CARROLL COUNTY BOARD OF DD

Confidentiality & Computer Security Policies

HIPAA, FERPA, IDEA & Ohio Law Compliance

Updated March 2019

Adopted by Carroll County Board of Developmental Disabilities

Date: _____

Signature of Board Officer:

_____

Policies governing confidentiality of the information regarding the individuals we serve, their privacy rights, and safeguarding the availability and integrity of electronic records.

Eagle Consulting Partners, Inc.
6779 Memphis Ave. #7
Cleveland, OH 44144
216.503.0333

gpritts@eagleconsultingpartners.com
www.eagleconsultingpartners.com

CONFIDENTIALITY AND COMPUTER SECURITY POLICIES

Change Log

Date	Policy	Description

Table of Contents

CONFIDENTIALITY AND COMPUTER SECURITY POLICIES

CONFIDENTIALITY & PRIVACY POLICIES

POLICIES FOR ALL STAFF

1000 Confidentiality, Privacy and Computer Security Definitions

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
The following definitions shall apply to all Confidentiality, Privacy, and Computer Security Policies, numbered 1000 through 4000.

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.

DEFINITIONS
1) **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.)
2) **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.
3) **Agency** – means CCBDD
4) **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.
5) **Authentication –** means the corroboration that a person is the one claimed.
6) **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.
7) **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.
    a) Breach *excludes*:
        i) 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.
        ii) 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.
        iii) 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.
    b) Except for the 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:

i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
ii) The unauthorized person who used the PHI or to whom the disclosure was made;
iii) Whether the PHI was actually acquired or viewed; and
iv) The extent to which the risk to the PHI has been mitigated.

8) **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.
9) **Confidentiality –** means the property that data or information is not made available or disclosed to unauthorized persons or processes.
10) **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.
11) **Designated Record Set –** Designated record set means:
    a) A group of records maintained by or for a covered entity that is:
        i) The medical records and billing records about Individuals maintained by or for a covered health care provider;
        ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
        iii) 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.
12) **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.
13) **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.
14) **DODD** – the Ohio Department of Developmental Disabilities
15) **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
16) **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.
17) **Education Records** –
    a) As defined in the FERPA regulations, means records that are:
        i) Directly related to a student; and
        ii) Maintained by an educational agency or institution or by a party acting for the agency or institution.
    b) The term does **not** include:
        i) 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.
        ii) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
        iii) Either of the following:
            (1) Records relating to an Individual who is employed by an educational agency or institution, that:
                (a) Are made and maintained in the normal course of business;
                (b) Relate exclusively to the Individual in that Individual's capacity as an employee; and
                (c) Are not available for use for any other purpose.
            (2) 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

(b)(iii)(1) of this definition.

iv) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
   (1) 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;
   (2) Made, maintained, or used only in connection with treatment of the student; and
   (3) 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.

v) 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.

vi) Grades on peer-graded papers before they are collected and recorded by a teacher.

18) **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.

19) **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.

20) **Facility –** means the physical premises and the interior and exterior of a building(s).

21) **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.

22) **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

23) **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.

24) **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.

25) **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 CFR § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

26) **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.

27) **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

28) **HIPAA –** HIPAA means the Health Insurance Portability and Accountability Act of 1996, cited in Pub.L. 104–191 and 110 Stat. 1936 and its regulations in 45 CFR Parts 160, 162 and 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.

29) **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.

30) **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.

31) **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.

32) **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.

33) **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.
34) **Integrity –** means the property that data or information have not been altered or destroyed in an unauthorized manner.
35) **Malicious software –** means software, for example, a virus, designed to damage or disrupt a system.
36) **May** – means the individual or entity is empowered, but not required, to perform the specified task.
37) **MOU –** MOU means a Memorandum of Understanding between governmental entities, which incorporates elements of a business associate contract in accordance with HIPAA rules.
38) **Must** – means the individual or entity is required to either perform or refrain from performing the following action. See also "Shall".
39) **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 his or her own behalf, unless he/she has a court-appointed guardian
40) **Password –** means confidential authentication information composed of a string of characters.
41) **Payment –** means, in the context of a County Board of DD:
    a) Both:
        i) Activities undertaken by the Agency to obtain reimbursement for services rendered, for example, from Medicaid of DODD, to Individuals served.
        ii) Activities undertaken by the Agency to provide reimbursement to contracted providers for services provided to Individuals 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.
42) **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.
43) **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.
44) **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.
45) **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.
46) **Psychotherapy Notes –** means notes recorded (in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
47) **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.

48) **Security or Security measures –** encompass all of the administrative, physical, and technical safeguards in an information system.
49) **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.
50) **Shall** – means the individual or entity is required to either perform or refrain from performing the following action. See also "Must".
51) **Should** – means the individual or entity is recommended to perform the specified task, even though the task may not be required.
52) **Social Engineering –** means "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information, he needs 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.
53) **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.
54) **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
55) **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers. This definition includes 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.
56) **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.
57) **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.
58) **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.
59) **User –** means a person or entity with authorized access.
60) **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.
61) **Workforce Member –** Workforce Member means the same as Employee. See definition above.
62) **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.

1010 Confidentiality – General Rules

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 1050 Authorizations.
   c) As permitted in Policy 1040 Speaking with the Family or Friends of an Individual Receiving Services.
   d) As permitted by in Policy 1090 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 1020 Minimum Necessary Policy.
3) All employees are responsible for safeguarding the information regarding Individuals served by CCBDD, as detailed in
   a) Policy 1030 Confidentiality Safeguards (Oral & Written)
   b) Policy 3080 Computer Usage
   c) Policy 3082 Social Media Use
   d) Policy 3085 Portable Computing Devices
   e) Policy 3087 Employee Work at Home
4) Rights of Individuals served by CCBDD may be exercised by parents, guardians and personal representatives as detailed in Policy1070 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 1080 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.

1020 Minimum Necessary Policy

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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
1) **FOR THE PRIVACY OFFICER**
   a) **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:
   b) **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 3015 Facility Security and Access Control.
      iv) The Privacy Officer will document the results of this analysis in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests. This report will be available for public inspection.
   c) **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 E – Minimum Necessary – Workforce, Disclosures and Requests.
   d) **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.

2) **FOR ALL EMPLOYEES**
   a) **Minimum Necessary Requirement**.
      i) **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.
      ii) **Exceptions**. The minimum necessary requirement does NOT apply to:
         (1) Disclosures to or requests by a health care provider for treatment
         (2) 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

(3) Uses of disclosures made pursuant to an Authorization
(4) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations

b) **Routine Requests or Disclosures.** Staff shall be familiar with and follow procedures detailed in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests when making requests for PHI or disclosures.

c) **Procedures for Non-Routine Disclosures or Requests**
   i) **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).
   ii) **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).
   iii) **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:
      (1) 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;
      (2) The request is from another **covered entity**;
      (3) 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

1030 Confidentiality Safeguards (Oral & Written)

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 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, "Records Retention Policy.pdf".
   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) **Destruction of PHI in non-paper formats**. Any written PHI in non-paper formats, such as imprints on carbon films used in fax machines, should be destroyed appropriately.
i) **Clean Desk Policy.** All employees shall clean their desks of PHI whenever leaving their work area for a time, especially at end-of-day.
j) **Confidentiality with Cleaning Personnel**. Cleaning personnel with access to the facility should be placed under a confidentiality agreement.

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.

1040 Speaking with the Family and Friends of an Individual Receiving Services

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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.

1050 Authorizations

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 § 3701.243 – Disclosing of HIV test results or diagnosis
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
42 CFR Part 2 – Confidentiality of records from federally-funded drug and alcohol abuse treatment centers

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.
   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 1060 Verification, after which the information may be released.
4) **Special Situations**. All staff should be aware of certain special situations. Records personnel shall be trained and shall follow legally-required and CCBDD procedures for all special situations, including:
   a) **HIV/AIDS Records**. Ohio Revised Code ORC 3701.243 specifies special procedures for release of HIV/AIDS test results or diagnosis which requires explicit authorization to release these records, plus a disclosure to the recipient regarding the prohibition of re-disclosure.
   b) **Records with names of other Individuals served**. If an Individual's records Include the name of another Individual served by CCBDD (such as an MUI report), the other Individual's name must be redacted prior to the release of the record.
   c) **Psychotherapy Notes**. See Policy 1000 for the definition of Psychotherapy Notes. Psychotherapy Notes may only be released when explicitly authorized. Psychotherapy Notes record releases require their own Authorization, that is, a release of Psychotherapy Notes may not be combine with any other request.
   d) **Records relating to Drug and Alcohol Abuse Treatment**. Any records obtained by CCBDD from a federally-funded drug and/or alcohol abuse treatment facility are subject to 42 CFR Part 2 regulations. 42 CFR Part 2 mandates specific language on the authorization, and further requires that recipients of the records be notified regarding the prohibition of re-disclosure without the Individual's consent.
5) **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.
6) **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.
7) **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.
8) Note that information from other service providers contained in the Individual's record may be released with the Individual's written authorization.

1060 Verification

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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

1) **REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY**
   a) **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:
      i) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI.
      ii) Presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person.
      iii) A written statement on appropriate government letterhead that the person is acting under the government's authority.
      iv) 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.
      v) A written statement of the legal authority under which the information is requested.
      vi) If a written statement would be impracticable, an oral statement of such legal authority.
      vii) 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.
   b) The following issues should be addressed before releasing PHI once a request is received:
      i) Is the requestor who she/he claims to be?
      ii) 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 1090 Disclosures that do Not Require an Authorization.

2) **REQUESTS FROM AN INDIVIDUAL RECEIVING SERVICES, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE**
   a) A properly completed, valid Authorization per the specifications in Policy 1050 Authorizations is sufficient verification of the identity and authority of the person requesting information.
   b) 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:
      i) If the person is known to the staff person, this is sufficient verification of identity.
      ii) 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.
      iii) 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 1040 Speaking with Family and Friends of an Individual Receiving Services for situations where it may be permissible to give information to a family member.

1070 Minors, Personal Representatives and Deceased Individuals

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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)**.**

1080 Duty to Report Violations and Security Incidents

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 3035 Breach Reporting.
4) **Procedure for Privacy Violation.** For Privacy Violations, the Privacy Officer will follow procedures in Policy 3065 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 the following policy:
   - Personnel Policy Section 5.01 Discipline Principles
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.

1090 Disclosures that do not Require an Authorization

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 § 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 "4.20 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.

INDIVIDUAL RIGHTS

1200 Individual's Right to Access Records

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 1070 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) **Redaction of Confidential Information**. Prior to release, Agency staff shall redact any confidential information (such as names of other Individuals served.)
   d) **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.

e) **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) **Explanation and Interpretation of Records.** CCBDD will respond to reasonable requests for explanation and interpretation of the records.
4) **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.
5) **Fees for copying/electronic media**
   a) CCBDD at present has no fees for photocopies, postage or electronic media used to provide records.

1210 Individual's Right to Request Amendment of Records

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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
1) **REQUESTS FOR AMENDMENTS**
   a) **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.
   b) **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.
   c) **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.
   d) **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.
   e) **Denied Request for Amendments**. Otherwise, if the CCBDD believes the existing record is correct as is, it may deny the amendment:
      i) **Written Notice.** If an amendment is denied, the CCBDD will give written notice in plain language which includes the following:
         (1) The basis for the denial;
         (2) The Individual's right to submit a written statement disagreeing with the denial and how the Individual may file such a statement;
         (3) 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
         (4) The Individual's right for a hearing to challenge the information.
      ii) **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.

iii) **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.

iv) **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.

f) **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).

g) **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.

2) **RECORDS HEARINGS**

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

a) **Hearing Procedures**

i) The HIPAA Privacy Officer will arrange the Records Hearing.

ii) The Privacy Officer must schedule the hearing within a reasonable time upon receiving a request.

iii) CCBDD shall give the Individual notice of date, time and place reasonably in advance of the hearing.

iv) 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.

v) 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.

vi) The decision shall be based solely on the evidence presented.

vii) 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.

b) **Results of Hearing**

i) 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.

ii) 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.

iii) 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.

1220 Individual's Right to Receive an Accounting of Disclosures

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 1090 Disclosures that do not Require an Authorization and 1050 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:
      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 that reasonably informs the Individual of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure.
      v) 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.
      vi) 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.

1230 Individual's Right to Request Additional Restrictions

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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.

1240 Individual's Right to Request Confidential Communications

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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.

1250 Individual's Right to Notice of Privacy Practices

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 the 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 are maintained to ensure appropriate distribution of Notice:
   a) All adults at intake 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) For all other Individuals, the Board shall coordinate with the appropriate education authority to ensure that the notice, "A Guide to Parent Rights in Special Education" (formerly "Whose IDEA Is This"), is distributed 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 "Records Retention Policy.pdf".

CONFIDENTIALITY POLICIES FOR SUPERVISORS

1300 Business Associate Contracts

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 § 164.502(e)
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.

1320 Non-intimidation and Non-retaliation

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 "4.20 Protection of Whistleblowers" as appropriate.

1330 HIPAA Assignments and Documentation

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 1250 Individual's Right to Notice of Privacy Practices, and signed acknowledgements that Individuals served have received a copy of the notice.
   c) Restrictions on use or disclosure of PHI agreed to by CCBDD as described in the Policy1230 Individual's Right to Request Additional Restrictions.
   d) Records of disclosures, as required by the Policy 1220 Individual's Right to Receive an Accounting of Disclosures.
   e) Any signed authorization as described in Policy 1050 Authorizations.
   f) All privacy-related complaints received, and their disposition, if any, as described in Policy 1340 Privacy Complaints.
   g) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Policy 1080 Duty to Report Violations and Security Incidents.
   h) Incident Reports and other documentation specified by Policy 3035 Breach Reporting and Policy 3090 Security Incident Response and Reporting.
   i) Records detailed in Policy 3000 Security Management Process, including the formal Security Risk Analysis, records that this was reviewed by all decision makers, and risk management actions taken.
   j) Training records maintained in accordance with Policy 1350 Policy Updating and Staff Training.

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 "current policies". Any previous versions will be renamed with the creation date in the file name, and placed in a computer file folder designated "archived policies".
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 "Records Retention Policy.pdf" for retention periods and destruction procedures.

1340 Privacy Complaints

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 "4.20 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 "4.20 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 1330 HIPAA Assignments and Documentation.

1350 Policy Updating and Staff Training

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

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 1330 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 Personnel Policy Manual Section 3.03.
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 Personnel Policy Manual Section 3.03.
4) **Documentation**. Training records shall be maintained in each employee's personnel file for at least 6 years.

HIPAA SECURITY POLICIES

POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER

3000 Security Management Process

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
CCBDD will appoint a HIPAA Security Officer. The HIPAA Security Officer will orchestrate the Agency's security management process.

AUDIENCE
Executive Management

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(2)

PROCEDURES
1) **The Superintendent will designate a HIPAA Security Officer**. The job responsibilities for this person are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer. Documentation of the designation of the HIPAA Security Officer will be retained with other HIPAA-mandated designations per Policy 1330 HIPAA Assignments and Documentation.
2) **The HIPAA Security Officer will be responsible for security management process**. This will include:
   a) **Security Team**. The HIPAA Security Officer may issue a request to the Superintendent to appoint a Security Team consisting of managers representing the different functional areas and facilities maintained by the Agency. The Security Team's charter would be defined by the Agency, to include assessing risks, recommending and implementing appropriate technical capabilities, drafting and deploying appropriate security policies and procedures, and periodically validating their effectiveness.
   b) **Computer Security Risk Analysis**. A risk analysis will be conducted and updated periodically. The Risk Analysis is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information maintained on systems owned or used by CCBDD. The Computer Security Risk Analysis will be handled as follows:
      i) CCBDD will use the risk analysis methodology detailed in NIST SP 800-30 Revision 1.
      ii) The results of this analysis shall be documented and maintained for 6 years
      iii) The risk analysis shall be updated on an annual basis, or more frequently if appropriate based on technical and environmental variables, major software updates, infrastructure or other technological changes.
      iv) The risk analysis shall be reviewed by the Security Officer, Privacy Officer, Superintendent, and any other person(s) involved in risk management decision making or implementation. CCBDD will maintain written documentation that these persons reviewed this risk analysis, and will maintain that documentation for 6 years.
   c) **Risk Management**. CCBDD shall manage the risks identified in the risk analysis:
      i) CCBDD's Superintendent, in conjunction with the Board of Trustees, shall articulate a risk threshold, that is, a dollar amount of risk that the organization is willing to accept.
      ii) Risks greater than this threshold should be either mitigated, that is the probability should be reduced, or transferred, either through contract or insurance. These decisions may be made by the Superintendent or his/her designee.

      The results of risk management decisions, and corrective action taken, including the timeframe for corrective action, shall be documented. Documentation shall be maintained for 6 years.

d) **Manage IT Infrastructure, Create and Deploy Security Policies**. On an ongoing basis, implement and maintain the IT infrastructure, create Security Policies and Procedures, and deploy them. More specifically, he/she will:
   i) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices.
   ii) Prepare recommendations for the Superintendent, for approval by the Board of Trustees as necessary, including implementation of new and updated policies, acquisition of technical security measures, or physical security measures.
   iii) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
   iv) Train Agency staff regarding compliance.
   v) Monitor Agency compliance with the information security policies, and take action as appropriate based on this monitoring.

e) **Information System Inventory**. The HIPAA Security Officer and/or Security Team shall maintain an inventory of the hardware, software and networking infrastructure.
   i) Content of Inventory:
      (1) Hardware inventory will document all servers, routers and other networking equipment, desktop computers, laptops, smartphones and other portable computing devices, external disk drives, and USB flash drives. Inventory will include physical location, primary user, manufacturer / model / serial number.
      (2) Network infrastructure documentation will include network topology and all other information necessary to recreate the network in the event of a catastrophic event.
      (3) Software inventory will include hardware installed on, Software manufacturer, program name, version number, license/serial number and date.
   ii) Update frequency. This inventory should be updated on an ongoing basis with a physical inventory no less frequent than annually for mobile devices.
   iii) Network Monitoring. (Optional Best Practice.) Network access monitoring may be performed to validate that devices which access the network are included in the inventory. Corrective action should be taken when an unknown device appears.
   iv) Backup copy. A copy of this inventory shall be maintained off-site to ensure availability in the event of a fire or other disaster.

f) **Change Management.** The HIPAA Security Officer shall proceed prudently with any changes to hardware or software.
   i) A full backup of any major software system will be performed prior to any software upgrade or movement of a server, to allow for restoration of a working copy in the event of malfunction. After upgrade, key functionality of system will be promptly verified so that the practice can revert to the previous version if necessary.
   ii) Prior to patching operating system or DBMS software on a server, the application software vendor will be contacted for validation that functionality has been tested and that no compatibility issues have been found. Automatic patching shall not be enabled on servers.
   iii) Interfaces will be monitored upon change of a software application on either end to validate proper functionality.

REFERENCES

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, 2001
NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, 2001
SANS at www.sans.org. See SANS Top 20 Controls, Control #1 for additional information re: Inventory.
Center for Internet Security at www.cisecurity.org

3005 Data Backup

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
The HIPAA Security Officer will ensure that a robust data backup regimen is in place and operational at all times. The HIPAA Security Officer shall personally ensure that the procedures below are consistently maintained.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(7)

PROCEDURES
1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality.
2) **Multiple Backup Generations**. Backups should include as many generations as is practical to store. One backup per day is appropriate.
3) **Backup Software**. Appropriate backup software shall be maintained, with appropriate scripting. These scripts shall be reviewed and adjusted as appropriate whenever hardware or software upgrades are performed to ensure that appropriate data backup is maintained.
4) **Off-site storage**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include an off-site backup, that is, in a separate facility from the one containing the physical hardware.
5) **Backup Documentation**.
   a) A written description of the backup regimen must be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
   b) User documentation, for use by a system administrator, shall be maintained to allow for an alternate person to verify the daily operation of the backup.
6) **Responsibility**. The HIPAA Security Officer shall designate the employee with primary responsibility to personally handle the backup. In the event that he/she is absent from work, an alternate person shall be responsible. All persons responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7) **Backup Log**. A daily written log shall be maintained documenting the date, person, verification that backup was completed successfully, and any comments. Problems should be immediately reported to the HIPAA Security Officer, or if the HIPAA Security Officer is away from the office, to the superintendent.
8) **Backup Media Security**. Backup media shall be maintained in a secure location.
9) **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT**.** On at least a quarterly basis, a trial restore shall be performed from the backup to verify the proper function of the backup process. Based on the results of this test, and any other environmental changes, the Data Backup Policy and Disaster Recovery Plan shall be updated. The results of this process should be documented and maintained for 1 year.
10) **Data Recovery Plan.** The HIPAA Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

3010 Disaster Recovery Plan and Emergency Mode Operation

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Agency personnel shall develop contingency plans to prepare for system failures, and for procedures for maintaining critical Agency operations in the event of system failure.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(7)
45 CFR § 164.312(a)(1)

PROCEDURES
1) **Disaster Recovery Team**. If appropriate, the HIPAA Security Officer shall establish a Disaster Recovery Team to assist in the preparation of contingency plans as well as to execute assigned tasks in the event of a disaster. The HIPAA Security Officer shall direct this team and is responsible for all tasks identified in this policy.
2) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios should include, at a minimum, failure of one or more servers, data corruption of one or more subsystems, and catastrophic loss of the entire facility due to fire or other natural disaster. These scenarios shall be included in the written plan and serve as the basis for the measures outlined below.
3) **Preventative Measures**. The HIPAA Security Officer shall, on an ongoing basis, evaluate the activities that are critical to Agency operations and implement preventative measures to reduce the likelihood of system failure. These would include technical measures such as RAID arrays, backup power supplies, fire suppression systems, raised floors, security systems, database transaction logging and the like.
4) **System and Data Recovery Plan**. The HIPAA Security Officer shall maintain a written system and data recovery plan, and take reasonable steps to mitigate losses, for likely failure scenarios.
    a) The written plan should include:
        i) Computer applications shall be reviewed and assessed as to their criticality for maintaining Agency operations. The results of this assessment shall be documented.
        ii) Development of written documentation of tasks and responsibilities for members of the Disaster Recovery Team in the event of various failure scenarios.
        iii) System configuration documentation, as specified in the policy "HIPAA Security Officer and Security Management Process" to facilitate replacement of vital equipment in the event of a catastrophic loss.
        iv) Complete and current employee information and vital records.
        v) Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster.
    b) Reasonable steps to assure rapid recovery and mitigate losses can include, if appropriate:
        i) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by Agency management.
        ii) Contracts with hot and/or cold system sites if deemed necessary and prudent by Agency management.
        iii) Steps to manage risk, such as insurance policies, as deemed appropriate, for possible losses to mitigate the financial impact of disasters.
5) **Emergency Mode Operations Plan**. The HIPAA Security Officer shall maintain a plan to maintain vital operations in the event of a partial or complete system failure. This should begin with an identification of likely failure scenarios as described above. Elements of this plan may include:
    a) Identification of situations which occur where immediate access to Individual data is necessary, as in certain MUIs involving health emergencies,
    b) Maintenance of Critical Individual Data from electronic in a paper chart, or other plan to protect against loss of access due to technical failure,

c) People assigned to assist Case Managers or other persons with immediate access to this information in the event of an emergency regarding an Individual (accident, medical incident, etc.)
d) Periodic training of staff regarding how to access information in the event of simultaneous computer downtime and Individual emergency,
e) For non-emergency situations, procedures which allow staff to function, to the extent possible, in the event of system downtime.

6) **Plan Testing**. The HIPAA Security Officer shall be responsible for plan testing. He or she shall design the approach to testing and the level of resources which are appropriate to invest in these activities based on the risk analysis.
7) **Off Site Storage of Key Documents**. A copy of the key documents described in this policy shall be maintained off site, in either paper or electronic form, so that they are readily and quickly accessible in the event of catastrophic loss of the facility.

REFERENCES

NIST SP 800-14
NIST SP 800-18
NIST SP 800-26
NIST SP 800-30
NIST SP 800-53

3015 Facility Security and Access Control

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
All employees shall be aware of facility security and access policies to ensure that only authorized personnel have physical access to the facility and its equipment.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(a)(1)

PROCEDURES
1) **Facility Security Planning**. The HIPAA Security Officer shall periodically evaluate physical security vulnerabilities, identify corrective measures, and develop a written facility security plan. The plan should focus especially on security of:
   a) Computer Servers
   b) Telephone and Networking equipment
   c) IT staff offices
   d) Workstation locations

   Attention should be given to areas with public access, whether workstations are protected from public access or viewing, the security of entrances and exits, and normal physical protections (locks on doors, windows, etc.).
2) **Employee Training**. The HIPAA Security Officer shall be responsible for employee training on their duties and responsibilities for facility security as described in the facility security plan.
3) **Maintenance of Physical Security Equipment**. The Director of Operations shall be responsible for maintaining equipment necessary to secure the facility, including locks, alarm systems, doors, security lighting, etc. Records of repairs and modifications shall be maintained.
4) **Unauthorized Persons**. Any staff who sees an unauthorized, unescorted person in the facility, except for those Public Access Areas, shall, in a polite manner, escort the person to a common area. Any suspicious incident shall be reported to the HIPAA Security Officer and/or police.

REFERENCES
NIST SP 800-66

3020 Annual Security Evaluation

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Annually the HIPAA Security Officer shall conduct a technical evaluation of the Agency's security policies and procedures, including a revised risk assessment, and update policies as necessary in response to environmental or operational changes affecting the security of electronic protected health information.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(8)

PROCEDURES
1) **Annual Review of Regulations, Statutes, and Technological Issues to Update Security Policies.** On an annual basis, the HIPAA Security Officer will review any updates to federal HIPAA regulations, other applicable federal and/or state statues, and technological issues and update the organization's security policies as appropriate. This review may be conducted internally, or upon the HIPAA Security Officer's recommendation and approval by the superintendent and/or Board of Trustees, contracted to an outside firm.
2) **Annual Evaluation.** On at least an annual basis, an evaluation of the technical infrastructure and/or the organizations compliance with computer security regulations will be conducted. From year to year, type of evaluation(s) may vary and will be selected by the HIPAA Security Officer. Appropriate evaluations may include
    a) Vulnerability scanning and remediation
        i) a commercial or open-source vulnerability scanning tool is used and/or a service is employed
        ii) Vulnerability scanning is performed both from outside of the network (targeting public facing IP addresses) and from inside the network
        iii) Devices connected to the devices are compared to the IT Asset inventory to identify unknown devices connected to the network
        iv) Missing assets are identified
        v) Vulnerabilities shall be prioritized for remediation

        Remediation shall be performed in a prioritized basis
    b) Penetration tests
    c) Social Engineering exercises/tests
    d) IT Asset audits to identify missing assets
    e) Audits of policies and procedures for compliance with the following standards/regulations
        i) HIPAA
        ii) CARF
        iii) FERPA/IDEA
        iv) State laws
    f) Audits of compliance with policies and procedures, including verification that the processes, procedures and documentation specified in the policies exist, and that the responsible personnel understand the policies

    Evaluations may be done more frequently, if determined by the Security Officer. More frequent evaluations are appropriate upon introduction of new technologies, the emergence of new environmental risks, regulatory changes, change in personnel, or other factors. Evaluations may be targeted to a specific area.
3) **Report and Recommendations.** The HIPAA Security Officer shall submit their report to the Superintendent and/or Board of Trustees, including any recommendations.
4) **Documentation of Review.** The results of the review will be documented, and documentation shall be retained for 6 years.

3025 Audit Control and Activity Review

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
System capabilities for maintaining audit trails of system use shall be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews should be conducted to identify inappropriate activity so that appropriate corrective action is possible.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(b)
45 CFR § 164.308(a)(1)
45 CFR § 164.308(a)(5) Log-in Monitoring

PROCEDURES
1) **System Activity Logs**. Activity logs shall be enabled at the following levels:
   a) **Operating System**: Audit Policy should be set to log logon events, account management events, policy changes, and system events.
   b) **Firewall Hardware and Software**: Logs should be enabled to track inbound and outbound activity, including internet access by person.
   c) **Application Software Logging**: All software which stores data on Individuals served shall have audit trail capabilities. Logs should be enabled in application software such as clinical record software, billing software, or information systems which store information regarding Individuals being served.
2) **Security on Logs**. Appropriate security features and passwords should be used at all levels above to permit log file access only by the HIPAA Security Officer and/or an person designated by him/her.
3) **Quarterly Audit of PHI Access**. A review of system activity will be conducted on at least a quarterly basis. The HIPAA Security Officer shall design an audit strategy to identify probable or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:
   a) Access by persons at unusual hours.
   b) Higher access/usage levels than normal.
   c) Accesses to records of relatives of celebrities, celebrities' children or employees.
   d) Unauthorized changes to security settings.
   e) Web sites viewed by employees to verify that they are work related.
   f) Outside probe attempts and/or accesses via the internet connection.
   g) Other Unusual patterns of activity.
4) **System Activity Review**. In a manner determined by the HIPAA Security Officer, he or she will monitor system activity to detect suspicious or unusual system activity.
5) **Corrective Action.** The HIPAA Security Officer will initiate corrective action, in conjunction with other members of the management staff, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
6) **Purge of Log files**. System Log files which grow large may be purged under the direction of the HIPAA Security Officer.
7) **Annual Policy Review**. Annual attention should be given this policy regarding audit controls, as the threat level varies and the cost of monitoring tools changes.

3030 Malicious Software Protection

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
All company computer systems will be protected by virus and malicious software protection capabilities.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)

PROCEDURES
1) **Multi-Layered Defense Strategy.** The HIPAA Security Officer will ensure that the computer network be protected from malicious software using a multi-layered defense strategy:
   a) Appropriately configured, commercial-grade firewall (per Policy 3060 Technical Safeguards)
   b) Centrally managed and updated anti-virus software
   c) DNS filtering service to limit connections to malicious sites, phishing attacks, and botnets per Policy 3060 Technical Safeguards
   d) Patching of operating system and application software per Policy 3060 Technical Safeguards
   e) Monitoring system logs per Policy 3020 Audit Control and Activity Log Review
2) **Special procedures** will be used, if appropriate, for any users who routinely access on-line banking accounts.
3) **Annual Review.** Annual review of this policy will be conducted to ensure that the products, services, and configuration, and policies appropriately manage risk for this rapidly evolving threat.

3035 Breach Reporting

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
The Agency will notify Individuals receiving services, the Secretary of HHS and, when appropriate, the news media regarding breaches of protected health information.

AUDIENCE
HIPAA Security Officer, HIPAA Privacy Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164, Subpart D
45 CFR § 164.400, 45 CFR § 164.402, 45 CFR § 164.404, 45 CFR § 164.406, 45 CFR § 164.408, 45 CFR § 164.410, 45 CFR § 164.412, 45 CFR § 164.414

PROCEDURES
1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer shall jointly determine if the incident meets the definition of a breach. If a Security Incident Response Team (Team) has not been assembled, they may assemble a Team at this point. Legal counsel and other outside expert advice shall be obtained, if appropriate, for additional guidance on the Team. An investigation should be launched, with attention to preserving evidence. The Team shall follow the following 3 step procedure:
   a) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   b) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   c) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.
      The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1330 HIPAA Assignments and Documentation. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred, and this process may stop. Otherwise, a breach has occurred, and the Team should proceed with the steps that follow in the remainder of this policy.
2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   a) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the Agency may use telephone, email or other means to immediately notify Individuals of the breach.
      ii) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         (1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
         (2) A description of the types of unsecured protected health information that were involved in the breach;

(3) Any steps that Individuals should take to protect themselves from potential harm resulting from the breach;
(4) A brief description of what the Agency is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and
(5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site or postal address.

iii) Send the primary breach notification to:
(1) Individuals affected by the breach by first-class mail at their last known address, or by e-mail if agreed in advance by the Individual for this type of notice, or
(2) Parent, guardian, or HIPAA Personal Representative of the Individual in the event the Individual is a minor and/or not competent to make decisions, or
(3) next of kin or personal representative of the Individual in the event that the Individual is deceased and the next of kin name and address are available.

iv) Track returned mail and provide a substitute notice to Individuals who did not receive the primary notification (no further effort is necessary for unreachable next-of kin):
(1) In the event that fewer than 10 Individuals are reachable by first class mail, the HIPAA Privacy Officer shall research updated address and/or phone number and make best efforts to inform those Individuals by either phone or mail.
(2) In the event that 10 or more Individuals are not reachable by first class mail,
(a) A toll-free phone number shall be established, and staffed with operators, for at least 90 days
(b) a notice shall be conspicuously placed on the Agency's web site home page with details of the above details on the breach plus the phone number

b) Notify the news media if more 500 Individual records are involved in the breach
i) Under direction of the Agency superintendent, a press release shall be prepared detailing the information in section 3(a)(ii) above, and other relevant information.
ii) Upon approval of the Superintendent, the press release shall be issued without unreasonable delay (and in no case later than 60 days after discovery of the breach) to the major print, broadcast and online media serving the county.

c) Notify the Secretary of the Department of HHS regarding the breach
i) In the event that the breach involves 500 or more Individuals, notice to the Secretary should be provided at the same time as the Individual notification in the manner detailed on the HHS Web site.
ii) For breaches involving fewer than 500 Individuals, a log including at a minimum the information in 3(a)(ii) above, and other relevant information, should be maintained. At the end of the calendar year, the contents of the annual log should be provided to the secretary in the manner detailed on the HHS Web site.

4) **Breaches by Business Associates**. Breaches by business associates are handled in the same manner. Business associates are obligated to cooperate in providing necessary information; the Agency is responsible for issuing the notice detailed in this policy.

5) **Law Enforcement Delay**. The notices to Individuals and the media may be delayed if a request is received by a law enforcement official:
a) If written notice is received from a law enforcement official which specifies the time period of delay, the Agency shall comply with that request.
b) If the request is made orally, the notification shall be delayed but not longer than 30 days from the date of the oral request.

6) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that the Agency should have become aware if it exercised reasonable diligence.

3040 Security Awareness Program

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
The HIPAA Security Officer will conduct an ongoing security awareness program to train and refresh staff on computer security behaviors and the Agency's security policies. Priority topics shall include recognizing and avoiding malicious software, avoiding "social engineering" ploys, using passwords effectively, and adhering to workstation use policies.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)

PROCEDURES
1) **Security Training Program for New Employees.** The HIPAA Security Officer shall develop, and maintain, a security training program for new employees. This should include, at a minimum:
   a) Password policies
   b) Recognizing and avoiding malicious software
   c) Understanding e-mail attachments
   d) Safe web browsing practices
   e) Dangers of downloading files from the internet
   f) Understanding of "Social Engineering" and how to recognize such ploys
   g) Knowledge of Workstation Use Policies
   h) Consequences for non-compliance
   i) Security Incident Reporting Procedures

   Other appropriate topics may be included at the discretion of the HIPAA Security Officer. The program may be conducted one-on-one, via e-learning system, or other media as determined by the HIPAA Security Officer.
2) **Upon initial implementation**, the Security Training program will be provided to all staff. Subsequently, all new staff should receive the training.
3) **Periodic security awareness training will offered to all employees**. The HIPAA Security Officer shall develop an annual plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; evaluation and measurement techniques; and the frequency of training. Possible topics would include:
   a) Reinforcement of topics for the Security Training Program and Security Policies
   b) Advisories regarding current threats
   c) Issues with new technologies such as smartphone/tablet security

   A variety of media and avenues should be explored such as sign-in banners, security reminder cards for posting at workstations, articles in employee newsletters, posting on bulletin boards, etc. At a minimum, Computer Security Awareness will be included annually as detailed in CCBDD Personnel Policy 3.03.

3050 Device and Media Disposal and Re-Use

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Electronic storage media and devices shall be cleaned of protected health information and other confidential information prior to disposal and/or re-use.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(d)(1)

PROCEDURES
1) **Media Disposal Handled by HIPAA Security Officer**. As specified in Policy 3080 Computer Usage, Agency employees are prohibited from storing Protected Health Information of the Agency's on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.
2) **Technical Guidance**. In accordance with instructions from the Secretary of HHS, technical guidance regarding media disposal should be obtained from NIST SP 800-88 *Guidelines for Media Sanitization*. The Agency requires that at a minimum, data from electronic media should be "cleared", as defined in the referenced NIST documentation.
3) **Media Disposal and Re-use**. Procedures vary based on type of storage media:
    a) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
    b) **Hard Drives and floppy disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
    c) **Other Media**. See NIST SP 800-88 for disposal/recycling methods for other media.
4) **Records.** Records of Media disposal should be maintained for 6 years. The following records should be maintained:
    a) Item Description
    b) Make/Model
    c) Serial number(s) / Property Number(s)
    d) Backup Made of Information (Yes/No)
    e) If Yes, location of backup
    f) Item Disposition (Clear/Purge/Destroy)
        i) Date Conducted
        ii) Conducted by
        iii) Phone #
        iv) Validated By
        v) Phone #
    g) Sanitization Method used
    h) Final disposition of media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer /Other)

3060 Technical Safeguards

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Technical Safeguards will be employed as necessary to maintain the integrity of data, and to ensure the security of data during transmission.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(c)
45 CFR § 164.312(d)
45 CFR § 164.312(e)

PROCEDURES
1) **Firewalls.** Commercial-grade hardware and/or software firewalls shall be employed to protect against network intrusions and to manage/monitor outbound traffic. Workstation-based software firewalls (e.g. Windows Firewall) should be used on laptop computers since they may be connected to an outside network.
2) **Secure Configurations.** Workstations and servers will be installed with a standard configuration that meets the following specifications:
   a) A standard list of software to be installed will be maintained. Only vendor-supported versions of software should be used. Additional software may be installed for specific users based on unique requirements.
   b) Windows, Microsoft Office, and Internet Explorer should be securely configured. Microsoft's security configuration guides shall be used, using the middle level of security, with modifications as necessary to allow for functionality.
   c) Microsoft Security Compliance Manager and Active Directory will be used to maintain and enforce security configurations.
3) **Operating System and Application Software Patching**. Operating Systems, application software and hypervisors, if used, shall be patched regularly on both servers and workstations. Auto-update functionally may be employed and update servers. Centralized patch management software such as Microsoft WSUS and/or third party-software may be utilized.
4) **Virtualization Software and Environment**. If virtualization technology is employed, the virtualization-enabling software, aka "hypervisors", shall be secured as follows:
   a) Unneeded capabilities shall be disabled to reduce potential attack vectors.
   b) A strong password (minimum of 8 characters, 1 upper case, 1 lower case, 1 digit) shall be used for the management console.
   c) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's.
   d) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations.
   e) Use separate logon credentials for each virtual server.
5) **DNS Filtering** shall be employed to reduce access to unsafe websites and to reduce phishing attacks, using OpenDNS or an alternative service.
6) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   a) The beacon shall be enabled.
   b) The SSID should be changed from the default.
   c) WPA/WPA2 should be enabled.
   d) WPS should be disabled.
   These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
7) **E-mail**. For transmission of PHI, secure, encrypted e-mail should be employed.

8) **Encryption of desktop, mobile devices and portable media**. When encryption of end-user devices is determined appropriate based on risk analysis, the Agency shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, the Agency should:
   a) consider solutions that use existing system features (such as operating system features) and infrastructure;
   b) use centralized management for all deployments of storage encryption except for standalone deployments; and very small-scale deployments;
   c) select appropriate user authenticators for storage encryption solutions; and
   d) implement measures that support and complement storage encryption implementations for end user devices.
9) **Transmission Security**. For data in motion, the HIPAA Security Officer implement solutions consistent with the Secretary of HHS's guidance on securing PHI. Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in:
   a) NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*.
   b) NIST 800-77, *Guide to IPsec VPNs*.
   c) NIST 800-113, *Guide to SSL VPNs*.
   d) Other FIPS 140-2 validated processes.
10) **Appropriate Audit Controls in Agency-Used Software**. Software used by Agency should be evaluated for the appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements should be made as appropriate. Appropriate audit controls should be a criterion for continued use of and/or procurement of any new operating or application software.
11) **Software utilizing Electronic Signatures**. The HIPAA Security Officer will review and approve any software that offers electronic signature capability prior to implementation at the Agency. The HIPAA Security Officer shall be responsible for implementation and ongoing monitoring/auditing of the software as specified in Policy 3070 Electronic Signatures.
12) **Automatic Log Off**. Appropriate measures shall be taken, based on the technology available, to enable the automatic log-off provisions as determined by the risk assessment. See also Policy 3080 Computer Usage and Policy 3075 Employee System Access and Termination Procedures.
13) **Integrity Checks**. The HIPAA Security Officer shall attend to integrity of electronic data:
   a) Periodic DBMS maintenance as recommended by the software vendor shall be performed.
   b) Message digest integrity reports shall be reviewed with corrective action taken as necessary.
   c) Monitoring any electronic interfaces, such as lab interfaces, to verify proper functionality.

3062 Technical Controls for Mobile Devices

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Employees who meet eligibility criteria may be provided with agency-owned smartphones or tablets, or use their personally-owned smartphones and tablets (BYOD) to access the organization's IT resources.

AUDIENCE
HIPAA Security Officer
IT Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(b) Standard: Audit Controls
45 CFR § 164.312(c)(1) Standard: Integrity
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation Specifications
45 CFR § 164.312(a)(2)(iv) Encryption and decryption
45 CFR § 164.308(a)(5)(ii)(D) Password Management
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software

DEFINITIONS
BYOD means "Bring Your Own Device" which is an industry term describing an organization's practice of permitting employees to use a personally-owned device to connect with the organization's computer network.

PROCEDURES
FOR THE HIPAA SECURITY OFFICER/IT DEPARTMENT
1) **Technical Controls.** The organization shall implement appropriate technical controls
   a) Use of an appropriate mobile device management system to maintain inventory of devices, enforce security configurations, provide remote wipe/lock capability, geo-location, monitor policy compliance and other appropriate controls.
   b) The use of appropriate security controls including secure communications, strong authentication, audit logging, control of third-party software, anti-malware, segregation of corporate from personal data, restricting the use of camera/microphone, restricting automatic backups of the organization's data to employee-controlled backup services and other controls and backup of any corporate data.
2) **Eligibility Criteria.** The Superintendent may establish eligibility criteria regarding who may use agency-provided or BYOD mobile devices.
3) **Resources Provided.** Smartphone access to agency resources shall be limited to agency email systems; PCs shall be configured for access to agency resources in the same manner as other PC workstations at the agency.
4) **Enrollment Procedures.** Agency may utilize a Mobile Device Management (MDM) system. If the Agency uses a MDM, the Agency will create an Operating Procedure for enrolling employee device with mobile device management system. This Operating Procedure should address the processes for both agency-owned devices and BYOD devices. The MDM will enforce a secure configuration of the employee phone/tablet, and enable remote wiping of the device:
   - Encryption (required by HIPAA)
   - Strong password (required by HIPAA)
   - Anti-malware software (required by HIPAA)
   - Require strong authentication, use password controls
   - Disable and/or limit Bluetooth communications

3065 Mitigation

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
In the event of an inappropriate use or disclosure of an Individual's PHI, the CCBDD will take reasonable steps to mitigate the harmful effects of the disclosure.

AUDIENCE
Privacy Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.530(f) – Mitigation

PROCEDURES
1) **Mitigating Harmful Effects of Privacy Violation.** In the event of a HIPAA Privacy rule violation, the Privacy Officer, in conjunction with other members of the management staff as he/she deems appropriate, shall take action to mitigate the harmful effects of the Privacy Violation, if this is reasonable and possible. The mitigation action should correspond to the nature of the violation. For example, if social security numbers are breached, it may be appropriate to purchase identity theft protection for 1 year.

3070 Electronic Signatures

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Electronic signatures may be utilized at CCBDD by both employees and providers. Electronic signatures are legally binding as a means to identify the author and to confirm that the contents are what the author intended.

AUDIENCE
Employees Using Electronic Signatures; Managers

AUTHORITY
ORC § 1306 Ohio Uniform Electronic Transactions Act
ORC § 304 Electronic Records and Signatures for Counties
ORC § 9.01 Official Records – Preserving and Maintaining
ORC § 117.111 State Audits shall review method, accuracy and effectiveness of electronic signature security procedures

DEFINITIONS
1) Electronic Signature, as defined by the Ohio Revised Code, means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted b y a person with the intent to sign the record.
2) Electronic facsimile. A computer image, such as one maintained in an electronic document imaging system, of a conventionally signed document is not an electronic signature. Rather, the electronic facsimile is legally equivalent to the original, traditionally signed document.

PROCEDURES
1) **Security**
   a) **Confidentiality statement**. Anyone authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature/ logon password, that the electronic signature will be legally binding and that passwords will not be shared and will be kept confidential.
   b) **Passwords**. All users will have their own user ID and password. Passwords must conform to complexity guidelines detailed in Policy 3080 Computer Usage.
   c) **Personal Identification Numbers (PIN)/ Secondary Password**s**.** PIN numbers and/or secondary passwords may be assigned when possible for use with electronic signatures to allow for another level of security (this is optional and county specific). PIN numbers or secondary passwords are not viewable on any screen.
   d) Vendors, outside agency or providers who have access to using an application requiring an electronic signature based upon the user's ID and password as described in this policy, shall use additional controls to ensure the security and integrity of each user's electronic signature:
      i) Follow loss management procedures to electronically de-authorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information and use suitable, rigorous controls to issue temporary or permanent replacements;
      ii) Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
      iii) Test or use only tested devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.
2) **Creating, Maintaining an Electronic Signature**
   a) Electronic signatures can be used wherever handwritten signatures are used except where stated by a specific law or rule.
   b) All who use a system that uses electronic signatures are required to review their entries.
   c) Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of

addendum to the original entry. The addendum should also be signed electronically and date/time stamped by the computer software.

d) System specific standards and procedures for use may vary by system and it will be required that the Agency must establish and maintain system specific procedures for any system which also satisfies other current policies.

3) **Auditing Electronic Signature Procedures**
The computer software and anyone using the software system must use a secure, computer-generated, time-stamped audit trail that records independently the date and time of user entries, including actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Audit trail documentation shall be retained for a period at least as long as that required for the record and shall be made available as needed upon request. Any misuse or disregard of electronic signature policy will be reviewed and acted upon by the Superintendent or designee.

4) **Review and Approval Prior to Using Electronic Signatures**
The HIPAA Security Officer shall review the software utilized for electronic signatures, and other procedures utilized, for compliance with this policy prior to permitting the use of electronic signatures. This review shall be conducted for each transaction to be electronically signed.

SECURITY POLICIES FOR HR STAFF & SUPERVISORS

3075 Employee System Access and Termination Procedures

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
System access will be granted to employees in a manner consistent with the HIPAA Privacy laws and other state regulations, including specific policies for access control, granting access to new staff and staff with assignment changes, handling staff terminations, password selection, maintenance and use, and access to the system in the event of an emergency.

AUDIENCE
Human Resource Department, Supervisors, HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(3)
45 CFR § 164.308(a)(4)
45 CFR § 164.312(a)(1)
45 CFR § 164.314(d)
45 CFR § 164.308(a)(5) Password Management

PROCEDURES
1) **AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS**
Audience: HIPAA Security Officer, Privacy Officer

a) **Minimum Necessary Analysis.** The HIPAA Security Officer shall coordinate with the Privacy Officer to maintain and document a current "minimum necessary" analysis, per Policy 1020 Minimum Necessary Policy which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to.
b) **Access Profiles.** The HIPAA Security Officer shall utilize the security capabilities of the various network and application software systems at the Agency and develop role-based "Access Profiles" for these different job descriptions. Vendors will be contacted for any enhancements necessary for appropriate implementation of these access profiles.
c) **Granting Access to Information Systems**. The authority to grant access to information systems rests with Superintendent and is delegated to the hiring manager. Implicit in a hiring decision is the provision of access to the information systems necessary for the job, as determined above based on the minimum necessary analysis and the Access Profiles.
d) **Granting Access Beyond the Standard Access Profile**. In certain situations, such as when employees are assigned special projects, information access may be required beyond what the job description would dictate. In these cases, the HIPAA Security Officer, after any necessary consultation with the management staff at the Agency, shall have the authority to grant access to information systems which go beyond the standard Access Profiles described above. Access should be terminated when the need for access is completed.
e) **Inventory of Employees with Access to PHI.** The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
f) **Annual Audit of Access Controls.** On an annual basis, the HIPAA Security Officer shall audit the access controls to verify that the above policies have been implemented properly and consistently. Such an audit could include verification that recently terminated employees no longer have access, a review of access for employees with job changes in the previous year, and a random sampling of other employee access authorization. Based on the results of this audit, the HIPAA Security Officer shall adjust policies and/or staff training as appropriate.

2) **SYSTEM AND FACILITY ACCESS FOR NEW HIRES**

Audience: Supervisors, Human Resource Department

a) **Requests for Access to Information Systems.** Supervisors and/or the human resources department shall direct requests for access to information systems to the HIPAA Security Officer or his/her designee. The HIPAA Security Officer shall verify with the human resources department in the event of any question regarding the accuracy of the job assignment.

b) **Assigning User ID and Password.** The HIPAA Security Officer will assign new hires requiring computer access a unique network User ID and password, and/or User IDs and passwords for other application systems. Security settings appropriate for the person will be assigned in accordance with this policy, as described above.

c) **Communicating User ID and Password.** The HIPAA Security Officer shall communicate the User IDs and passwords in a manner which does not compromise security by revealing the passwords to another person.

d) **Documentation of System Access Rights**. As described above, the HIPAA Security Officer will maintain documentation of system access rights.

e) **User Data Area.** The HIPAA Security Officer will configure a User Data Area on the Server to provide data storage space for the employee. All data is to be stored on the server and not on workstations.

f) **Security Awareness Training.** Employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Policy 3040 Security Awareness Program. In addition, new employees should receive a written copy of the Policy 3080 Computer Usage, and they will sign written acknowledgement that they understand and will adhere to all policies. This will be maintained in the employee personnel file.

3) **PASSWORDS and PASSWORD MANAGEMENT**

Audience: HIPAA Security Officer

a) **Password Complexity**. Network policies shall be established to enforce password complexity as follows:

i) Passwords should be at least 8 characters long and should include upper case letters, lower case letters and numbers. Passwords longer than 8 characters are recommended, as are "passphrases" (a passphrase is a sequence of 3 or more words). The password should not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.

b) **Lockout**. The system shall lock accounts after 5 unsuccessful attempts.

c) **Password Reuse**. The system shall maintain the previous 5 passwords and prohibit re-use of any of these recent passwords.

4) **EMPLOYEE JOB CHANGES**

Audience: Human Resources Department, HIPAA Security Officer

a) The Human Resource Department shall notify the HIPAA Security Officer of all job changes so that adjustments to system access can be made if necessary.

5) **EMPLOYEE TERMINATION**

Audience: Supervisors, Human Resource Department, HIPAA Security Officer

a) **Change Employee Password, Disable User ID and Eliminate Access to Share Cloud Systems.** On the last day of employment, employee passwords to the network and Application Software will be changed and/or their User IDs will be disabled. Account access to all shared cloud systems will be adjusted or terminated.

b) **Documentation.** The HIPAA Security Officer shall document the disabling of system access.

c) **Security Precautions for Involuntary Terminations.** For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the head of human resources who shall coordinate with the Information Security Manager so that appropriate precautions will be taken to ensure the integrity and security of confidential Agency information. This could include such measures as:

i) Physically escorting the person off the premises after notifying him/her of the termination.

ii) Disabling system access and access to all shared cloud systems as specified above on a timely basis.

iii) Requiring all staff in the former employee's workgroup to change passwords.

iv) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the person and perceived threat.

6) **EMERGENCY SYSTEM ACCESS**

Audience: Supervisors, HIPAA Security Officer

a) In the event of an emergency, such as a MUI in which immediate access to PHI is required, a staff member who does not have appropriate system permission but requires access shall contact the HIPAA Security Officer (or another staff person in that department) who will provide the necessary access on an expedited basis.

HIPAA ADMINISTRATIVE REQUIREMENTS

SECURITY POLICIES FOR ALL STAFF

3080 Computer Usage

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Each staff member is responsible for understanding and following the policies regarding workstation use and security.

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(b) Workstation Use
45 CFR § 164.310(c) Workstation Security
45 CFR § 164.308(a)(5) Log in Monitoring

PROCEDURES

1) **WORKSTATION USE**
   a) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the Individuals served: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related.
   b) **Personal Use of Computer Workstation, Including Internet Use**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use. In general, "limited use" means:
      i) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
      ii) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.
      iii) Workstations must never be used for any activity that would be embarrassing to the Agency if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
         (1) downloading or viewing pornographic, racist, profane or otherwise objectionable material
         (2) conducting conversations of a sexual nature of relating to an illicit affair
         (3) relating to any illegal activity
         (4) political activity
         (5) operating a business

         If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.
      iv) Personal use of Social Media, such as Facebook, Twitter, LinkedIn and others is detailed separately.
      v) Employees are prohibited from checking social media and their personal email except during their own time.
      vi) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the Agency.

      For any clarifications of what "Limited use" employees should contact their supervisors.
   c) **E-Mail Use**. Employees with Agency e-mail accounts should check e-mail daily. Agency E-mail accounts in general are to be used for Agency purposes only. Personal email addresses must never be used for agency communications. E-mail should be written in a professional manner and should be courteous and

respectful. Other policies when using e-mail:

i) Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and must not be used to send Protected Health Information unless it is appropriately encrypted.

ii) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in CCBDD's Records Retention Policy.

iii) For personal matters, employees must use a personal account such as Gmail or Yahoo mail, on a personally-owned device

(1) In the event that any Agency e-mail is received on a personal account, the employee must forward the email to the employee's Agency account so that it is entered into the public record.

(2) In the event that a personal email is received on an Agency account, redirect the discussion to a personal email account.

d) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to any unauthorized cloud service or removable media, such as Flash drives, CDs, DVD or portable hard drives, any Agency confidential information or Protected Health Information on Agency computer system, except when specifically authorized by the HIPAA Security Officer for Agency purposes.

e) **All Usage is Logged**. THE AGENCY RESERVES THE RIGHT TO MONITOR ALL USAGE OF AGENCY WORKSTATIONS THROUGH THE LOGGING AND STORAGE OF ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY, INCLUDING ANY PERSONAL USE OF AGENCY COMPUTERS. All logs of employee activity are property of the Agency.

f) **Data Storage on Network Only**. All data must be stored on the network, not on a workstation hard drive. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate User Directory on the server. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions on how to access their User Directory on the server. DATA STORED ON WORKSTATION HARD DRIVES IS NOT BACKED UP, AND MIGHT BE DELETED WITHOUT NOTICE. ALL DATA STORED ON THE NETWORK IS BACKED UP!

g) **Duplication of copyrighted material prohibited**. No employee may duplicate copyrighted software or other media using Agency equipment.

h) **Agency approved hardware only**. Only Agency-approved and Agency-installed hardware may be utilized. No wireless networking equipment, smartphones, video cameras, or other hardware or software may be installed or used without permission of the systems department.

i) **Electronic signatures**. Employees using software that includes Agency-approved electronic signature capabilities shall follow all procedures specified in Policy 3070 Electronic Signatures.

2) **WORKSTATION SECURITY**

a) Except with specific approval of the HIPAA Security Officer, workstations must not be setup in a public access area.

b) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.

c) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.

d) Employees should logoff or lock their screen when leaving their workstation area for a period of time.

e) Workstations should be configured with automatic logoff capability so that they will become inaccessible after 20 minutes of system inactivity. Employees must not install any software on their computer without authorization from the HIPAA Security Officer, and must not alter or reconfigure network settings, printers, logging software, audit controls, or security settings without permission of the systems staff.

f) All Agency servers must be secured with a strong password (see "User IDs and Passwords" below) and set to automatically lock out user access after a maximum of three (3) minutes of inactivity.

3) **USER IDs and PASSWORDS**

a) Each employee is assigned a unique User ID and Password. Employees must only use their User ID to access Agency systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution.

Consequently, passwords should be kept secure and confidential and not shared with anyone else. If an employee reveals a password, or if becomes known to someone else, that employee must change the password.

b) Passwords should be at least 8 characters long and should include upper case letters, lower case letters and numbers. Passwords longer than 8 characters are recommended, as are "passphrases" (a passphrase is a sequence of 3 or more words). The password should not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.
c) In general, passwords should be memorized and not written. Any written reminder should not be maintained near the workstation.
d) Passwords should be changed only if there is evidence or suspicion of compromise.
e) Two-factor authorization and/or Single Sign-On technology should be used, if available.
f) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

4) **EMERGENCY SYSTEM ACCESS**

a) In the event of an emergency where immediate access to system information is required but not immediately possible, employees should contact the HIPAA Security Officer, who has contingency plans to allow access to vital data in a wide variety of scenarios (system down, MUIs, Individual emergencies which mandate system access by personnel who otherwise are not permitted access.)

3082 Social Media Use

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Social media has become a significant communication medium in our world. Agency guidelines for using these sites and applications require that confidentiality and privacy of Individuals being served is maintained.

AUDIENCE
All Staff

DEFINITIONS
Social Media – means websites or applications that enable linking with other people, sharing information, and communicating. Popular examples include Facebook, Twitter, Instagram, Snapchat, LinkedIn, and others.

PROCEDURES
1) **Agency-Sponsored Use**.
   a) The Superintendent may approve the establishment of one or more Agency-sponsored social media pages or accounts.
   b) Prior to placing an image or other personally identifiable information on the Agency website or social media, both a properly completed HIPAA authorization and a media release shall be completed and retained by the agency.
      i) If an Individual discloses PHI on an Agency-sponsored social media page, the Agency must not respond to or affirm the posting in any way. This includes, but is not limited to, replying or "liking" the posting because doing so is an affirmation by the Agency that an Individual is enrolled with the Agency. For example, the agency must not "like" a favorable review posted on the Agency's social media page.
   c) If an Individual or Individual's guardian asks a question or makes a request, either by way of a private message or visible post, to an agency-sponsored page, the agency must not respond through social media. Instead, call, secure email, or mail the Individual. If possible, delete the message or post.
   d) The Superintendent may issue additional guidelines for Agency-sponsored use of social media.
2) **Personal Use of Social Media by Employees**.
   a) **Employee Use During Work Hours**. During work hours, employees are expected to focus on work-related activities. Consequently, in general, they are expected not to open any social media to avoid distraction and/or loss of employee productivity.
   b) **Employee Use Outside of Work Hours**. Any statement or image on social media has the potential to become a public communication, so employees of the Agency must follow the following guidelines:
      i) **Sharing of work-related activities**. Employees should limit the sharing of any Agency-related information to information that they would deem acceptable to be made public, for example, on the front page of a major newspaper.
         (1) Examples of information that are appropriate to share on social media include:
            (a) The employee's excitement and satisfaction with the work and mission of the Agency.
            (b) Details of an upcoming public event sponsored by the Agency, such as a local "Special Olympics" day.
            (c) The name of a friend who is a co-worker at the Agency.
         (2) Examples of information that are inappropriate to share on social media include:
            (a) The name of an Individual receiving services from the Agency, unless in compliance with both an authorization form and a media release form.
            (b) Any Protected Health Information, or PHI (which includes facial images or videos of Individuals being served). This includes any information that could be used to identify someone as an enrolled Individual at the Agency.

         Employees are further encouraged to portray themselves in a professional manner on any social media.
      ii) **Friending/Connecting/Linking**. In general, employees should not "friend", "link", "follow", or otherwise connect to any Individual, including any parent/guardian of an Individual, being served by

CCBDD on any social media. The Agency expects employees to maintain an acceptable professional boundary with Individuals being served. In the rare instances where any employee does friend/connect/link with an Individual served or a family member of an Individual served, any communications via social media must be of strictly a personal nature and not related to agency business.

iii) **Messaging**. Employees must not use social media for Agency-related communications regarding an individual served. This is prohibited since the Agency does not have a Business Associate agreement with any social media platform. Employees are reminded that all Agency-related communications are subject to public records disclosure.

3) **Social Media and Workplace Harassment.** Harassing communications about coworkers on social media can constitute workplace harassment, even if done outside of the office and/or outside work hours. If you feel that you are the target of workplace harassment, report according to the anti-harassment policy.

3085 Portable Computing Devices

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Employees who meet eligibility criteria may either be issued agency-owned smartphones and tablets, or use their personally-owned smartphones and tablets to access the organization's IT resources. Employees who are permitted to use either an employee-owned device or an agency-provided device must follow all guidelines in this policy.

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(b) Standard: Audit Controls
45 CFR § 164.312(c)(1) Standard: Integrity
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation Specifications
45 CFR § 164.312(a)(2)(iv) Encryption and decryption
45 CFR § 164.308(a)(5)(ii)(D) Password Management
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software

PROCEDURES
1) **EMPLOYEE-OWNED MOBILE DEVICES**
   a) **Agreement**. Employees must follow the organization's procedures for enrollment of their mobile device, including signing the Employee-Owned Mobile Device Agreement.
   b) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.
   c) **Personal Use of Phone/Data Backup**. The employee agrees to accept responsibility to back up personal applications and data.
   d) **Text Messaging**. Any text messaging performed from an employee-owned device must be done in accordance with the requirements of this policy. Text messaging using a CCBDD-approved text messaging app is permitted and is the preferred method for any text messaging. The use of standard text messaging with individuals served and/or their parents is discouraged, but not prohibited, for "transient" messages regarding meeting dates and times. Medical, behavioral, diagnosis and similar PHI must not be transmitted with standard text messaging. If unsolicited PHI is received via text by a staff member, any response should be via an approved method such as phone call, secure email, or CCBDD-approved text messaging app.
   e) **Upload of Data**. Any organization-related data created on the mobile device must be uploaded to the organization's network on at least a daily basis.
   f) **Audit**. Random audits to ensure compliance with this policy will be conducted by the Information Technologies Department. Employees must surrender the device for audit. Employees failing to comply with this policy may lose access to the CCBDD network resources through a mobile device.
   g) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Policy 3090 Security Incident Response and Reporting.
   h) **Permission Granted for Remote Lock/Wipe**. Employee grants the IT Department permission to perform a remote lock, remote wipe and/or geo-location of a device. Employee understands and accepts that the IT Department may perform a remote lock or remote wipe if employee's supervisor makes a written request to the Human Resources Department.
   i) **Use While Driving**. Any use of Agency-approved, personally-owned mobile devices while driving must be done so in accordance with the laws of the jurisdiction in which you are physically present.
   j) **Use of Device by Other People.** Employees using personal devices under this policy are responsible for controlling and/or managing the access and/or use of their device by other people including family members and friends. Employees will be held accountable for any actions performed by others who the

employee permits to use the device.

k) **Replacing a Device**. Prior to replacing/upgrading a device, employees must first remove all of the organization's data prior to returning/selling/disposing of their current device. [Enter any organization-specific procedure here.]

l) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.

m) **Discovery and other Legal Processes**. In case of legal action, personal devices used for agency business are subject to e-discovery. Users are responsible for bringing or sending the mobile device to the IT Department and giving the necessary device access codes when notified that the device is needed for e-discovery purposes.

n) **Termination and/or Suspension from Employment.** Upon termination of employment, employee agrees to provide the device to the IT department who will remove all organization data and disable access to the organization's IT resources. At the discretion of the organization, employees who are placed on administrative leave will have access suspended until their return to work.

2) **AGENCY-PROVIDED MOBILE DEVICES**

a) **Eligibility Criteria and Signed Agreement**. Management will evaluate, on an individual basis, the eligibility of employees to use agency-owned mobile devices. Employees who wish to use an agency-owned mobile device must sign the Agency-Owned Mobile Device Agreement.

b) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.

c) **Text Messaging**. Any text messaging performed from an agency-owned device must be done in accordance with the requirements of this policy. Text messaging using a CCBDD-approved text messaging app is permitted and is the preferred method for any text messaging. The use of standard text messaging with individuals served and/or their parents is discouraged, but not prohibited, for "transient" messages regarding meeting dates and times. Medical, behavioral, diagnosis and similar PHI must not be transmitted with standard text messaging. If unsolicited PHI is received via text by a staff member, any response should be via an approved method such as phone call, secure email, or CCBDD-approved text messaging app.

d) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Policy 3090 Security Incident Response and Reporting.

e) **Proper Use.** Agency-owned mobile devices must generally be used for agency-related purposes. *Minimum* personal use is permitted, such as checking weather or making a brief personal call.

f) **Use While Driving**. Any use of Agency-owned mobile devices while driving must be done so in accordance with the laws of the jurisdiction in which you are physically present.

g) **Use of Device by Other People Not Permitted.** Employees using agency-owned mobile devices under this policy must not allow anyone to use agency-owned mobile devices who is not permitted to use these devices under this policy.

h) **Agency-Owned Mobile Devices May Not Be Sold, Transferred, Disposed of, Recycled or Damaged.** Employees must not sell, transfer, dispose of, recycle, or intentionally or recklessly damage agency-owned mobile devices.

i) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.

j) **Termination and/or Suspension from Employment.** Upon termination of employment or upon administrative leave, employee agrees to return the device to the IT department.

3087 Employee Work at Home

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
Employees who are eligible to work at home must follow these procedures to ensure data security.

AUDIENCE
All Staff
HIPAA Security Officer and Technical Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation specifications

PROCEDURES
1) **Eligibility to Work at Home.** Agency management will evaluate, on an individual basis, the eligibility of employees to work at home.
2) **No Agency Data on Home Computer/Laptop.** Employees working at home and using their home computers/laptops for work purposes are prohibited from storing agency data on their home computers/laptops.
3) **Unauthorized Cloud Storage Prohibited.** Employees are prohibited from storing agency data on any unauthorized cloud storage service.
4) **VPN Required for Network Access.** Except as permitted by Policy 3085 Portable Computing Devices, Employees must use agency-supplied Virtual Private Network (VPN) to access the agency network. The use of third-party services from remote access is prohibited.
5) **Agency Webmail.** Employees are permitted to access, from home, agency email through web-based email (webmail).
6) **Computers and Laptops Must be Kept Up-to-Date.** Employees working from home and using a personally-owned PC must ensure that the PC is routinely patched and has functioning anti-malware installed and operating.
7) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required by this policy.

3090 Security Incident Response and Reporting

Adopted: MM/DD/YYYY
Revised: MM/DD/YYYY
Effective: MM/DD/YYYY

POLICY
The Agency will monitor all electronic information systems for breaches of security, mitigate harmful effects of security incidents to the extent practicable, and document any such security incidents and their outcomes.

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(6)

PROCEDURES
1) **Creation of Response Team, Contingency Planning and Drills**
   a) **Incident Response Team.** The HIPAA Security Officer is responsible for managing security incident response and reporting. At the Superintendent's option, the Agency may appoint an Incident Response Team. The mandate to this group would be to coordinate the Agency's response to security incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services by the Agency and the media.
   b) **Contingency Plans.** The Incident Response Team may meet on a periodic basis to develop contingency plans, such as identification of a security consulting firm, public relations firm, or legal counsel who can be contacted in the event of a serious incident.
   c) **Security Incident Drills.** The Incident Response Team may conduct security incident drills to develop skills and improve performance in the event of a serious security incident.
2) **Security Incident Reporting and Response Procedure**
   a) **Reporting Security Incidents.** Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
   b) **Response Procedure.** The HIPAA Security Officer and/or Incident Response Team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Policy 3035 Breach Reporting and Policy 1080 Duty to Report Violations and Security Incidents, Policy 3065 Mitigation will be followed as appropriate. The superintendent of the Agency will be notified and any contingency plans will be activated.
   c) **Documenting Security Incidents.** In conjunction with the HIPAA Security Officer, a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include:
      i) Date and time of report
      ii) Date and time of incident
      iii) Description of circumstances
      iv) Corrective action taken
      v) Mitigating action taken

      Documentation will be kept for 6 years.
3) **Post-Incident Analysis.** The HIPAA Security Officer and/or Incident Response Team will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response, and recommend to management any changes they believe appropriate.

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.
- A 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

HIPAA BUSINESS ASSOCIATE AGREEMENT

This business associate contract ("Agreement") is entered into by and between _____ ("COVERED ENTITY") and _____ ("BUSINESS ASSOCIATE").

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 45 C.F.R. Part 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", "business associate contract", "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" as defined and regulated by the HIPAA regulations. BUSINESS ASSOCIATE is a "business associate" as defined and regulated by the HIPAA regulations.
4) Per the January 25, 2013, HIPAA Regulation changes, HIPAA business associates are also regulated by the HIPAA regulations.
5) COVERED ENTITY has entered into a HIPAA business associate contract with BUSINESS ASSOCIATE.
6) COVERED ENTITY and BUSINESS ASSOCIATE agree 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**. BUSINESS ASSOCIATE provides services for COVERED ENTITY. 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 – Permitted Uses and Disclosures. In performance of the tasks specified in Attachment A – Permitted Uses and Disclosures, 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 BUSINESS ASSOCIATE's business, and/or
      ii) to carry out the legal responsibilities of 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 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) BUSINESS ASSOCIATE may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by COVERED ENTITY.
   C) Use appropriate physical, technical and administrative safeguards and comply with the requirements of the HIPAA Security Regulations (45 CFR § 164 Subpart C) to prevent use or disclosure of PHI other than as provided for by the Agreement.
   D) Report to COVERED ENTITY any security incident, and any use or disclosure of PHI not provided by this contract, including breaches of unsecured protected health information as required by 45 C.F.R § 164.410 within 10 days. Upon notification of a security incident, BUSINESS ASSOCIATE shall provide its preliminary risk assessment, as required by 45 CFR § 164.402(2), to COVERED ENTITY. COVERED ENTITY shall make final determinations regarding the risk assessment.
   E) 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.

F) 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".

G) 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".

H) Maintain and make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528.

I) To the extent that BUSINESS ASSOCIATE is to carry out COVERED ENTITY's obligations under the HIPAA Privacy Regulations, 45 CFR § 164 Subpart E, comply with the requirements of the Privacy Regulations in the performance of those obligations.

J) 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 BUSINESS ASSOCIATE's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

K) Return to COVERED ENTITY or destroy, as requested by 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 of protected health information. 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, whose 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 obligations 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 in this Agreement herein or by written mutual agreement of the parties.

B) Termination. As provided for under 45 C.F.R. § 164.504, COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that BUSINESS ASSOCIATE has breached a material provision of this Agreement. Alternatively, COVERED ENTITY may choose to: (i) provide BUSINESS ASSOCIATE with 30 days written notice of the existence of an alleged material breach; and (ii) afford 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 2K above, detailing BUSINESS ASSOCIATE's return of 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 contracts. Further, it may be modified or amended only in writing as agreed to by each party.

7) **Indemnification**. BUSINESS ASSOCIATE agrees to reimburse COVERED ENTITY for all costs reasonably associated with a breach of the confidentiality of protected health information which BUSINESS ASSOCIATE is responsible for safeguarding. Costs reasonably associated with a breach include, but are not limited to, regulatory fines, costs of breach notification, costs of breach mitigation and legal costs.

8) **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:_____	By:_____
Name: _____	Name:_____
Title: _____	Title:_____
Date:_____	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.]

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 ASSOCIATE 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 B2: Sample Service Provider Agreement

Service providers such as Physical Therapists, Speech Therapists, and Occupational Therapists who are independent contractors do not meet the definition of a HIPAA Business Associate. However, they should be placed under a confidentiality agreement that includes similar provisions.

CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement ("Agreement") is entered into by and between _____ ("SERVICE PROVIDER") 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 as amended.
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) Providers of medical and related services, if they submit electronic claims on their own behalf, are also HIPAA Covered Entities. Healthcare providers who do not transmit electronic claims are not subject to the HIPAA regulations, and consequently COVERED ENTITY is requiring the confidentiality assurances detailed in this agreement.

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

1) **Covered Entities Attest to HIPAA Compliance**. If SERVICE PROVIDER is a HIPAA covered entity, SERVICE PROVIDER attests that it fully complies with all applicable HIPAA regulations.
2) **Allowed Uses and Disclosures of Protected Health Information**. The SERVICE PROVIDER provides services for the COVERED ENTITY. The SERVICE PROVIDER may use and disclose protected health information only as follows:
   A) SERVICE PROVIDER may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, SERVICE PROVIDER may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.
   B) SERVICE PROVIDER may further use and disclose PHI, if necessary:
      i) for the proper management and administration of the SERVICE PROVIDER's business, and/or
      ii) to carry out the legal responsibilities of the SERVICE PROVIDER if the disclosure is either
         a) required by law, or
         b) SERVICE PROVIDER 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 SERVICE PROVIDER of any instances of which it is aware in which the confidentiality of the information has been breached.
3) **Responsibilities of SERVICE PROVIDER**. With regard to its use and disclosure of protected health information, SERVICE PROVIDER 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. These include:
      i) Any PHI stored on any portable computer equipment owned by SERVICE PROVIDER must be encrypted.
      ii) Text messaging with any information relating to individuals served shall be strictly limited to scheduling appointments.
      iii) Records shall be removed from COVERED ENTITY's premises only with permission of COVERED ENTITY

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.

D) Require that subcontractors who create, receive, maintain or transmit ePHI on behalf of SERVICE PROVIDER agree to the same confidentiality provisions specified in this agreement.

E) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to COVERED ENTITY if requested as part of COVERED ENTITY's compliance program.

F) 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 SERVICE PROVIDER's possession and retain no copies or electronic back-up copies. If this is not feasible, SERVICE PROVIDER 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.

4) **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.

5) **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. COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that the SERVICE PROVIDER has breached a material provision of this Agreement. Alternatively, the COVERED ENTITY may choose to: (i) provide the SERVICE PROVIDER with 30 days written notice of the existence of an alleged material breach; and (ii) afford the SERVICE PROVIDER 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.

6) **Survival**. The respective rights and obligations of SERVICE PROVIDER and COVERED ENTITY under the provisions of paragraph 3F above, detailing SERVICE PROVIDER's return and/or ongoing protections of protected health information, shall survive the termination of this Agreement.

7) **Amendment**. This Agreement supersedes any previously negotiated confidentiality agreements. Further, it may be modified or amended only in writing as agreed to by each party.

8) **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 SERVICE PROVIDER _____
_____
_____
_____

If to COVERED ENTITY: _____
_____
_____
_____

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

SERVICE PROVIDER	**COVERED ENTITY**
By:_____	By:_____
Name: _____	Name:_____
Title: _____	Title:_____
Date:_____	Date:_____

Attachment A – Permitted Uses and Disclosures

SERVICE PROVIDER is authorized to use protected health information for the purposes of

[INSERT A CLAUSE THAT DESCRIBES SERVICE PROVIDER's ALLOWED USES AND DISCLOSURES. THIS WILL VARY DEPENDING ON THE NATURE OF THE RELATIONSHIP.

Example Clauses:

Physical, Speech or Occupational Therapist: SERVICE PROVIDER is authorized to use and disclose protected health information for the execution of duties described under any other agreement with COVERED ENTITY and for providing therapy services to individuals, including any coordination of care and/or consultations with other medical professionals.

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.

HIPAA Security Officer Job Description

REPORTS TO: Superintendent

GENERAL PURPOSE:
The information security manager serves as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of Individual, provider, employee, and business information in compliance with organization policies and standards.

DUTIES:
1) Document security policies and procedures created by the information security committee/council.
2) Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures.
3) Initiate activities to create information security awareness within the organization.
4) Perform information security risk assessments and act as an internal auditor.
5) Serve as the security liaison to clinical administrative and behavioral systems as they integrate with their data users,
6) Implement information security policies and procedures.
7) Review all system-related security planning throughout the network and act as a liaison to information systems.
8) Monitor compliance with information security policies and procedures, referring problems to the appropriate department manager.
9) Coordinate the activities of the information security committee.
10) Advise the organization with current information about information security technologies and issues.
11) Monitor the access control systems to assure appropriate access levels are maintained.
12) Prepare the disaster prevention and recovery plan.

QUALIFICATIONS:
Information security certification, such as the CISSP, is preferred.

Source: http://www.hipaadvisory.com/

Appendix D: Facility Security and Access Plan

General

- All exterior doors shall be locked from the outside at all times
- All employees shall enter via main entrance
- Building Access control system shall be maintained by Executive Secretary (High St.) and School Secretary (School) to restrict access of employees to permitted times
- Servers, Telecommunication Equipment, Routers and Switches shall be maintained in locked rooms and/or locked cabinets
- Video surveillance cameras are in place to monitor activity in all buildings
- Nurse rooms shall be locked when nurse is away
- File cabinets with confidential information shall be locked
- Office doors shall be locked when the person is away
- A full-time contract Resource Officer is stationed at the entrance to the school to screen all visitors, issue visitor badges and record their ingress and egress

Appendix E: Minimum Necessary – Workforce, Disclosures and Requests

Workforce Access to PHI and Safeguards

Person, Classes of Persons, or Business Associates	***Categories of PHI Needed***	***Additional Safeguards(*)***
Administration		
Superintendent	All	
Business Manager	All	
Nurses	Medical notes, relevant medical information	
Executive Secretary	All records	
Training Coordinator	All Records	Does eligibility determinations
Community Relations / Special Projects Coordinator	All Records	Currently serving as HIPAA Privacy / Security Officer
Adult Services		
Community Employment Supervisor	All Adult Records	
Workshop Specialists	All Adult Records	
Job Coach	Medical Needs	
Service & Support		
Service & Support Director	All	
Service & Support Administrators	All	
Transportation/Maintenance		
Bus Drivers	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
Maintenance / Custodian	None	No User ID will be provided;
School		
Director of Educational Services	All School Records	
School Secretary	All School Records	
Administrative Assistants	All School Records	
Maintenance / Custodian	None	
Teachers	Records for students in their classes	
Classroom Aides	Records for students in their classes	
Developmental Specialist	All Student Records	
Business Associates		
Tuscarawas County Board of DD	Data in computer systems	Tuscarawas County Board provides computer support services
Mid East Ohio Regional Council (MEORC)	Gatekeeper (PAWS person); MUI person	PAWS entry, MUI Investigators

	needs access to records for investigation	
Stark County Educational Service Center	Student Records	Contract PT / OT / ST, EI Contract Manager
County Auditor's Office	records pertinent to bill payment	
Superior Technology Group	All computer data on Servers	Dave Josey
Primary Solutions, Inc.	Gatekeeper Data	
Special Olympics Coordinator	Medical needs	
Other Entities		
Sheriff's Department	None	Tammy Dowdell; however, Sheriff's department can request incident reports as part of criminal investigations

*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) **Superior Technology Group.** Support vendor Superior Technology is under contract to provide support for hosted computer servers. 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. Access is enabled only when support is needed.
   C) **IT Support.** The Tuscarawas County Board IT Specialists has 24/7 access to the computer network and servers for IT Support purposes.
   D) **Document Imaging Support.** Vendor GBS is provided access, when required, for technical support.
   E) **Family Office Equipment.** PC repair services. PC is dropped off for service/repair.
2) **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.
3) **Auditor's Office –** When authorizing payment of bills, fiscal files may be reviewed by the Auditor's office prior to authorization of payment.
4) **Ohio DODD –** Information will be shared routinely with Ohio DODD in order to ensure continuity of services for Individuals.
   A) Targeted Case Management billing is uploaded via Gatekeeper to the Ohio DODD website.
   B) Specific to MUI case files, the Investigative Agent and internal UI staff will utilize the State's secure website to input required information.
   C) Inspectors come on-site. Any information requested will be provided.
5) **Transportation Providers –** Use Carroll County Transit**.** To ensure quality of care for adults served, medical needs and guardian/family contact information will be shared with contracted providers. SSAs will call or send information via secure email.
6) **Ohio Department of Education -**Multiple interactions
   A) During accreditation, inspectors come on-site. Any school records requested will be provided.
   B) Transportation billing via direct upload to ODE site
   C) Child count is placed in an Excel spreadsheet and uploaded to ODE portal

7) **County School Districts –** Individual information will be shared, such as change of address, via phone, fax or secure email.
8) **Bureau of Disability Determination (OOD) –** Using the Bureau's forms, assessment information will be shared in order to determine Individual's eligibility for benefits. Sent via secure email by SSA.

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.
2) **County School Districts** – Referrals are received from school districts.

Appendix F: Miscellaneous

POLICY 1330 HIPAA Assignments and Documentation
HIPAA Privacy Officer: Tim Liversage
HIPAA Security Officer: Tim Liversage
Staff person to receive HIPAA Complaints: Tim Liversage
Staff person to provide access to Individual records: Tim Liversage
Staff person to receive requests for amendment of Individual records: Tim Liversage
Staff person to answer questions about HIPAA policies and procedures: Tim Liversage

Hybrid entity designation, if any: No Hybrid Entity designation
Designated Record Set:
All information in Gatekeeper software
All information relating to Individuals served in FileBound.

Authorization Form

Carroll County Board of Developmental Disabilities

Carroll County Board of DD
P.O. Box 429
Carrollton, OH 44615
330-627-6555

Carroll Hills School
2167 Kensington Rd. NE
Carrollton, OH 44615
330-627-7651

AUTHORIZATION FOR RELEASE OF CONFIDENTIAL INFORMATION

Name of Individual Served _____ Date of Birth _____

I authorize CCBDD to:

Release to: _____
The following information:
___ Assessment and diagnosis (MFE)
___ Treatment and progress
___ Social History
___ Psychological Test results
___ Other _____

Obtain from: _____
The following information:
___ Assessment and diagnosis (MFE) (F.E.D.)
___ Treatment and progress
___ Most current IP (ISP, IEP, IHP)
___ Psychological Test results
___ 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

Carroll 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 CARROLL HILLS 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 Carroll Hills 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.

WHO USES AND DISCLOSES MY RECORDS?

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: Administrative Office, Carroll Hills School].

At Carroll Hills 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 Carroll County Board of Developmental Disabilities.

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,
- 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 the 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:

HIPAA Privacy Officer
Carroll County Board of DD
P.O. Box 429
Carrollton, OH 44615
(330) 627-6555
HIPAA@CarrollHills.com]

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: HIPAA Privacy Officer
Carroll County Board of DD
P.O. Box 429
Carrollton, OH 44615
(330) 627-6555

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 5/1/2019

Employee-Owned Mobile Device Agreement

I, _____, have read, understand, and agree to abide by the requirements of Policy 3085 Portable Computing Devices (and any updates to the Policy). I agree to the following:

- I agree to complete all necessary training regarding implementing the security features of my enrolled mobile devices.
- I accept responsibility to back up personal applications and data on my enrolled mobile device(s).
- If applicable, I agree to upload all organization-related data created on my enrolled mobile device(s) to the organization's network daily.
- I agree to report the loss of a device containing PHI within 24 hours in accordance with Policy 3090 Security Incident Response and Reporting.
- I grant the IT Department permission to remotely-lock/wipe and/or use geo-location technology if my device is lost or stolen. I understand that a remote-wipe of my device may cause loss of my personal data and will not hold the agency liable for personal data loss in the event of a remote-wipe.
- I accept responsibility for any actions performed on my enrolled device(s) by others whom I permit to use the enrolled device(s).
- I agree to follow all procedures concerning the removal of the organization's data prior to returning/selling/disposing of my enrolled mobile device(s).
- I understand that I may be subject to disciplinary action if I access the agency's network with my enrolled mobile device(s) without following all requirements specified in Policy 3085 Portable Computing Devices.
- I understand that I may be subject to disciplinary action if I use an Agency-approved, personally-owned mobile device while driving in a manner that is in violation of the laws of the jurisdiction in which I am physically present.
- Upon notification, I agree to provide my enrolled mobile device(s) to the IT Department and provide all necessary access codes for e-discovery purposes and/or compliance audits.
- I understand and accept that I may lose access to the network resources and/or have my enrolled mobile device(s) wiped upon written request from my supervisor to the Human Resources Department.
- Upon termination of employment, I agree to provide all my enrolled mobile device(s) to the IT department to remove all agency data and disable access to the organization's IT resources.

_____

Employee Name (please print)

_____

Employee signature

_____

Date

Agency-Owned Mobile Device Agreement

I, _____, have read, understand, and agree to abide by the requirements of Policy 3085 Portable Computing Devices (and any updates to the Policy). I agree to the following:

- I agree to complete all necessary training regarding implementing the security features of my agency-owned mobile device(s).
- I agree to report the loss of a device containing PHI within 24 hours in accordance with Policy 3090 Security Incident Response and Reporting.
- I understand that I may be subject to disciplinary action if I access the agency's network with my agency-owned mobile device(s) without following all requirements specified in Policy 3085 Portable Computing Devices.
- I understand that I may be subject to disciplinary action if I use an Agency-owned mobile device while driving in a manner that is in violation of the laws of the jurisdiction in which I am physically present.
- I understand that I may be subject to disciplinary action if I allow others unauthorized access to my agency-owned mobile device.
- I understand that I may be subject to disciplinary action if I dispose of or intentionally or recklessly damage an agency-owned mobile device.
- I understand that I may be subject to disciplinary action if I exceed acceptable personal use of an agency-owned mobile device.
- Upon termination of employment, I agree to return my agency-owned mobile device(s) to the IT department.

_____

Employee Name (please print)

_____

Employee signature

_____

Date

CCBDD Disclosure Log

Date	Person or Entity receiving Records	Description of records disclosed	Purpose of disclosure/ Legitimate interest	Description of threat to health or safety (if reason is in response to health or safety threat or emergency)

CCBDD ACKNOWLEDGEMENT OF HIPAA POLICIES AND PROCEDURES

Name_____ Date_____

I have reviewed and understand the HIPAA policies and procedures that are relevant to my job duties. These include:

Policy number	**Description**
1010	HIPAA – General Rules
1020	Minimum Necessary
1030	Confidentiality Safeguards (Oral and Written)
1040	Speaking with the Family or Friends of an Individual Receiving Services
1050	Authorizations
1070	Minors, Personal Representatives and Deceased Individuals
1080	Duty to Report Violations and Security Incidents
1090	Disclosures that do not Require an Authorization
3080	Computer Usage
3082	Social Media Use
3085	Portable Computing Devices
3087	Employee Work at Home

Further, I understand all other HIPAA policies that are relevant to my job duties.

I have been assigned my own User ID, will access the computer only with my User ID, and I will keep my password confidential. I further understand that the software used by CCBDD tracks all records viewed, changed, deleted or printed based on User ID. I understand that I will be held responsible for all computer usage performed with my User ID, and that failure to follow these procedures could result in discipline, termination of employment, civil fines and/or criminal prosecution.

Signature:_____ Date:_____