to a communicable disease
 - Q) To health oversight agencies for audits, civil or criminal investigations, inspections, licensure or disciplinary actions
 - R) In response to a court order
 - S) In response to a subpoena or discovery request
 - T) As required by law for wound or injury reporting
 - U) For identification & locating suspect or fugitive
 - V) Unlawful and unauthorized disclosures we have knowledge of
- 4) **Requests to Suspend Individual's Right to Disclosure.** Health oversight agencies and law enforcement officials may request a suspension of an Individual's rights to disclosure. If such a request is received, follow procedures in [45 CFR §164.528](#).
- 5) **Compliance with Request for Accounting Within 45 Days.** The HIPAA Privacy Officer shall comply with an Individual's request for an accounting within 45 days of the request. The CCBDD does not charge a fee for accountings.
- 6) **The written accounting must meet the following requirements:**
- A) All disclosures of the Individual's PHI during the 6 years prior to the request (or such shorter period as is specified in the request) as stated above.
 - B) As to each disclosure, the accounting must include:
 - ii) The date of the disclosure.
 - iii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
 - iv) A brief description of the PHI disclosed.
 - v) A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure.
 - vi) If during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period, and the date of the last such disclosure during the accounting period.
 - vii) If the accounting request includes school records, consult legal counsel regarding the need to obtain records of redisclosures by state or local school officials (see [34 CFR 99.32](#)).
 - C) CCBDD will retain documentation (in written or electronic format) for a period of 6 years:
 - i) All information required to be included in an accounting of disclosures of PHI.
 - ii) All written accountings provided to Individual.

2400.02.04 Individual's Right to Request Additional Restrictions

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD supports Individual's right to request restrictions on the use or disclosure of protected health information which are more stringent than the restrictions defined in organizational policy. CCBDD maintains procedures compliant with HIPAA regulations to process any requests it receives and to ensure that any requests it agrees to will be properly implemented.

AUDIENCE

Privacy Officer, Supervisors

AUTHORITY

[45 CFR § 45 CFR § 164.522\(a\)](#)

PROCEDURES

- 1) **Refer the Request to CCBDD' Privacy Officer or Designee:** All requests for additional restrictions on the use or disclosure of PHI will be referred to the HIPAA Privacy Officer, or his/her designee. Upon receiving a request, the Privacy Officer shall consider the following factors, in the decision to grant or deny the request:
 - A) Whether the restriction might cause the organization to violate applicable federal or state law;
 - B) Whether the restriction might cause the organization to violate professional standards, including medical ethical standards;
 - C) Whether CCBDD' systems and organization make it very difficult or impossible to accommodate the restriction;
 - D) Whether the restriction might unreasonably impede the organization's ability to serve the Individual;
 - E) Whether the restriction appears to be in the best interests of the Individual.
- 2) **Decision Whether CCBDD will agree:** The CCBDD is not obligated to agree to any requests for restriction, except in the unlikely event that the request is not to bill the Medicaid program or other 3rd party payer and that the Individual receiving services agrees to pay for the service themselves.
- 3) **Notify the Individual:** CCBDD will notify the Individual of its final decision (whether approving or denying the request) in writing. The notice will be maintained in the Individual's record.
 - A) **Granting the Request:** If CCBDD agrees to the restriction, the notice to the Individual will clearly state what restriction CCBDD is agreeing to in language the Individual will understand. This notice will state that the restriction will not apply if the information is needed for emergency treatment.
 - B) **Denying the Request:** If the request is denied, the notice will clearly state why the request cannot be complied with, in language the Individual will understand.
- 4) **Take Appropriate Action to Implement Restrictions:** If CCBDD agrees to the requested restriction, the Privacy Officer/designee will be responsible for taking appropriate action to implement the restriction.
- 5) **Modifying or Terminating a Restriction:** An Individual may request a restriction to be eliminated at any time. If CCBDD desires a modification, consult legal counsel regarding appropriate procedures.
- 6) **Documentation:** The Privacy Officer is responsible for maintaining the following documents, to assure that additional privacy protections are handled properly, and assure they are maintained for six years from the date of their creation:
 - A) Copies of Individual requests for restrictions.
 - B) Copies of any notice informing the Individual about CCBDD' decision to grant or deny a restriction.
 - C) Copies of any written Individual request to terminate a restriction, or alternatively, copies of any documentation in the Individual's record that the Individual made such request orally.

2400.02.05 Individual's Right to Request Confidential Communications

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

Individuals (or their parents) are entitled to request confidential communications, including for example, to not receive communications at their home address. These requests will be honored to the extent that they can be reasonably accommodated with CCBDD administrative systems.

AUTHORITY

[45 CFR § 164.502](#)(h) Confidential communications

[45 CFR § 164.522](#)(b) Confidential communications requirements

AUDIENCE

Privacy Officer

PROCEDURES

- 1) **Individual's Right to Request Confidential Communications.** Individuals, or their personal representative, may make a request for confidential communications in writing to the Privacy Officer.
- 2) **Receiving a Request.** When the Privacy Officer receives a request, the Privacy Officer may not ask the reason for the request. The Privacy Officer shall contact the Individual making the request to obtain an alternate means of contacting them (e.g. cell phone, PO Box, etc.). The Individual will be informed at that time of steps CCBDD will take to implement the request.
- 3) **Implementing the Request.** If existing systems are capable of administering the request, the Privacy Officer shall take necessary steps to implement the request, such as adjusted phone numbers or addresses in computer files or mailing lists.
- 4) **Documenting the Request.** The Privacy Officer shall document the request, and disposition, in the Individual's Record.
- 5) **Recommending Necessary Improvements in Computer Systems or Administrative Procedures.** When needed, the Privacy Officer will make recommendations to the Superintendent of improvements necessary in computer systems or administrative procedures in order to implement reasonable requests for confidential communications.

2400.02.06 Individual's Right to Notice of Privacy Practices

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

Individuals (or their parents) are entitled to a Notice detailing the privacy practices of the Agency. CCBDD will provide such Notice to each Individual (or their parents), in a manner compliant with both the HIPAA and FERPA regulations

AUTHORITY

[45 CFR § 164.520](#) Notice of privacy practices for protected health information

[45 CFR § 164.502\(i\)](#) Uses and disclosures consistent with Notice

[34 CFR 99.7](#) Notice (FERPA)

[34 CFR 300.612](#) Notice (IDEA Part B)

[34 CFR 303.404](#) Notice (IDEA Part C)

[ORC § 1347.08\(A\)\(3\)](#) (Personal Information Systems)

[OAC 3301-51-05](#)

[OAC § 5123:2-1-02\(M\)](#) County Board Administration – Records

[34 CFR 99.7](#) FERPA Annual Notification

LEGAL NOTES

FERPA and IDEA require an annual Notice. HIPAA requires a one-time Notice, with redistribution upon change. HIPAA requires signed acknowledgement of receipt.

AUDIENCE

Privacy Officer

PROCEDURES

- 1) **Drafting of Notice.** The Privacy Officer shall draft a Notice which is compliant with the requirements of the HIPAA, FERPA and IDEA regulations as well as OAC 3301-51-04(C). This shall include translations as necessary based on the language needs of the Individuals served. Further, the Notice shall be consistent with the Agency's privacy practices as detailed in these policies. Notice is detailed in Appendix, Notice of Privacy Practices.
- 2) **Updating Notice.** The Privacy Officer shall update the Notice as necessary based on changes in the Agency's privacy policies and/or the legal requirements as necessary. Upon update, the website and Notices posted at each facility (see below) shall be updated. Additionally, an updated copy will be provided to all Individuals receiving services and/or parents.
- 3) **Distribution of Notice.** The Privacy Officer shall ensure that Agency policies and procedures, namely [Policy 2400.02.06 Individual's Right to Notice of Privacy Practices](#) are maintained to ensure appropriate distribution of Notice:
 - A) All adults at intake, and children attaining age 18 as part of the Transfer of Parental Rights at Age of Majority, will be given a copy of the Notice of Privacy Practices. At the time that the Notice is provided, the Individual or guardian, shall sign an acknowledgement of his or her receipt of this Notice as part of the intake/transition of rights paperwork. This acknowledgement will be retained as part of the permanent record, for compliance with HIPAA requirements.
 - B) While the Individual is under age 18, the IDEA/FERPA Notice is included in the document *Whose IDEA is This?* and is distributed annually to all parents annually.
 - C) An additional copy of the Notice shall further be provided upon request by an Individual or parent.
- 4) **Posting of Notice.** The Privacy Officer shall ensure that the Notice is posted:
 - A) **Website.** On the Agency's website.
 - B) **At Each Facility.** At each facility, in a place where Individuals served can be reasonably expected to see the Notice, such as the reception areas of all Agency facilities.
 - C) Copies of the Notice will be maintained for 6 years, as detailed in [Policy 803 Records Retention and Destruction](#).

2400.03 CONFIDENTIALITY POLICIES FOR SUPERVISORS

2400.03.01 Business Associate Contracts

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD will obtain satisfactory assurance that Business Associates will safeguard PHI by maintaining appropriate HIPAA Business Associate agreements with businesses and MOUs with other governmental agencies.

AUTHORITY

[45 CFR 160.103](#)

[45 CFR § 45 CFR § 164.502\(e\)](#)

[45 CFR § 45 CFR § 164.504\(e\)](#)

[34 CFR 99.31\(a\)\(1\)\(i\)\(B\)](#)

[ORC § 5126.044](#) – Ohio Statute on confidentiality of records

PROCEDURES

- 1) **Business Associate Contract or Memorandum of Understanding.** CCBDD will have a written Business Associate Contract with every Business Associate. For a COG or other government agencies, a Memorandum of Understanding will be executed. See [Appendix A Identifying Business Associates](#).
- 2) **Annual Review of all Contractual Relationships.** On an annual basis, the HIPAA Privacy Officer will review all contractual relationships to verify that up-to-date Business Associate contracts are in place.
- 3) **Satisfactory Assurances.** The Business Associate Contract will provide satisfactory assurances that the Business Associate will not use or disclose the PHI of CCBDD Individuals receiving services other than as provided in the Business Associate Contract. The Business Associate Contract will conform to both the requirements of the HIPAA regulations. See [Appendix B - Sample HIPAA Business Associate Agreement](#).
- 4) **Material Breach or Violation of Business Associate Contract.** In the event CCBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, CCBDD will take steps to cure the breach or end the violation. If CCBDD is unable to cure the breach or end the violation, CCBDD will terminate the Business Associate Contract.

2400.03.02 Non-intimidation and Non-retaliation

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against Individuals receiving services who exercise any HIPAA-related right. Further, CCBDD will not intimidate or retaliate against staff or other persons who express the opinion that CCBDD policies are not consistent with the law, or not being implemented properly, or who file a whistleblower action. CCBDD will not require any Individual receiving services to waive any of his/her rights under HIPAA as a condition of education, treatment, or enrollment.

PROCEDURES

- 1) **CCBDD will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:**
 - A) **Individuals Receiving Services.** Any Individual for the exercise by the Individual of any right under, or for participation by the Individual in any process established by the HIPAA regulations;
 - B) **Individuals Receiving Services and others.** Any Individual receiving services, or other person for:
 - i) Filing of a complaint with the Secretary of HHS regarding a HIPAA issue;
 - ii) Testifying, assisting or participating in an investigation, compliance review, proceedings or hearing under Part C of Title XI; or
 - iii) Opposing any act or practice made unlawful by the HIPAA regulations, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information.
- 2) **Retaliatory action is defined as doing any of the following:**
 - A) Removing or suspending the employee from employment;
 - B) Withholding from the employee salary increases or employee benefits to which the employee is otherwise entitled;
 - C) Denying the employee a promotion that would have otherwise been received;
 - D) Transferring or reassigning the employee;
 - E) Reducing the employee in pay or position.
- 3) **Non-retaliation statement.** A person who in good faith brings a complaint will not be subject to retaliation. Retaliation against any person who falls within this definition, either Individual served or staff member of CCBDD, is strictly prohibited.
- 4) **Prohibition against Waiver of Rights.** No office, program, facility or employee of the CCBDD shall require Individuals to waive any of their rights under HIPAA as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits. The Agency may require parents of children under age 18 receiving services reimbursed by Medicaid to sign an authorization granting the Agency permission to bill Medicaid.
- 5) CCBDD will also follow [Policy 324 Protection of Whistleblowers](#) as appropriate.

2400.03.03 HIPAA Assignments and Documentation

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD will maintain written Policies and Procedures, including a 6-year audit trail. In addition, all documentation required by HIPAA regulations will be maintained for 6 years. The HIPAA Privacy Officer shall be responsible for insuring the proper maintenance of all required documentation.

AUTHORITY

[Federal Law 45 CFR § 164.530\(j\)](#) – Documentation requirement,
[45 CFR § 164.520\(e\)](#) – Notices of Privacy Practices;
[45 CFR § 164.524\(e\)](#) – Access of individuals to protected health information;
[45 CFR § 164.526\(f\)](#) – Amendment to protected information;
[45 CFR § 164.508\(b\)\(6\)](#) – Uses and disclosures for which an authorization is required;
[45 CFR § 164.512\(i\)\(2\)](#) – Uses and disclosures for research purposes;
[45 CFR § 164.522\(a\)\(3\)](#) – Rights to request privacy protection for protected health information;
[45 CFR § 164.528\(d\)](#) – Accounting of disclosures of protected health information – Implementation specification
[ORC § 5126.044\(E\)](#) (General records of DD Boards)

LEGAL NOTES

State law requires notice and approval prior to destruction of an Individual's records which contain PHI. There is no comparable requirement in HIPAA.

PROCEDURES

- 1) **Designating a Privacy Officer and Other Individuals to Assist HIPAA Committee.** The superintendent shall designate a person to be the Privacy Officer, who is responsible for development, implementation, enforcement, and update of HIPAA Privacy policies and procedures. The superintendent may also designate other persons to assist, a HIPAA committee, which may include representatives from each program (e.g. workshop, adult services, residential services, administration, SSA, information systems).
- 2) **Documenting Records Covered by HIPAA and FERPA.** The records covered by HIPAA and FERPA shall be detailed and documented following the procedures for the "Designated Record Set" of the HIPAA regulations.
- 3) **HIPAA Mandated records.** HIPAA Mandated records include the following:
 - A) HIPAA Required designations, including, Hybrid entity designation if applicable, description of records in Designated Record Set, the names of staff responsible for duties of Privacy Officer, receiving HIPAA complaints, providing access to Individual records, receiving requests for amendment of Individual records, answering questions about HIPAA policies and procedures. See Appendix F.
 - B) Notice of Privacy Practices, as described in [Policy 2400.02.06 Individual's Right to Notice of Privacy Practices](#).
 - C) Restrictions on use or disclosure of PHI agreed to by CCBDD as described in the [Policy 2400.02.04 Individual's Right to Request Additional Restrictions](#).
 - D) Records of disclosures, as required by the [Policy 2400.02.03 Individual's Right to Receive an Accounting of Disclosures](#).
 - E) Any signed authorization as described in [Policy 2400.01.06 Authorizations](#).
 - F) All privacy-related complaints received, and their disposition, if any, as described in [Policy 2400.03.04 Privacy Complaints](#).
 - G) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in [Policy 2400.01.09 Duty to Report Violations and Security Incidents](#).
 - H) Documentation that persons responsible for risk management decisions have reviewed each risk analysis, and records of risk management actions taken, as specified in [Policy 2500.01.01 Security Management Process](#).

I) Incident Reports and other documentation specified by [Policy 2500.01.08 Breach Reporting](#) and Policy [2500.04.05 Security Incident Response and Reporting](#).

The above records will be maintained for 6 years.

- 4) **Policy and Procedure Audit Trail.** When created or updated, all policies will be annotated with the approval date and revision history. Current policies will be maintained in a computer file folder designated as the current policies. Any previous versions will be kept in a computer file folder designated by year of decommissioning.
- 5) **Updating Required Designations.** The Privacy Officer, will maintain and update HIPAA Required Designations as necessary.
- 6) **Compliance Notes.** The Privacy Officer and Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, and internal audit activities.
- 7) **Internal Audit.** The Privacy Officer shall conduct a periodic audit, as necessary, to ensure proper maintenance of all documentation itemized in this policy.
- 8) See also [Policy 803 Records Retention and Destruction](#) for retention periods and destruction procedures.

2400.03.04 Privacy Complaints

Adopted: 7/1/2013

Revised Date:

Effective:

POLICY

Any Individual or employee to may complain about the CCBDD's Confidentiality and Privacy policies and procedures and/or the CCBDD's compliance with those policies and procedures. The CCBDD shall take action and document all such complaints.

AUDIENCE

All Staff

AUTHORITY

[45 CFR § 164.530](#)(d) HIPAA complaint procedures

[ORC § 5123.64](#)(A) requires establishment of a complaint procedure

[OAC § 5123:2-1-12](#) administrative resolution of complaints involving the programs, services, policies, or administrative practices of a county board or the entities acting under contract with a county board

PROCEDURES

- 1) **The HIPAA Privacy Officer shall manage this complaint process**, and shall be designated in the Notice of Privacy practices as the person to receive complaints.
- 2) The CCBDD will extend the provisions of [Policy 324 Protection of Whistleblowers](#), to all persons who file confidentiality or privacy related complaint.
- 3) **Employee to File Written Complaint with Privacy Officer.** An employee or Individual should file their complaint in writing to the Privacy Officer. Employees may review [Policy 324 Protection of Whistleblowers](#) which provides for alternate officials to receive the written complaint.
- 4) **Review and Investigation of Complaint.** Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Superintendent) shall review and investigate the complaint.
- 5) **Corrective Action.** If warranted, the Privacy Officer shall take corrective action, which may include:
 - A) Change of policy and/or procedure.
 - B) Intervention with an employee who is not following procedures including additional training and/or sanctions.
 - C) Other action as appropriate.
- 6) **Communicating Results of Investigation and Corrective Action.** The Privacy Officer shall communicate the results of the investigation and any corrective action taken to the person filing the complaint.
- 7) **Documentation of Complaints.** The CCBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with [Policy 2400.03.03 HIPAA Assignments and Documentation](#).

2400.03.05 Policy Updating and Staff Training

Effective Date: 7/1/2013

Revised Date:

Approved: 7/1/2013

POLICY

CCBDD's HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to ensure that policies and procedures required by HIPAA, FERPA/IDEA and other laws are updated at least annually for compliance, and to train staff as necessary on these policies and procedures.

AUTHORITY

[45 CFR § 164.530\(b\)](#)

[45 CFR § 164.530\(i\)](#)

[45 CFR § 164.520](#)

[ORC § 5123.64\(A\)](#) training in rights

[OAC § 5123:2-5-01\(E\)](#) training requirements for adult service workers

[OAC § 5123:2-5-02\(D\)](#) training requirements for adult service workers

[OAC § 5123:2-5-05\(D\)](#) training requirements for early intervention workers

[OAC § 5123:2-5-07](#) training requirements for investigative agents

PROCEDURES

- 1) **Annual Review and Update of All Policies.** The HIPAA Privacy Officer shall conduct an annual review of all policies, and update policies as necessary based on new circumstances, changes in federal regulations and any changes in Ohio state laws and regulations governing DD Boards. An audit trail of policy changes will be maintained as detailed in [Policy 2400.03.03 HIPAA Assignments and Documentation](#).
- 2) **Training New Staff on Confidentiality and Computer Security Policies.** The HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to ensure that all new staff will be receive training on CCBDD Confidentiality and Computer Security policies promptly after hiring. The two officers shall create an appropriate training program. See [Policy 320 Orientation and Training](#).
- 3) **Training All Staff When Policies are Substantially Changed.** The HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to ensure that staff receive training on Confidentiality and Computer Security policies when they are substantially changed. This training shall be implemented as detailed in [Policy 320 Orientation and Training](#).

APPENDICES

Appendix A: Identifying Business Associates

Identifying your Business Associates

County Boards of DD are obligated to identify and place any “Business Associate” under a contract that meets the specifications of the HIPAA regulations. Further, these Business Associates, as of January 25, 2013, are directly regulated by the HIPAA regulations and for the first time are subject to the same civil and criminal penalties for any failures to comply with the portions of the HIPAA regulations that apply to them.

An abbreviated definition of “Business Associate” is a person or entity, other than a member of the workforce, that performs certain functions, activities or provides services that involve the use or disclosure of PHI on behalf of a DD Board.

More specifically, the functions and activities that create a Business Associate relationship are:

- claims processing or administration,
- data analysis, processing or administration,
- utilization review,
- quality assurance,
- patient safety activities listed at 42 CFR 3.20,
- billing,
- benefit management,
- practice management,
- repricing,
- legal,
- actuarial,
- accounting,
- consulting,
- data aggregation,
- management,
- administrative,
- accreditation or
- financial services.

Subcontractors of Business Associates are Business Associates. A significant change in the January 25, 2013 HIPAA Rule changes is that subcontractors of your business associates, who have access to PHI, are now Business Associates. For example, suppose you contract with your COG to handle all of your MUI investigations. The COG subcontracts with an independent agency XYZ to do this work. Agency XYZ is a Business Associate. However, it is the COGs responsibility, not yours, to place XYZ under the Business Associate contract.

Common examples of Business Associates for DD Boards include

- A consultant that performs utilization reviews, compliance audits, financial services or billing support.
- A software vendor who provides customer support involving access to PHI.
- A computer contractor that provides support for Agency software and/or its computer network and has access to PHI as part of its support and service capacity.
- An contractor who carries out MUI investigations.
- A COG which manages IO waiver contracts for member DD Boards (or any other function involving PHI)
- An accreditation organization (such as CARF or JCAHO) that reviews PHI as part of the accreditation process.
- An attorney whose legal services involve access to protected health information.
- A CPA firm whose accounting services involve access to protected health information.

Examples of relationships which are NOT Business Associates

- 1) A Provider contracted by the Agency to provide services, billed to Medicaid under its own Provider number, such as a provider of psychological, speech, OT or PT services.
- 2) A Provider with a contract subject to ORC § 5126.035, such as a Provider of waiver or supported living services which bills Medicaid under its own Provider number.
- 3) Ohio Department of Developmental Disabilities. There are numerous interactions with DODD. DODD is a health oversight agency and a payer.
- 4) Cleaning services. However, since these organizations may be able to easily and inappropriately access PHI, it is appropriate to include a confidentiality clause in their agreement that expressly prohibits such behavior.
- 5) Contractors such as electricians, plumbers, exterminators who perform services in Agency facilities.
- 6) Contractors who perform construction or remodeling of an Individual's house for accessibility or other adaptive living.

Full Definition of Business Associate from the HIPAA Rules (1/25/2013 Revision):

- 1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:
 - A) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
 - B) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §45 CFR § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
- 2) A covered entity may be a business associate of another covered entity.
- 3) Business associate includes:
 - A) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
 - B) A person that offers a personal health record to one or more Individuals on behalf of a covered entity.
 - C) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.
- 4) Business associate does not include:
 - A) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the Individual.
 - B) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 45 CFR § 164.504(f) of this subchapter apply and are met.
 - C) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
 - D) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Appendix B: Sample HIPAA Business Associate Agreement

County Boards are obligated to place Business Associates under a contract that meets detailed specifications that were updated on 1/25/2013. Below is a contract that meets these specifications. Note that it must be customized in Appendix A with a brief clause which defines the “allowed uses and disclosures”. Several example clauses are included.

Any new contracts must comply with the new specifications.

Limited Grandfathering of Existing Contracts. BA Contracts compliant with earlier specifications that existed prior to 1/25/2013 and were renewed no later than 3/26/2013 will be deemed compliant until 9/22/2014. However, if the agreement is renewed on or after 9/23/2013, it must be updated to the new specifications.

HIPAA BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE Agreement (“Agreement”) is entered into by and between _____ (“BUSINESS ASSOCIATE”) and _____ (the “COVERED ENTITY”).

RECITALS

- 1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 45 CFR § 164. This agreement is written to comply with the revisions enacted in the HITECH statute in February 2009, the regulation changes published in August 2009 and further updates published January 25, 2013.
- 2) Terms used in this agreement, including but not limited to “covered entity”, “business associate”, “Protected Health Information (PHI)”, “unsecured protected health information”, “use”, “disclose”, “breach”, and “security incident”, shall have the same meaning as defined in most current versions of the above referenced regulations.
- 3) COVERED ENTITY is a covered entity and regulated by the HIPAA regulations.
- 4) Per the January 25, 2013 HIPAA Regulation changes, BUSINESS ASSOCIATE is also regulated by the HIPAA regulations, and further agrees to comply with the unique requirements of this agreement.

NOW, THEREFORE, in consideration of the foregoing, the parties agree as follows:

- 1) **Allowed Uses and Disclosures of Protected Health Information.** The BUSINESS ASSOCIATE provides services for the COVERED ENTITY. The BUSINESS ASSOCIATE may use and disclose protected health information only as follows:
 - A) BUSINESS ASSOCIATE may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, BUSINESS ASSOCIATE may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.
 - B) BUSINESS ASSOCIATE may further use and disclose PHI, if necessary:
 - i) for the proper management and administration of the BUSINESS ASSOCIATE’s business, and/or
 - ii) to carry out the legal responsibilities of the BUSINESS ASSOCIATE if the disclosure is either
 - a) required by law, or
 - b) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person

notifies the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.

- 2) **Responsibilities of BUSINESS ASSOCIATE.** With regard to its use and disclosure of protected health information, BUSINESS ASSOCIATE agrees to do the following:
- A) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.
 - B) Use appropriate physical, technical and administrative safeguards to protect electronic PHI, and comply with the requirements of the HIPAA Security Regulations (45 CFR § 164 Subpart C) which are applicable to business associates.
 - C) Report to the COVERED ENTITY any security incident, and any use or disclosure not provided by this contract, including breaches of unsecured protected health information as required by 45 CFR § 164.410.
 - D) Require that subcontractors who create, receive, maintain or transmit ePHI on behalf of Business Associate comply with applicable HIPAA Security regulations by entering into a Business Associate contract with these subcontractors. The Business Associate contract shall meet the specifications of 45 CFR § 164.314.
 - E) Make available to the Individual any requested protected health information, in accordance with procedures specified by COVERED ENTITY and in compliance with 45 CFR § 164.524, "Access of individuals to protected health information".
 - F) Make available for amendment, and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR § 164.526, "Amendment of protected health information".
 - G) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528.
 - H) To the extent that BUSINESS ASSOCIATE is to carry out COVERED ENTITY's obligations under the HIPAA Privacy Regulations, 45 CFR § 164 Part E, comply with the requirements of the Privacy Regulations in the performance of those obligations.
 - I) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the COVERED ENTITY's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.
 - J) Return to the COVERED ENTITY or destroy, as requested by the COVERED ENTITY, within 30 days of the termination of this Agreement, the protected health information in BUSINESS ASSOCIATE's possession and retain no copies or electronic back-up copies. If this is not feasible, BUSINESS ASSOCIATE will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.
- 3) **Mutual Representation and Warranty.** Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.
- 4) **Term and Termination.**
- A) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.
 - B) Termination. As provided for under 45 C.F.R. §45 CFR § 164.504, the COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that the BUSINESS ASSOCIATE has breached a material provision of this Agreement. Alternatively, the COVERED ENTITY may choose to: (i) provide the BUSINESS ASSOCIATE with 30 days written notice of the existence of an alleged material breach; and (ii) afford the BUSINESS ASSOCIATE an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

- 5) **Survival.** The respective rights and obligations of BUSINESS ASSOCIATE and COVERED ENTITY under the provisions of paragraph 2J above, detailing BUSINESS ASSOCIATE’s return and/or ongoing protections of protected health information, shall survive the termination of this Agreement.
- 6) **Amendment.** This Agreement supersedes any previously negotiated HIPAA Business Associate agreements. Further, it may be modified or amended only in writing as agreed to by each party.
- 7) **Notices.** Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party’s address given below as follows:

If to BUSINESS ASSOCIATE _____

If to COVERED ENTITY: _____

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of _____.

BUSINESS ASSOCIATE

COVERED ENTITY

By: _____
 Name: _____
 Title: _____
 Date: _____

By: _____
 Name: _____
 Title: _____
 Date: _____

Attachment A – Permitted Uses and Disclosures

BUSINESS ASSOCIATE is authorized to use protected health information for the purposes of

[INSERT A CLAUSE THAT DESCRIBES BUSINESS ASSOCIATE’S ALLOWED USES AND DISCLOSURES. THIS WILL VARY DEPENDING ON THE NATURE OF THE RELATIONSHIP. THE FOLLOWING IS AN EXAMPLE OF A CLAUSE FOR A BILLING SERVICE.]

Example Clauses:

MUI Investigator: Business Associate is authorized to use and disclose protected health information for the purposes of conducting MUI investigations.

Fiscal Services Consultant: Business is authorized to use protected health information for the purposes of providing fiscal consulting services.

Computer Software Vendor: Business Associate is authorized to use and disclose protected health information for the purposes of providing software training, support and troubleshooting.

Computer Network Support Consultant: Business Associate is authorized to use and disclose protected health information for the purposes of providing computer network support services.

Appendix C: Sample Privacy & Security Officer Job Descriptions

HIPAA Privacy Officer Job Description

REPORTS TO: Superintendent

General Purpose:

The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the CCBDD's policies and procedures covering the privacy of, and access to, Individual health information in compliance with federal and state laws and the CCBDD's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of CCBDD information privacy policies and procedures in coordination with CCBDD management and administration, the HIPAA Committee, and legal counsel.
- Works with CCBDD senior management to establish an CCBDD-wide HIPAA Committee.
- Serves in a leadership role for all HIPAA activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and the HIPAA committee to ensure the CCBDD has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current CCBDD and legal practices and requirements.
- Oversees, directs, delivers, or ensures delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Assists HIPAA Security Officer with handling of any security incidents and/or security rule violations.
- Establishes with management and operations a mechanism to track access to protected health information, within the purview of the CCBDD and as required by law and to allow qualified persons to review or receive a report on such activity.
- Works cooperatively with the applicable CCBDD units in overseeing Individual rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the CCBDD's privacy policies and procedures and, when necessary, legal counsel.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all persons in the CCBDD's workforce, extended workforce, and for all business associates, in cooperation with administration, and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the CCBDD and related entities.
- Assists HIPAA Security officer by reviewing all system-related information security plans throughout the CCBDD's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all CCBDD personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the CCBDD's policies and procedures and legal requirements
- Maintains current knowledge of federal privacy laws, specifically HIPAA and FERPA, as well as state privacy laws, accreditation standards, and monitors advancements in information privacy technologies to ensure CCBDD adaptation and compliance.
- Serves as information privacy consultant to the CCBDD for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.

- Works with CCBDD administration, legal counsel, and other related parties to represent the CCBDD's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications of Privacy Officer:

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of health information management, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

Appendix D: Minimum Necessary – Workforce, Disclosures and Requests

Workforce Access to PHI and Safeguards

<i>Person, Classes of Persons, or Business Associates</i>	<i>Categories of PHI Needed</i>	<i>Additional Safeguards(*)</i>
Administration		
Superintendent	All	
Business Manager	All	
Medicaid/Records Clerk	All	
Nurse	Medical notes, relevant medical information	
Administrative Assistant	Computer data	
Janitor	None	No User ID will be provided
Adult Services		
Workshop Director	All	
Habilitation Program Manager	All	
Production Manager	Medical Needs	
R.S.A.S.W's	Medical Needs	
Account Clerk	Medical Needs	
Secretary I	Medical Needs	
Language Development Specialist	Medical Needs, notes pertinent to speech/language	
Service & Support		
Service & Support Director	All	
Service & Support Coordinators	All	
Transportation/Maintenance		
Vehicle Operators	Medical needs related to transportation	No User ID will be provided; medical needs and behavioral support needs will be provided in hardcopy format by SSA
Grounds Maintenance	None	No User ID will be provided;
School		
M.H. Coordinator	records regulated under FERPA	
Classroom Instructors	records regulated under FERPA	
Instructor Assistants	records regulated under FERPA	
Language Development Specialist	Medical Needs, notes pertinent to speech/language	
Early Intervention Specialists	All Early Intervention files	
Business Associates		
County Auditor's Office	records pertinent to bill payment	

XYZ Computer	All computer data	
Primary Solutions, Inc.	Gatekeeper Data	
Special Olympics Coordinator	Medical needs	

*Safeguards: All employees will receive training on Agency confidentiality policies and will be subject to sanctions for violations. The table above lists additional safeguards that will be employed.

Procedures for Routine Disclosures of PHI

Note: Disclosures to medical, vocational, residential and other providers, and service coordination with other agencies are “treatment” and not part of Minimum Necessary procedures.

- 1) **Software & Network Providers** – Information in the computer system is incidentally available during system support activities.
 - A) **XYZ Support.** Network support vendor XYZ Support is under contract to provide 24/7 network support. Access is provided at all times.
 - B) **Gatekeeper and other Support.** Primary Solutions and other support vendors will be granted access rights on an as needed basis. Technical solutions for implementing this authorization will be deployed by the Agency.
- 2) **Job and Family Services** – For services rendered, which are reimbursed by ODJFS, submit requested information to JFS.
- 3) **Health Department** – Contents of the early intervention file may be shared with the Health Department, upon their request, if the initial referral for services came through the Help Me Grow network.
- 4) **Prosecutor’s Office.** When a warrant or subpoena is presented, any file may be released to the Prosecutor’s Office. In addition, if the Agency is seeking legal counsel, file contents to be revealed will be reviewed by the Privacy Officer to ensure that minimum necessary standards are being followed.
- 5) **Auditor’s Office** – When authorizing payment of bills, fiscal files may be reviewed by the Auditor’s office prior to authorization of payment.
- 6) **DODD** – Information will be shared routinely with Ohio DODD in order to ensure continuity of services for Individuals. Specific to MUI case files, the Investigative Agent and internal UI staff will utilize the State’s secure website to input required information.
- 7) **Surveyors** – Upon confirmation of surveyors’ credentials, the superintendent or his/her designee may authorize review of any files requested by the surveyor with the exception of MUI State Files.
- 8) **Transportation Providers** – To ensure quality of care for Individuals, medical needs and guardian/family contact information will be shared with contracted providers.
- 9) **County School Districts** – Individual information will be shared, upon written request on School District letterhead, if the request for services originated in the school district.
- 10) **Bureau of Disability Determination** – Using the Bureau’s forms, assessment information will be shared in order to determine Individual’s eligibility for benefits.
- 11) **Attorneys** – When a subpoena is presented, the protocol in [Policy 2400.01.10 Disclosures that do Not Require an Authorization](#) will be carefully followed to determine, with legal counsel assistance, if the subpoena should be honored.
- 12) **Other Outside Agencies** – In order to ensure continuity of services to Individuals, the Director of SSA or the Director of Adult Services will share IP, medical limitation and incident reports with authorized contacts from Family Services.
- 13) **Law Enforcement** – As identified by the Director of Services & Supports, guardianship, family contact information and behavior support plans will be shared with law enforcement agencies. In addition, upon presentation of a warrant and verification of credentials if presented in person, other file information may be shared with law enforcement agencies. See [Policy 2400.01.10 Disclosures that do not Require an Authorization](#).

Procedures for Routine Requests of PHI

- 1) **Eligibility Inquiry** – Individual insurance eligibility will be verified by using procedures provided by the Ohio Dept of DD.

Appendix E – Change Log and Formatting Notes

Formatting Notes

- 1) The abbreviation CCBDD is used for the abbreviated Agency name throughout the document. A global replace for your preferred abbreviation is recommended.
- 2) The hyperlinks throughout the policy manual are best utilized with an online version of this manual. It can be saved either as a PDF or a HTML web page, which provides easy online access to all staff. If saved in HTML format it can be viewed in a web browser.
- 3) The Style “Heading 1” is used for Policy titles. A Microsoft Word bookmark is placed at the beginning of each Policy Title, and at beginning of certain key terms in the definitions page. It is essential that these bookmarks remain intact so that the hyperlinks to operate properly. To avoid deleting these bookmarks, it is best to set Word Options as follows. In the “Advanced” section, under “Show Document Content”, select “Show Bookmarks”.
- 4) The Table of Contents on the following page is a Microsoft Word “TOC” field, which can be updated by selecting the table of contents and pressing the F9 key. This will recreate the table of contents (policy names, page numbers) based on your changes.

Change Log

Date	Policy	Description

Clermont County Board of Developmental Disabilities (CCBDD) - Authorization Form

Thomas A. Wildey Center
2040 US Highway 50
Batavia, OH 45103
513-732-7000

AUTHORIZATION FOR RELEASE OF CONFIDENTIAL INFORMATION

Name of Individual Served _____ Date of Birth _____

I authorize CCBDD to:

Release to: _____

Obtain from: _____

The following information:

The following information:

Assessment and diagnosis (MFE)

Assessment and diagnosis (MFE) (F.E.D.)

Treatment and progress

Treatment and progress

Social History

Most current IP (ISP, IEP, IHP)

Psychological Test results

Psychological Test results

Other _____

Results of recent physical examination

Other _____

The purpose of this disclosure is

Coordination of care

Requested by Individual Receiving Services, or guardian/parent

Other _____

- 1) I understand that I may revoke this authorization at any time by submitting a written request, unless the records have already been released.
- 2) I understand that the party receiving my information might not be subject to HIPAA, FERPA or Ohio confidentiality laws and might be allowed to disclose this information.
- 3) The CCBDD does not require that I sign this authorization in order to receive services.

Expiration Date:

90 days from date signed

other date: _____

Approved by: _____ Date: _____

If signed by someone other than the Individual being served:

Print Name _____

Authority to sign: Parent or Guardian

Appointed by Individual as HIPAA Personal Representative

Other _____

For staff use (complete the following steps and indicate by a check. Name of Staff Person _____)

Copy of signed authorization given to Individual / Parent / Guardian

Copy of records released given to Individual / Parent / Guardian (if requested)

Disclosure logged on Disclosure Log

Revocation received on _____ and acted upon.

Notice of Privacy Practices

Clermont County Board of Developmental Disabilities

FOR YOUR PROTECTION

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. IT ALSO DESCRIBES OUR PRACTICES ABOUT Thomas A. Wildey Center SCHOOL RECORDS.

YOUR RECORDS ARE PRIVATE

We understand that information we collect about you or your child and records of the services and supports we provide, are personal. Keeping these records private is one of our most important responsibilities. The Agency must follow many laws to protect your privacy. For the Thomas A. Wildey Center School records, we follow the federal FERPA laws. For adult services, and certain services for children, we follow the federal HIPAA laws. In addition, we follow many laws specific to Ohio Developmental Disability Boards. For this notice, we will use the term "records" to mean the paper or electronic records we maintain about you.

Your records may be used and disclosed by the employees and volunteers at the Agency who serve you, as well as persons or agencies who work for us and sign strict confidentiality contracts.

Our organization includes Thomas A. Wildey Center.

At Thomas A. Wildey Center School, for example, records may be shared with "school officials" who have a "legitimate educational interest" in your child. "Educational interest" means any matter related to your child's instruction, developmental or behavioral support, dietary, health or safety. "School officials" include teachers, paraprofessionals, aides, bus drivers and administrators at Clermont County Board of Developmental Disabilities.

WHO USES AND DISCLOSES MY RECORDS?

In general, we use and disclose your information:

- For teaching, behavioral and medical support, transportation and school administration. For example, a school administrator will review progress data created by teachers.
- To provide the full range of services we provide: early intervention, habilitation, supported employment, and other services. For example, your service and support coordinator will review your records to create an ISP, which may be shared with you, your guardian, a vocational specialist, and other persons involved with providing services and supports to you.
- To get payment for services provided: for example, the billing clerk uses service records of services provided to submit bills to the Ohio Department of Developmental Disabilities, and
- For other operations to operate and manage the Agency: these include improving quality of care, training staff, managing costs, and conducting other business duties. For example, a quality assurance reviewer may audit your records to determine whether appropriate services were provided,
- To remind you or a guardian of an appointment for services,
- The Agency or an affiliated foundation may contact you to raise funds. You have the right to opt out of any fundraising communications.

COULD MY RECORDS BE RELEASED WITHOUT MY PERMISSION?

There are limited situations when we are permitted or required to disclose your records, or parts of them, without your signed permission. These situations include:

- Record transfers to other schools your child enrolls in,
- Reports to public health authorities to prevent or control disease or other public health activities,
- To protect victims of abuse, neglect, or domestic violence,
- For oversight including investigations, audits, accreditation and inspections, such as are conducted by the Ohio Department of Developmental Disabilities, Ohio Department of Education and federal agencies,
- When a court order, subpoena or other legal process compels us to release information,
- Reports to law enforcement agencies when reporting suspected crimes, when responding to an emergency, or in other situations when we are legally required to cooperate,

- In connection with an emergency, or to reduce or prevent serious threat to public health and safety, or the safety of a person,
 - to coroners, medical examiners and funeral directors,
 - to victims of alleged violence or sex offenses,
 - For workers' compensation programs,
 - For specialized government functions including national security, protecting the president, operating government benefit programs, and caring for prisoners,
 - In connection with "whistleblowing" by an employee of the Agency.
- All other uses not described above require that we obtain your signed permission.

WHAT IF MY RECORDS NEED TO GO SOMEWHERE ELSE

For any purpose not described above, we will release your information only with your explicit written authorization. Federal law requires that we notify you that any healthcare provider must obtain your explicit permission to release your information for any of the following:

1. Psychotherapy Notes will only be released with your signed authorization;
2. For marketing purposes;
3. To sell information about you.

It has never been the Agency's practice to release information for marketing purposes or to sell your information. Your written authorization tells us what, where, why and to whom the information must be sent. Your signed authorization is good until the expiration date you specify. You can cancel your permission at any time by letting us know in writing.

WHAT ARE MY RIGHTS REGARDING PRIVACY, ACCESS TO MY RECORDS, AND THE ACCURACY OF MY RECORDS?

You have legal rights concerning your privacy, access to your records, and the accuracy of your records. You have the following rights:

1. To see your records, or to get a copy, including an electronic copy;
2. To request a correction to your records if you believe they are incorrect;
3. To receive all communications at a confidential address or phone number;
4. To receive an "accounting of disclosures", that is, a list of any place we sent your record without your authorization;
5. To request additional limits on how we use or disclose your information, although we are not obliged to honor these requests except that if you choose to personally pay for services delivered, we will not bill Medicaid.
6. You may receive a paper copy of this notice.

To exercise any of these rights, or if you have any questions or complaints regarding our privacy practices, call, deliver, mail or email your request to:

[Kathy Booth](mailto:kbooth@clermontdd.org)
 Clermont County Board of DD
 2040 US Highway 50
 Batavia, OH 45103
 513-732-7000
kbooth@clermontdd.org

Ask any employee if you need help in putting your request in writing.

OUR DUTIES

We are obligated by law to maintain the privacy of your information and to provide this notice. In the event of a breach, that is, an improper disclosure of your information, we are required to notify you. We are required by law to abide by the terms of this notice. From time to time we may make changes to our policies, and if and when we do, your records will be protected by our new, changed policies. Our current notice will always be available on our website.

QUESTIONS OR COMPLAINTS?

If you have any questions or complaints about our privacy practices, please contact us:

[Attn: Kathy Booth](mailto:kbooth@clermontdd.org)
 Clermont County Board of DD
 2040 US Highway 50
 Batavia, OH 45103
 513-732-7000
kbooth@clermontdd.org

We will never retaliate against you for filing a complaint. Further, if you are not satisfied with the results, you may also complain to the federal government:

For School issues:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

For any other issues:
Secretary of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201
www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

Current Revision effective 1/1/2018.

