Union County Board of Developmental Disabilities
POLICY

Policy Number: HC-1	Page: 1	Of: 30
Title: Definitions		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: ~~1/20/16~~, 8/21/17		
Reviewer/Job Title: Director of Operations		

HIPAA CONFIDENTIALITY & PRIVACY POLICIES

POLICIES FOR ALL STAFF

Confidentiality, Privacy and Computer Security Definitions

(A) POLICY

The following definitions shall apply to all Confidentiality, Privacy, and Computer Security Policies.

(B) DEFINITIONS

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 in order 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.

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) **Applicable Requirements –** Applicable requirements mean applicable federal and Ohio law and the contracts between the UCBDD and other persons or entities which conform to federal and Ohio Law.
4) **Authentication –** means the corroboration that a person is the one claimed.
5) **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.
6) **Breach –** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information.

Breach *excludes*:

a) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.

b) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.

Except for the two 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:

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

7) **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.
8) **Confidentiality –** means the property that data or information is not made available or disclosed to unauthorized persons or processes.
9) **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.
10) **Council of Government (COG) –** A Council of Government is a group of DD Boards or other governmental entities which have entered into an agreement under ORC Chapter 167 and are operating in accordance with that agreement.
11) **Designated Record Set –** Designated record set means:
A group of records maintained by or for a covered entity that is:

a) The medical records and billing records about individuals maintained by or for a covered health care provider;

b) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
c) 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) **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.
13) **DODD** – the Ohio Department of Developmental Disabilities
14) **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.
15) **Education Records** – As defined in the FERPA regulations, records that are:
    a) Directly related to a student; and
    b) Maintained by an educational agency or institution or by a party acting for the agency or institution.
        i) The term does not include:
            a. Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
            b. Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
    c) Records related to employment.
        i) 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.
        ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition.
    d) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
        i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
        ii) Made, maintained, or used only in connection with treatment of the student; and
        iii) Disclosed only to individuals 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; and

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

16) **Employee –** Employee means any person employed by the board, volunteers, board members and other persons whose conduct, in the performance of work for the DD Board, is under the direct control of the DD Board, whether or not they are paid by the DD Board.
17) **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.
18) **Facility –** means the physical premises and the interior and exterior of a building(s).
19) **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.
20) **Guardian of the Person –** Guardian of the Person means an individual appointed by the Probate Court to provide consent for and make decisions for the ward
21) **HCBS –** HCBS means Medicaid-funded home and community-based services waiver program available to individuals with DD granted to ODJFS by CMS as permitted in §1915c of the Social Security Act, with day-to-day administration performed by DODD.
22) **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.
23) **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.
24) **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 §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 §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 §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

25) **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.

26) **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

27) **HIPAA –** HIPAA means the Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 - 1320d-9 and at 42 CFR Parts 160, 162 and 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.
28) **ICF/IID –** An ICF/IID is an intermediate care facility for persons with developmental disabilities certified to provide services to individuals with DD or a related condition in accordance with 42 CFR part 483, subpart I, and administered in accordance with OAC § 5101:3-3.
29) **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.
30) **Individual, or Individual Receiving Services** – Means a person who receives services from the County Board. In the event that the individual is a minor, the term "individual" in these policies may also include the parent or guardian of the individual. In addition, in regard to any privacy rights, individual may also mean an individual's "personal representative" as it is defined under HIPAA regulations.
31) **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
        j)

ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

32) **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.

33) **Integrity –** means the property that data or information have not been altered or destroyed in an unauthorized manner.

34) **ISP –** ISP means the Individual Service Plan which is a document developed by the ISP team, containing written descriptions of the services and activities to be provided to an individual, which shall conform to the applicable requirements, including, but not limited to OAC § 5123:1-2-02, 5123:2-3-17 and 5123:2-12-03. References to the ISP shall include Individual Plans developed in accordance with OAC § 5123:2-15-18.

35) **Limited Data Set –** means protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
   a) Names;
   b) Postal address information, other than town or city, state and zip code;
   c) Telephone numbers;
   d) Fax numbers;
   e) Electronic mail addresses;
   f) Social Security numbers;
   g) Medical record numbers;
   h) Health plan beneficiary numbers;
   i) Account numbers
   j) Certificate/license numbers;
   k) Vehicle identifiers and serial numbers, including license plate numbers;
   l) Device identifiers and serial numbers;
   m) Web Universal Resource Locators (URLs);
   n) Internet Protocol (IP) address numbers;
   o) Biometric identifiers, including finger and voice prints; and
   p) Full face photographic images and any comparable images.

36) **Malicious software –** means software, for example, a virus, designed to damage or disrupt a system.

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) **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

39) **Password –** means confidential authentication information composed of a string of characters.

40) **Payment –** means, in the context of a County Board:

a) Both
   i. Activities by the board required determine if an individual is eligible for services
   ii. Activities of the Board either to reimburse contracted providers for services rendered to individuals served or seeking reimbursement, for example from Medicaid of DODD, for services rendered to an individual served

b) The activities in paragraph (1) 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.

41) **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 UCBDD and the minor.

42) **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.

43) **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 board'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.

44) **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.

45) **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.

46) **Security or Security measures –** encompass all of the administrative, physical, and technical safeguards in an information system.
47) **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.
48) **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.
49) **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.
50) **TCM –** Targeted Case Management means an Ohio State Plan Medicaid service that provides case management, including service coordination, services to eligible individuals with DD in accordance with OAC Chapter 5123.
51) **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
52) **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
53) **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.
54) **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.
55) **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.
56) **User –** means a person or entity with authorized access.
57) **Violation**, **or violate** – means, as the context may require, failure to comply with a provision of either the HIPAA Privacy or Security rules.
58) **Workforce Member –** Workforce Member means the same as Employee. See definition above.
59) **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.

Revised: 12/30/2015

Policy Number: HC-2	Page: 1	Of: 1
Title: General Rules		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A) HIPAA CONFIDENTIALITY – GENERAL RULES

Confidentiality is the basis for professional relationships, as well as for the respect due personal privacy. It involves trust and confidence, and is the key to our professional relationships. All information in an enrollee's records, including information electronic information, is confidential.

The UCBDD shall conform to all requirements for privacy and confidentiality set forth by the State of Ohio, the federal HIPAA and FERPA laws, and any other applicable law. The UCBDD shall not use or disclose PHI except in accordance with applicable requirements.

1) Staff of the UCBDD may use or disclose PHI only as follows:
   a) For education, treatment, payment or health care operations. This information is to be used by employees who are official members of a habilitation/educational team, with the goal of serving the enrollee.
   b) In accordance with a release or authorization of the individual in accordance with policy and procedure set forth in Authorizations.
   c) As permitted in Speaking with the Family or Friends of an Individual Receiving Services.
   d) As permitted by in 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 Minimum Necessary Policy.
   a) All employees are responsible for safeguarding the information regarding individuals we serve, as detailed in Confidentiality Safeguards (Oral & Written)
3) Rights of individuals served by UCBDD may be exercised by parents, guardians and personal representatives as detailed in Minors, Personal Representatives and Deceased Individuals.
4) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in Duty to Report Violations and Security Incidents.
5) Supervisors, managers and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.

Policy Number: HC-3	Page: 1	Of: 2
Title: Minimum Necessary Policy		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A) MINIMUM NECESSARY POLICY

For purposes other than those listed below, the use and disclosure of PHI must be limited to the minimum necessary to satisfy the request or to complete the task. The Privacy Officer shall implement safeguards and protocols to implement this policy. All employees shall follow those protocols.

FOR THE PRIVACY OFFICER

1) **Implementation Approach**. The Privacy Officer will implement the minimum necessary requirement with the steps detailed below. Measures to limit workforce access, and procedures for both routine disclosures and requests for PHI will be created and documented as detailed below:

a) **Limiting Workforce Access to PHI**: Access to the PHI will be granted based on the individual's role and determined by the Superintendent and Privacy Officer of UCBDD. UCBDD 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 necessary 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.

iv) The Privacy Officer will document the results of this analysis in Minimum Necessary – Workforce, Disclosures and Requests.

b) **Procedures for Routine Disclosures and Requests.** The HIPAA Privacy Officer will identify all routine disclosures made by Board employees, for which the minimum necessary requirement applies, and create procedures to implement these. The same shall be done for routine requests for PHI. These results shall be documented in Minimum Necessary – Workforce, Disclosures and Requests.

c) **Implementation.** The Privacy Officer shall take the steps to implement the results of the analysis above, including configuring access control on software, staff training for routine requests and disclosures, and any other measures necessary.

FOR ALL EMPLOYEES

2) **Minimum Necessary Requirement**.

a) **Basic Requirement**. When using or disclosing PHI, or when requesting PHI from another entity, employees must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

b) **Exceptions**. The minimum necessary requirement does NOT apply to:

i) Disclosures to or requests by a health care provider for treatment

ii) Uses or disclosures made to the individual served, including but not limited to any requests for their records or requests for an accounting of disclosure

iii) Uses of disclosures made pursuant to an Authorization

iv) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations

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

4) **Procedures for Non-Routine Disclosures or Requests**

a) **For non-routine disclosures**, when subject to the minimum necessary provision, the individual making the disclosure will apply the minimum necessary principle. He or she may seek the guidance, if necessary, of the Privacy Officer (or his/her designee).

b) **For non-routine requests**, the requesting party will utilize the minimum necessary principle, seeking the guidance, if necessary, of the Privacy Officer (or his/her designee).

c) **Good Faith Reliance** – UCBDD staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:

i) The disclosure is made to a **public official**, permitted to receive information, and the public official represents that the request is for the minimum necessary information;

ii) The request is from another **covered entity**;

iii) The request is from a **professional** at UCBDD, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary

Title: Confidentiality Safeguards (Oral & Written)
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A) CONFIDENTIALITY SAFEGUARDS (ORAL & WRITTEN)

UCBDD shall maintain appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

1) **Safeguards for Electronic PHI**. The HIPAA Security policies detail physical, technical and administrative safeguards to protect electronic PHI. In addition, these policies detail some of the physical security measures for paper records.
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 in a locked and secured area. 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.
   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 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 Privacy 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 Director of Operations, especially upon disposal to insure 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) **When leaving for the night**, all employees shall clean their desks of PHI to reduce exposures to cleaning personnel and others who may have access to the facilities at night.

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 shall 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.

Policy Number: HC-5	Page: 1	Of: 2
Title: Sharing Information		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

A) **SPEAKING WITH THE FAMILY AND FRIENDS OF AN INDIVIDUAL RECEIVING SERVICES**

UCBDD personnel are allowed to disclose protected health information to individuals involved with the care an individual being served, in specific situations, after giving the Individual the opportunity to either agree to or object to the disclosure.

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 the 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 UCBDD, 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.

Title: Authorizations
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

A) AUTHORIZATIONS

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

Legal Notes: FERPA applies to records created for education; HIPAA applies to all other records

1) **Valid Authorization**. Unless otherwise authorized by UCBDD policy and/or state or federal law operations requires specific authorization by the Individual being served or his/her legal representative. A standard authorization form is required. In the event that 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 individual, person, or agency disclosing the information.
   e) Names of the individual, person, or agency to whom the disclosure is to be made.
   f) The date, event, or condition upon which the authorization expires (which can be no longer than 180 days from the date of signing).
   g) Statement of the individual's right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke.
   h) Statement that UCBDD 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) UCBDD is aware authorization has been revoked.
e) UCBDD is aware information is false.
f) Authorizations to release PHI cannot be combined with other documents.

3) **For authorizations presented in person for immediate release**, the staff member shall verify the identity of the recipient, after which the information may be released.
4) **Proper Completion of Authorization Form by Staff**. The staff person handling the request should complete the following steps, and annotate the bottom of the Authorization Form:
   a) The employee should write their name on the completed authorization form.
   b) The original signed authorization shall be saved in the individual's master record, and a copy must be given to the Individual.
   c) A record of the release shall be maintained in the individual's main record, using the Disclosure Log included as an Appendix, detailing the following information:
      i) The date of the disclosure.
      ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
      iii) A brief description of the PHI disclosed.
      iv) A brief statement of the purpose of the disclosure.
      v) If the disclosure was due to a health or safety emergency, a description of the significant threat to health or safety.
5) **Retention Period for Written or Electronic Copy of Authorization**. The UCBDD must retain the written or electronic copy of the authorization for a period of six (6) years from the later of the date of execution or the last effective date.
6) **Revocation of Authorization.** Upon instructions of revocation of authorization, UCBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.
7) Note that information from other service providers contained in the Individual's record may be released with the Individual's written authorization.

Title Minors, Personal Representatives and Deceased Individuals
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A) MINORS, PERSONAL REPRESENTATIVES AND DECEASED INDIVIDUALS

Purpose

To establish 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.

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 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.

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**. UCBDD 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 UCBDD Authorization Form which permits release of PHI.
3) **Recognized Personal Representative**. UCBDD 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 3109.051(H)),
   c) An individual 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 UCBDD 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, UCBDD may elect not to recognize a person as a personal representative of an individual. In order for UCBDD to choose not to recognize a person as a personal representative, UCBDD 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 UCBDD 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, UCBDD 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 (with a valid consent), quality assurance or other auditing or program review functions. UCBDD 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**. PHI may be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate (ORC § 5126.044).

c) **Proper Party to Authorize Release of PHI Absent Executor, Administrator, or Court Appointed Representative**. Absent an executor, administrator, or other court-appointed representative for the deceased individual's estate, the following persons listed below may authorize the release of PHI in order of priority. An entire category must be exhausted (i.e., no people in the category exist or are still alive) before moving to the next category.

i) Spouse (if married)
ii) The person's children
iii) The Person's parents
iv) The Person's brothers or sisters
v) The person's uncles or aunts;
vi) The person's closest relative by blood or adoption
vii) The person's closest relative by marriage

Policy Number: HC-8	Page: 1	Of: 1

Title: Duty to Report Violations and Security Incidents
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A) DUTY TO REPORT VIOLATIONS AND SECURITY INCIDENTS

Confidentiality of individual information, and the computer security required to protect information regarding individuals receiving services is taken very seriously at UCBDD. 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.

For the purpose of this policy the Privacy and/or Security Officer are currently one in the same.

2) **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.
3) I**nvestigation.** 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 the Board 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.
4) **Procedure for Security Breach.** For security breaches, **the** Privacy and/or Security Officer will follow any procedures detailed in Breach Reporting.
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, action will be taken and documented in accordance with the discipline policy
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.

Title: Disclosures that do Not Require an Authorization
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A) DISCLOSURES THAT DO NOT REQUIRE AN AUTHORIZATION

UCBDD 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:

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.

For judicial and administrative proceedings.

For law enforcement purposes.

To coroners, medical examiners, and funeral directors.

For organ, eye or tissue donation.

Research.

To reduce or prevent a serious threat to public health and safety.

Specialized government functions.

For workers' compensation or other similar programs if applicable.

(B)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.

(C) SPECIAL CIRCUMSTANCES

UCBDD 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 board intends to enroll in, or is already enrolled in, for the purposes of Individual's enrollment or transfer.
   b) The UCBDD may use or disclose protected health information 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.

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 UCBDD receives PHI disclosed under this section in its role, the UCBDD may use the PHI to carry out its duties.

4) **To protect victims of abuse, neglect, or domestic violence**
   a) **Reports of child abuse**
      i) Reports of child abuse shall be made in accordance with Ohio law.
      ii) The UCBDD 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 UCBDD 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 UCBDD 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 UCBDD 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 UCBDD would be informing a personal representative, and the UCBDD

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 UCBDD, in the exercise of professional judgment.

5) **For health 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 UCBDD receives PHI disclosed under this section in its role as LMAA, the UCBDD may use the PHI to carry out its duties.
6) **For judicial and administrative proceedings**
   a) The UCBDD 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 UCBDD may comply with such legal requests only if:
      i) The UCBDD 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 UCBDD 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 UCBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements.
7) **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 UCBDD may disclose to a law enforcement official protected health information that the UCBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the UCBDD.
   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.

The UCBDD shall not respond to a court order, subpoena, or request for information from law enforcement without review by an attorney to ensure compliance with applicable requirements.

8) **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.
9) **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.
10) **To reduce or prevent a serious threat to public health and safety**
   a) The UCBDD may disclose PHI 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.

11) **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 UCBDD 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 individuals 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.

12) **In connection with "whistleblowing"**. In connection with "whistleblowing", or reporting of a violation of law or ethics, an employee of UCBDD 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

13) **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.

Policy Number: HC-10	Page: 1	Of: 3
Title: Individual's Right to Access Records		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A) INDIVIDUAL'S RIGHT TO ACCESS RECORDS

Individuals, served by UCBDD, and their personal representatives, have the right to access and/or inspect the PHI 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

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(I)(7)(d) County Board Administration – Record Policy – Right of Access

OAC § 5123:2-1-02(I)(7)(a)(iv) County Board Administration – Records policy – Informing individuals receiving services about types and locations of records kept

LEGAL NOTES:

State laws, HIPAA, and FERPA all provide that individuals receiving services have access to their records.
State law offers greater right of access than HIPAA, which includes exceptions; consequently the state law applies with no restrictions to an individual's access.

1) **Who May Access Records**
   a) An individual served by the board 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 any of those individuals 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.** UCBDD 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 individual was appointed a "Personal Representative" under HIPAA.

c) **Forms of Access Requested by the Individual**. The UCBDD shall provide the individual with access to their records in any of the following ways requested by the individual:

i) **By inspection**. UCBDD shall provide a private room for the individual to review the records under the supervision of a UCBDD staff member who will insure that the record is not altered, or

ii) **Photocopy**. UCBDD shall provide a photocopy of the entire record or portion of the record requested.

iii) **Electronic format**. UCBDD shall provide an electronic copy of the information requested if this is feasible; if not, the Privacy 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 board shall honor requests for commonly used media, such as USB Flash drives.

d) **Record of Parties Accessing Records.** The Privacy Officer or his/her designee shall maintain a record of parties accessing records (except the access by the individual or their parent) including the name of the party, the date access was given, and the purpose of access.

3) **Other services/rights of individuals, parents, and guardians**

a) **Explanation and Interpretation of Records.** UCBDD will respond to reasonable requests for explanation and interpretation of the records.

b) **List of Types and Locations of Records Maintained by UCBDD.** Upon request, UCBDD must provide individuals, parents and guardians a list of the types and

locations of records maintained or used by UCBDD.

c) **Known Records Not Maintained by UCBDD**. If the UCBDD does not maintain the PHI that is the subject of the individual's request for access, and the UCBDD knows where the requested information is maintained, the UCBDD must inform the individual where to direct the request for access.

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) UCBDD at present has no fees for photocopies, postage or electronic media used to provide records.

Title: Individual's Right to Request Amendment of Records
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)Individual's Right to Request Amendment of Records

Subject to the rules set forth in applicable requirements and UCBDD procedures, an individual has the right to have the UCBDD amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

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.

(B)REQUESTS FOR AMENDMENTS

1) **Amending Statements Believed to be Inaccurate, Misleading or in Violation of Individual's Rights.** An individual, parent, guardian, or other person acting as a HIPAA personal representative may request amendment of PHI about the individual (and exercise rights for hearing and statements of disagreement), which they believe is inaccurate, misleading, or violates the rights of the individual, and is held by the UCBDD or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
2) **Responsibility of Privacy Officer**. The Privacy Officer of the UCBDD is responsible for receiving requests for amendment, processing the requests, arranging for any hearings,

and completing required documentation.

3) **Time to Act on a Request for Amendment.** The UCBDD will act on a request for amendment without unnecessary delay and no later than 60 days after the date of the request.
4) **Accepted Request for Amendments.** If the UCBDD accepts the requested amendment, in whole or in part,
   a) the UCBDD must make the appropriate amendment, and inform the individual and other persons or entities who have had access to the information.
5) **Denied Request for Amendments.** Otherwise, if the UCBDD believes the existing record is correct as is, it may deny the amendment:
   a) **Written Notice.** If an amendment is denied, the UCBDD will give written notice in plain language which includes the following:
      i) The basis for the denial;
      ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
      iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the UCBDD provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
      iv) The individual's right for a hearing to challenge the information.
   b) **Statement of Disagreement.** If the individual submits a statement of disagreement, the Privacy Officer will insert this statement into the appropriate portion of the record. Otherwise, the Privacy officer will insert into the record that the individual requested an amendment and the UCBDD's denial.
   c) **Written Rebuttal.** The UCBDD may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the UCBDD must provide a copy to the individual who submitted the statement of disagreement.
   d) **Permanent Record.** The inserted statement of disagreement and any rebuttal become a part of the permanent record and must be included with all future disclosures of the covered records.
   e) **Individual's Request for Copy of Changed Record.** At the individual's request, UCBDD will send a copy of the changed record to any party requested by the individual (per ORC 1347.09).
   f) **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 UCBDD may separately transmit the information to the recipient of the transaction in a standard EDI format.

(C) RECORDS HEARINGS

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

1) **Hearing Procedures**

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

2) **Results of Hearing**
   a) If, as a result of the hearing, UCBDD decides that the information in its records is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the individual, it must amend the information accordingly and inform the individual in writing.
   b) If, as a result of the hearing, UCBDD 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 UCBDD.
   c) Any information placed in the record as a result of this hearing, UCBDD must maintain this statement as part of its permanent record, and include it with any subsequent disclosure.

Policy Number: HC-12	Page: 1	Of: 3
Title: Individual's Right to Receive an Accounting of Disclosures		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A)Individual's Right to Receive an Accounting of Disclosures
In accordance with HIPAA Regulations, Individuals must be told, if they ask, what personal health information has been sent to whom and why.

Audience

Privacy Officer, Supervisors

REFERENCES

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

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 UCBDD 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 5b 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 UCBDD does not charge a fee for accountings.

6) **The written accounting must meet the following requirements**:
   a) All disclosures of the Individual's PHI during the 6 years prior to the request (or such shorter period as is specified in the request) as stated above.
   b) As to each disclosure, the accounting must include:
      ii) The date of the disclosure.
      iii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
      iv) A brief description of the PHI disclosed.

v) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure.

vi) If during the time period for the accounting, multiple disclosure 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 disclosure made during the accounting period and the date of the last such disclosure during the accounting period.

vii) If the accounting request includes school records, consult legal counsel regarding the need to obtain records of redisclosures by state or local school officials (see 34 CFR 99.32).

c) UCBDD 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.

Policy Number: HC-13	Page: 1	Of: 2

Title: Individual's Right to Request Additional Restrictions
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)Individual's Right to Request Additional Restrictions

UCBDD supports Individual's right to request restrictions on the use or disclosure of protected health information which may be above and beyond the restrictions in organizational policy

Audience

Privacy Officer, Supervisors

REFERENCES

45 CFR § 164.522(a)

1) **Refer the Request to UCBDD' Privacy Officer or Designee:** All requests 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 UCBDD' 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 UCBDD will agree**: The UCBDD 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:** UCBDD will notify the Individual of its final decision (whether approving or denying the request) in writing. The notice will be maintained in the Main Individual Record.
   a) Granting the Request: If UCBDD agrees to the restriction, the notice to the Individual will clearly state what restriction UCBDD 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 UCBDD 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 UCBDD 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 UCBDD' 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.

Title: Individual's Right to Request Confidential Communications
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A) INDIVIDUAL'S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

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 our administrative systems.

Audience

Privacy Officer

REFERENCES

45 CFR 164.502(h) Confidential communications

45 CFR 164.522(b) Confidential communications requirements

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 UCBDD 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.

Policy Number: HC-15	Page: 1	Of: 1

Title: Individual's Right to Notice of Privacy Policies
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)Individual's Right to Notice of Privacy Policies

Individuals (or their parents) are entitled to a notice detailing the privacy practices of the board. The board will provide such notice in a manner compliant with both the HIPAA and FERPA regulations.

Audience

Privacy Officer

REFERENCES

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)

1) **Drafting of Notice**. The Privacy Officer shall draft a notice which is compliant with the requirements of the HIPAA regulations and FERPA regulations. This shall include translations as necessary based on the language needs of the individuals served. Further, the notice shall be consistent with the board's privacy practices as detailed in these policies.
2) **Updating Notice.** The Privacy Officer shall update the Notice as necessary based on changes in the board's privacy policies and/or the legal requirements. Upon update, the website and notices posted at each facility (see below) shall be updated.
3) **Distribution of Notice.** The Privacy Officer shall insure that Board policies and procedures, are maintained to insure appropriate distribution of Notice:
    a) The first distribution shall be documented in the records of the individual served. This documentation shall consist of a signed acknowledgement that the individual or parent received the Notice, for compliance with HIPAA requirements.
    b) While the individual is in the Harold Lewis School the Notice shall be distributed annually to all parents, in compliance with FERPA requirements for Annual Notice.
    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 insure that the Notice is posted:
    a) **Website.** On the board's website.
    b) At Each Facility. At each facility, in a place where individuals served can be reasonably expected to see the notice.

Policy Number: HC-16	Page: 1	Of: 1
Title: CONFIDENTIALITY POLICIES FOR SUPERVISORS--Business Associate Contracts		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A)CONFIDENTIALITY POLICIES FOR SUPERVISORS--Business Associate Contracts
UCBDD will obtain satisfactory assurance that Business Associates will appropriately safeguard PHI by maintaining appropriate HIPAA Business Associate agreements or MOUs.

REFERENCES:

45 CFR 160.103

45 CFR § 164.502(e)

45 CFR § 164.504(e)

ORC § 5126.044 – Ohio Statute on confidentiality of records

1) **Business Associate Contract or Memorandum of Understanding.** UCBDD 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 and 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 UCBDD 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 UCBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, UCBDD will take steps to cure the breach or end the violation. If UCBDD is unable to cure the breach or end the violation, UCBDD will terminate the Business Associate Contract.

Policy Number: HC-17	Page: 1	Of: 1

Title: Notice of Privacy Practices
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)NOTICE OF PRIVACY PRACTICES

UCBDD will provide a written Notice of Privacy Policies, as required by law, to each Individual.

REFERENCES

45 CFR 164.520

ORC § 1347.08(A)(3) (Personal Information Systems)

OAC § 5123:2-1-02(I) County Board Administration – Records, Informing individuals about policies

34 CFR 99.7 FERPA Annual Notification

LEGAL NOTES:FERPA requires an annual notice. HIPAA requires a one-time notice, with redistribution upon change.

1) **Creation and Update of Notice**.
   a) The HIPAA Privacy Officer shall create the Notice of Privacy Practices to conform to requirements of HIPAA and FERPA. See Appendix F - UCBDD Notice of Privacy Practices.
   b) Upon material change of the notice, which is required upon any material change of privacy policies, an updated copy will be provided to all Individuals receiving services and/or parents.
2) **Distribution of Notice.**
   a) All individuals and/or their parents will receive a copy of the Notice of Privacy Practices upon intake with the board.
   b) As part of that intake process, the Individual and/or parent, guardian or personal representative, shall sign an acknowledgement of their receipt of this Notice as part of the intake paperwork. This acknowledgement will be retained as part of the permanent record.
   c) For children in the school, an updated copy of the notice will be sent to individuals and/or their parents each year with the Back To School information.
3) **Other Postings and Requirements**
   a) The Notice of Privacy Practices will be posted in reception areas of all board facilities.
   b) The Notice of Privacy Practices will be posted on the website.
   c) Copies of the notice will be maintained for 6 years

Policy Number: HC-18	Page: 1	Of: 1

Title: Notice of Privacy Practices
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)NON-INTIMIDATION AND NON-RETALIATION

UCBDD will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals who exercise any right, not against staff or other individuals who express the opinion that UCBDD policies are not consistent with the law, or not being implemented properly. UCBDD will not require any individual receiving services to waive any of his/her rights under HIPAA as a condition of education, treatment, or enrollment.

1) **UCBDD 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 compliance rule;
   b) **Individuals receiving Services and others**. Any Individual receiving services, or other person for:
      i) Filing of a complaint with the Secretary under HIPAA compliant;
      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 HIPAA compliance rules, 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 protection 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 UCBDD, is strictly prohibited.
4) **Prohibition against Waiver of Rights**. No office, program, facility or employee of the UCBDD 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.
5) UCBDD will also follow the whistleblower policy as appropriate.

Policy Number: HC-19	Page: 1	Of: 3
Title: **HIPAA Assignments and Documentation**		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A)HIPAA ASSIGNMENTS AND DOCUMENTATION

UCBDD 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.

REFERENCES:

Federal Law 45 CFR 164.530(j) – Documentation requirement,

164.520(e) – Notices of Privacy Practices;

164.524(e) – Access of individuals to protected health information;

164.526(f) – Amendment to protected information;

164.508(b)(6) – Uses and disclosures for which an authorization is required;

164.512(i)(2) – Uses and disclosures for research purposes;

164.522(a)(3) – Rights to request privacy protection for protected health information;

164.528(d) – Accounting of disclosures of protected health information – Implementation specification

ORC § 5126.044(E) (General records of DD Boards)

OAC § 5101:3-3-20(L) (ICFs/IID)

OAC § 5123:1-2-02(J)(8) (Waiver records)

OAC § 5123:1-2-08(R) (IO waivers)

OAC § 5123:1-2-11(P) (HCBS waivers for licensed providers)

OAC § 5123:2-1-02(I)(7) appointment of person responsible for ensuring the safekeeping of records and securing them against loss or use by unauthorized persons.

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.

1) **Designating a Privacy Officer and Other Individuals to Assist HIPAA Committee.** The superintendent shall designate an individual 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 individuals 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.
   b) Notice of Privacy Practices, as described in Notice of Privacy Practices.
   c) Restrictions on use or disclosure of PHI agreed to by UCBDD as described in the Individual's Right to Request Additional Restrictions.
   d) Records of disclosures, as required by the Individual's Right to Receive an Accounting of Disclosures.
   e) Any signed authorization as described in Authorizations.
   f) All privacy-related complaints received, and their disposition, if any, as described in 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.

   The above records will be maintained for 6 years.

4) **Policy and Procedure Audit Trail**. When created or updated, all policies will be annotated with the approval date and revision history. Current policies will be maintained in a computer file folder designated "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 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 insure proper maintenance of all documentation itemized in this policy.

Title: Privacy Complaints
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)PRIVACY COMPLAINTS

Any individual or employee to may complain about the UCBDD's Confidentiality and Privacy policies and procedures and/or the UCBDD's compliance with those policies and procedures. The UCBDD 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

1) **The HIPAA Privacy Officer shall manage this complaint process**, and shall be designated in the Notice of Privacy practices as the individual to receive complaints.
2) The UCBDD will extend the provisions of the whistleblower policy to all individuals 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 the whistleblower policy 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

individual filing the complaint.

7) **Documentation of Complaints.** The UCBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with policy. HIPAA Assignments and Documentation.

Policy Number: HC-21	Page: 1	Of: 1

Title: Policy Updating and Staff Training
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)Policy Updating and Staff Training

UCBDD is committed to maintaining updated Policies as required by law, and to train staff as necessary on these policies.

REFERENCES

45 CFR 164.530(b)
45 CFR 164.530(i)
45 CFR 164.520
ORC § 5123.64(A) training in rights

OAC § 5123:2-3-08 staff training in licensed facilities

OAC § 5123:2-5-01(C)(12) training requirements for adult service workers

OAC § 5123:2-5-02(C)(12) training requirements for adult service workers

OAC § 5123:2-5-05(C)(13) training requirements for early intervention workers

OAC § 5123:2-5-07(C)(9) training requirements for investigative agents

1) Annual Review and Update of All Policies. The HIPAA Privacy Officer shall each 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 shall insure that all new staff will be receive training on UCBDD Confidentiality and Computer Security policies promptly after hiring.
3) **Training All Staff When Policies are Substantially Changed**. The HIPAA Privacy Officer shall insure that staff receive training on Confidentiality and Computer Security policies when they are substantially changed.

Title: policies for executive management & HIPAA privacy/security officer
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)HIPAA SECURITY POLICIES--POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA PRIVACY/SECURITY
OFFICER Security Management Process

UCBDD will appoint a HIPAA Privacy/Security Officer. The HIPAA Privacy/Security Officer will orchestrate the board's security management process.

Audience

Executive Management

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(2)

OAC § 5123:2-1-02(I)(7) appointment of person responsible for ensuring the safekeeping of records and securing them against loss or use by unauthorized persons.

REFERENCES

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, 2012

NIST SP 800-53, Security Self-Assessment Guide for Information Technology Systems, 2010

Center for Internet Security at www.cisecurity.org

1) **The Superintendent will designate a HIPAA Privacy/Security Officer**. The job responsibilities for this individual are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer. The HIPAA Privacy/Security officer will assume the duties detailed in OAC § 5123:2-1-02(I)(7)(a)(5), which include overall responsibility for safekeeping of all records, electronic and paper. 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 Privacy/Security Officer will be responsible for security management process**. This will include:
    a) **Security Team**. The HIPAA Privacy/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 board. The Security Team's charter would be defined by the board, 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 Assessment**. The Risk Assessment is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the board. The Computer Security Risk Assessment will be handled as follows:
   i) The county board will use the risk assessment methodology detailed in NIST SP 800-30 (2012).
   ii) The results of this assessment shall be documented and maintained for 6 years.
   iii) The Risk Assessment shall be updated on an annual basis.

c) **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 including implementation of new and updated policies, acquisition of technical security measures, or physical security measures. The Board shall have final authority on risk management decisions.
   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 board staff regarding compliance.
   v) Monitor Board compliance with the information security policies, and take action as appropriate based on this monitoring.

d) **Information System Inventory**. The HIPAA Privacy/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 insure availability in the event of a fire or other disaster.

Title: Data Backup
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)DATA BACKUP

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

Audience

HIPAA Privacy/Security Officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(7)

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.
1) **Multiple Backup Generations**. Backups should include as many generations as is practical to store. One backup per day is appropriate.
2) **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 insure that appropriate data backup is maintained.
3) **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.
4) **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.
5) **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 individual shall be responsible. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.

6) **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.
7) **Backup Media Security**. Backup media shall be maintained in a secure location.
8) **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.
9) **Data Recovery Plan.** The HIPAA Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

Title: Disaster Recovery Plan and Emergency Mode Operation
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)DISASTER RECOVERY PLAN AND EMERGENCY MODE OPERATION

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

Audience

Hipaa privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(7)

164.312(a)(1)

References

NIST SP 800-14

NIST SP 800-18

NIST SP 800-26

NIST SP 800-30

NIST SP 800-53

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 board operations and implement preventative measures to reduce the likelihood of system failure. These would include technical measures such as 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. The written plan should include:
    a) Computer applications shall be reviewed and assessed as to their criticality for maintaining board operations. The results of this assessment shall be documented.
    b) Development of written documentation of tasks and responsibilities for members of the Disaster Recovery Team in the event of various failure scenarios.
    c) 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.
    d) Complete and current employee information and vital records.
    e) Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster.

Reasonable steps to assure rapid recovery and mitigate losses can include, if appropriate:

    a) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by board management.
    b) Contracts with hot and/or cold system sites if deemed necessary and prudent by board management.
    c) 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 individuals 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 assessable in the event of catastrophic loss of the facility.

Title: Facility Security and Access Control
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)FACILITY SECURITY AND ACCESS CONTROL

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

Audience

HIPAA Privacy / Security Officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.310(a)(1)

References

NIST SP 800-66

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
   e) Individual Paper Records

   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 Operations Manager 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 Individuals**. 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 Privacy/Security Officer and/or police.

Policy Number: HC-24	Page: 1	Of: 1

Title: Annual Security Evaluation
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)ANNUAL SECURITY EVALUATION

Annually the HIPAA Privacy/Security Officer shall conduct a technical evaluation of the board'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 privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.308(a)(8)

ORC § 5123:2-1-02(I) County Board Administration, Records, Annual Review of Safeguards

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, contracted to an outside firm.
   a) Standards and Measurements shall first be developed as the basis for the evaluation. These may include checklists, interviews with personnel, penetration testing, and review of required documentation. The evaluation design should evaluate compliance with current HIPAA Security requirements.
   b) The evaluation shall be conducted and the results documented. Weaknesses should be identified and any recommendations prepared.
2) **Report and Recommendations.** The HIPAA Security Officer shall submit their report to the Superintendent and/or Board including any recommendations.
3) **Documentation of Review.** The results of the review will be documented, and documentation shall be retained for 6 years.
4) **Additional Security Evaluation with the Introduction of New Technology.** A security evaluation should additionally be conducted with the introduction of new technology, such as wireless access, instant messaging, new smartphones etc., in response to newly recognized risks, or other event which would likely impact overall system security.

Policy Number: HC-25	Page: 1	Of: 2
Title: Audit Control and Activity Review		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A)AUDIT CONTROL AND ACTIVITY REVIEW
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 privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.312(b)

164.308(a)(1)

164.308(a)(5) Log-in Monitoring

1) **System Activity Logs**. Activity logs shall be enabled at the following levels:
   a) **Operating System** (Windows Server 2007): 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 individual.
   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 individual 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 individuals 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 Information System 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.

Policy Number: HC-26	Page: 1	Of: 1

Title: Malicious Software Protection
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)MALICIOUS SOFTWARE PROTECTION

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

Audience

Hipaa privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.308(a)(5)

1) **Multi-Layered Defense Strategy.** The HIPAA Security Officer will insure 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 insure that the products, services, and configuration, and policies appropriately manage risk for this rapidly evolving threat.

Policy Number: HC-27	Page: 1	Of: 3
Title: Breach Reporting		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

(A)Breach Reporting
The board 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

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164, Subpart D

164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, 164.414

1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Privacy Officer and the Superintendent 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 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 board 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 board 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, the HIPAA Security 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
                (a) a notice shall be conspicuously placed on the board'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 board superintendent, a press release shall be prepared detailing the information in section 2Ab above, and other relevant information.
ii) Upon approval of the board 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 2Ab 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.

2) **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 board is responsible for issuing the notice detailed in this policy.

3) **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 board 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.

4) **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 board should have become aware if it exercised reasonable diligence.

Title: Security Awareness Program
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)SECURITY AWARENESS PROGRAM

The board will conduct an ongoing security awareness program to train and refresh staff on the board'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 Part 164; 164.308(a)(5)

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.

Policy Number: HC-29	Page: 1	Of: 2

Title: Device and Media Disposal and Re-Use
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)DEVICE AND MEDIA DISPOSAL AND RE-USE

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 Part 164; 164.310(d)(1)

1) **Media Disposal Handled by HIPAA Security Officer**. As specified in Policy 3080 Computer Usage, board employees are prohibited from storing Protected Health Information on the board'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* board requires that at a minimum, data from electronic media should be "cleared", that is, protected against a robust keyboard attack but not necessarily against a laboratory attack.
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)

Title: Technical Safeguards
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)TECHNICAL SAFEGUARDS

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

Audience

HIPAA Security Officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.312(c)

164.312(d)

164.312(e)

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 "Enterprise Client" level of security, with modifications as necessary to allow for functionality.
   c) Microsoft Security Configuration 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.
   e) 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 board shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. *Specifically,* the board 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.
   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 Board-Used Software**. Software used by board 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 criteria 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 county board. 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**. Automated integrity checks should be run on server data periodically. Any problems should be reported to the HIPAA Security Officer for corrective action.

Policy Number: HC-31	Page: 1	Of: 1

Title: Mitigation
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)MITIGATION

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

Audience

Privacy officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.530(f) – Mitigation

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.

Title: Electronic Signatures
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)ELECTRONIC SIGNATURES

Electronic signatures may be utilized at UCBDD 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

1) Definitions

a) 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 by a person with the intent to sign the record.
b) 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.

2) 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.

3) **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 board must establish and maintain system specific procedures for any system which also satisfies other current policies.

4) **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.

5) **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.

Policy Number: HC-33	Page: 1	Of: 4
Title: Security policies for HR staff & supervisors		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

SECURITY POLICIES FOR HR STAFF & SUPERVISORS

(A)EMPLOYEE SYSTEM ACCESS AND TERMINATION PROCEDURES

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 Part 164

164.308(a)(3)

164.308(a)(4)

164.312(a)(1)

164.314(d)

164.308(a)(5) Password Management

(B)AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS

Audience: HIPAA Security Officer, Privacy Officer

1) **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.
2) **Access Profiles.** The HIPAA Security Officer shall utilize the security capabilities of the various network and application software systems at the board 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.

3) **Granting Access to Information Systems**. The authority to grant access to information systems rests with board of directors and is delegated to the human resources department. 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.
4) **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 board, 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.
5) **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.
6) **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.

(C)SYSTEM AND FACILITY ACCESS FOR NEW HIRES

Audience: Supervisors, Human Resource Department

1) **Requests for Access to Information Systems.** Supervisors and/or the human resources department shall direct requests for access to information systems shall be directed 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.
2) **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 individual will be assigned in accordance with this policy, as described above.
3) **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.
4) **Documentation of System Access Rights**. As described above, the HIPAA Security Officer will maintain documentation of system access rights.
5) **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 individual workstations.

6) **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.

(D)PASSWORDS and PASSWORD MANAGEMENT

Audience: HIPAA Security Officer

1) **Password Complexity**. Network policies shall be established to enforce password complexity as follows: 8 character minimum, minimum of 1 upper case letter, 1 lower case letter and 1 non alphanumeric symbol.
2) **Lockout**. The system shall lock accounts after 5 unsuccessful attempts.
3) **Password Reuse**. The system shall maintain the previous 5 passwords and prohibit re-use of any of these recent passwords.
4) **Password Changes**. The HIPAA Security Officer may implement a mechanism to insure that all employees change their passwords at least every 6 months.

(E)EMPLOYEE JOB CHANGES

Audience: Human Resources Department, HIPAA Security Officer

1) 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.

(F)EMPLOYEE TERMINATION

Audience: Supervisors, Human Resource Department, HIPAA Security Officer

1) **Change Employee Password and Disable User ID.** 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.
2) **Documentation.** The HIPAA Security Officer shall document the disabling of system access.
3) **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 insure the integrity and security of confidential board information. This could include such measures as:
    a) Physically escorting the individual off the premises after notifying him/her of the termination.

b) Disabling system access as specified above on a timely basis.
c) Requiring all staff in the individual's workgroup to change passwords.
d) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the individual and perceived threat.

(G)EMERGENCY SYSTEM ACCESS

Audience: Supervisors, HIPAA Security Officer

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.

Title: HIPAA Administrative Requirements Security Policies For All Staff--**Computer Usage**
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

HIPAA ADMINISTRATIVE REQUIREMENTS
SECURITY POLICIES FOR ALL STAFF

(A)COMPUTER USAGE

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 Part 164

164.310(b) Workstation Use

164.310(c) Workstation Security

164.308(a)(5) Log in Monitoring

(B)WORKSTATION USE

1) **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 we serve: 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.
2) **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. "Limited use" is not easily defined so employees should contact their supervisors for clarification. In general, "limited use" means:
   a) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
   b) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.

c) Workstations must never be used for any activity that would be embarrassing to the Board if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
   i) downloading or viewing pornographic, racist, profane or otherwise objectionable material
   ii) conducting conversations of a sexual nature of relating to an illicit affair
   iii) relating to any illegal activity
   iv) political activity
   v) 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.

d) Personal use of Social Networking tools, such as Facebook, Twitter, LinkedIn, MySpace and others is detailed separately.
e) Employees are discouraged from staying logged in to social networking sites, instant messaging sites/tools, and their personal email except during their own time.

3) **E-Mail Use**. Employees with board e-mail accounts should check e-mail daily. Board E-mail accounts in general are to be used for board purposes only. E-mail should be written in professional manner and should be courteous and respectful. Other policies when using e-mail:
   a) 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 Protected Health Information unless it is appropriately encrypted.
   b) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the board.
   c) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in the public records policy
   d) For personal matters, employees must use a personal account such as Gmail or Yahoo mail.
      i) In the event that any board e-mail is received on a personal account, the employee must forward the email to the employee's Board account so that it is entered into the public record.
      ii) In the event that a personal email is received on a Board account, redirect the discussion to a personal email account.
4) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to removable media, such as Flash drives, CDs, DVD or portable hard drives, or transmit via e-mail or fax or other method, any board confidential information or Protected Health Information on board computer system, except when specifically authorized by the HIPAA Security Officer for board purposes.
5) **All Usage is Logged**. THE BOARD RESERVES THE RIGHT TO MONITOR ALL USAGE OF BOARD 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 BOARD COMPUTERS. All logs of employee activity are property of the board.

6) **Data Storage on Server Only**. All data must be stored on the server. 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. The storage of large volumes of images is discouraged because of the large storage capacity used. 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. ANY DATA FOUND ON WORKSTATIONS MAY BE DELETED WITHOUT NOTICE. NO DATA ON WORKSTATIONS IS BACKED UP!
7) **Duplication of copyrighted material prohibited**. No employee may duplicate copyrighted software or other media using board equipment.
8) **Board approved hardware only**. Only board approved and 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.
9) **Electronic signatures**. Employees using software that includes board-approved electronic signature capabilities shall follow all procedures specified in Policy 3070 Electronic Signatures

(C)WORKSTATION SECURITY

1) Except with specific approval of the HIPAA Security Officer, workstations must not be setup in a public access area.
2) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.
3) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.
4) 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.
5) All board servers must be secured with a strong password (see "User IDs and Passwords" below) and setup to automatically lock out user access after a maximum of three (3) minutes of inactivity.

(D)USER IDs and PASSWORDS

1) Each employee is assigned a unique User ID and Password. Employees must only use their User ID to access board 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.

2) Passwords should be at least 8 characters long and include upper case letters, lower case letters and numbers. The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed.
3) In general, passwords should be memorized and not written. Any written reminder should not be maintained in the vicinity of the workstation.
4) Users are required to change all passwords at least every 6 months.
5) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

(E)EMERGENCY SYSTEM ACCESS

1) 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.)

Title: HIPAA Administrative Requirements Security Policies For All Staff-- **Social Media Use**

Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC

Effective Date: 1/20/16

Reviewer/Job Title: Director of Operations

(A)Social Media Use

Social networking sites, notably Facebook but including many others, have become a significant communication medium in our world. The board mandates specific guidelines for the use of these sites both limiting certain activities to insure confidentiality and privacy of individuals being served while permitting other uses that advance the mission or the board, for example with fundraising.

Audience

All staff

1) **Definitions**

a) Social Networking Sites – means sites that enable linking with other people, sharing information, and communicating. Popular examples include Facebook, Twitter, LinkedIn, Google+ and others.

2) **Board Sponsored Use**. The HIPAA Privacy officer or Superintendent may approve the establishment of a board sponsored Fan Page or Group. The Privacy Officer and/or superintendent will provide guidelines for use in the event of any board sponsored use of Facebook or similar social network.
3) **Personal use of Facebook and other social network sites by employees**.
   a) Employee Personal use of Facebook.
      i) **Employee Use During Work Hours**. During work hours, employees are expected to focus on work-related activities. Consequently, in general, they are expected to not keep Facebook open as management believes that this communication medium has the potential to be distracting and has the potential to reduce the employee's productivity.
      ii) **Employee Use at any time**. Facebook is a new communication medium. The medium is semi- public; while it includes many options for specifying levels of privacy, Facebook users often share private information in unintended ways. Further, the Facebook site has a history of malfunctions and security breaches. Consequently, any use of Facebook has the potential to become a public communication, so, employees of the board must follow the following guidelines: (1) **Sharing of work-related activities**. Employees should limit the sharing of

any Board related information to information that they would be acceptable to be made public, for example, on the front page of a major newspaper.

(a) Examples of information that would be appropriate to share on one's wall include:
    (i) The employee's excitement and satisfaction with the work and mission of the board.
    (ii) Details of an upcoming public event sponsored by the board, such as a local "Special Olympics" day.
    (iii) The name of a friend who is a co-worker at the board.

(b) Examples of information that would be inappropriate to share on one's wall include:
    (i) The name of an Individual receiving services from the Board.
    (ii) A complaint about the Board such as displeasure with a supervisor or co-worker.
    (iii) Any Protected Health Information, or PHI, (which includes facial images of Individuals being served).

Employees are further encouraged but not required to limit communications on Facebook to those that would portray them in a professional manner.

Policy Number: HC-36	Page: 1	Of: 1

Title: HIPAA Administrative Requirements Security Policies For All Staff-- **Portable Computing Devices and Home Computer Use**
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)Portable Computing Devices and Home Computer Use

Data on laptops should be encrypted and various security measures should be employed with employee-owned PDAs.

Audience

All staff

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.312(a)(2)(iv) Encryption and decryption

1) **Encryption on Laptops and other mobile devices**. Employees who use board provided laptop computers, smartphones, or other portable computing devices containing PHI shall use the encryption features to reduce the impact of disclosure in the event that the device is lost or stolen. The staff will use an encryption solution as detailed in Policy 3060 Technical Safeguards.
2) **Lost devices**. Employees must immediately report lost or stolen devices to their supervisor and the HIPAA Security Officer in accordance with the Security Incident procedure.
3) **Employee-owned portable computing devices**. Employees may not use their personal smartphones or other portable devices to conduct board activities.
4) **Work at home and use of employee's home computer.** Employees working at home and using their home computers for work purposes in general should avoid storing PHI on their home computers. Employees **must** consult with the HIPAA Security Officer regarding safeguards prior to storing any PHI on their home computers.
5) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required while using these devices.

Title: HIPAA Administrative Requirements Security Policies For All Staff-- **Security Incident Response and Reporting**
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

(A)SECURITY INCIDENT RESPONSE AND REPORTING

The board 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 Part 164; 164.308(a)(6)

(B)CREATION OF RESPONSE TEAM, CONTINGENCY PLANNING AND DRILLS

1) **Incident Response Team.** The HIPAA Security Officer is responsible for managing security incident response and reporting. As part of a pro-active management process, he or she may recommend to the Superintendent assignment of individuals for an Incident Response Team. The mandate to this group would be to coordinate the board's response to security incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services from the Board and the media.
2) **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.
3) **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.

(C)SECURITY INCIDENT REPORTING AND RESPONSE PROCEDURE

1) **Reporting Security Incidents.** Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
2) **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 Breach Reporting and Duty to Report Violations and Security Incidents, Mitigation will be followed as appropriate.

The superintendent of the Board will be notified and any contingency plans will be activated.

3) **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
   a) Date and time of report
   b) Date and time of incident
   c) Description of circumstances
   d) Corrective action taken
   e) Mitigating action taken

   Documentation will be kept for 6 years.

4) **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.

Title: Appendix A: Minimum Necessary
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

APPENDIX A: 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	
IU's	All	
Director of Operations	All	
Special Olympics Coordinator	All	
Family Outreach Coordinator	All	
Medicaid Officer	All	
Administrative Secretary	Computer data	Limited to report entries
Human Resources Officer	All	
WorkNet		
Director	All	
Job Developer	All	
Services Coordinator	All	

3)

Service & Support		
Service & Support Director	All	
Administrative Secretary	All	
Service & Support Coordinators	All	
Nurse	All	
School		
Director	records regulated under FERPA	
Preschool Coordinator	records regulated under FERPA	
Classroom Instructors	records regulated under FERPA	
Instructor Assistants	records regulated under FERPA	
Language Development Specialist	Medical Needs, notes pertinent to speech/language	
Occupational Therapist	Medical needs, notes pertinent to service provision	
Physical Therapist	Medical needs, notes pertinent to service provision	

Early Intervention Specialists	All Early Intervention files	
Custodian	Medical Needs	
Business Associates		
County Auditor's Office	records pertinent to bill payment	
Primary Solutions, Inc. Intellivue GateKeeper	Database Data	
DODD	Medical needs	
First Student	Medical needs related to transportation	
NetGain	As needed for technical assistance	

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

Title: Appendix B: Procedures For Routine Disclosures and Requests Of PHI
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC
Effective Date: 1/20/16
Reviewer/Job Title: Director of Operations

APPENDIX B: PROCEDURES FOR ROUTINE DISCLOSURES AND REQUESTS 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) **NetGain.** Network support vendor NetGain is under contract to provide 24/7 network support. Access is provided at all times.
   B) **Primary Solutions and other Support.** Primary Solutions and other support vendors will be granted access rights on an as needed basis. Technical solutions for implementing this authorization will be deployed by the board.
2) **Job and Family Services** – For services rendered, which are reimbursed by ODJFS, submit requested information to JFS.
3) **Health Department –** Contents of the early intervention file may be shared with the Health Department, upon their request, if the initial referral for services came through the Help Me Grow network.
4) **Prosecutor's Office**. When a warrant or subpoena is presented, any file may be released to the Prosecutor's Office. In addition, if the Board is seeking legal counsel, file contents to be revealed will be reviewed by the Privacy Officer to ensure that minimum necessary standards are being followed.
5) **Auditor's Office –** When authorizing payment of bills, fiscal files may be reviewed by the Auditor's office prior to authorization of payment.
6) **DODD –** Information will be shared routinely with Ohio DODD in order to ensure continuity of services for individuals. Specific to MUI case files, the Investigative Agent and internal UI staff will utilize the State's secure website to input required information.
7) **Surveyors –** Upon confirmation of surveyors credentials, the superintendent or his/her designee may authorize review of any files requested by the surveyor with the exception of MUI State Files.
8) **Transportation Providers –** To ensure quality of care for individuals, medical needs and guardian/family contact information will be shared with contracted providers.
9) **County School Districts –** Individual information will be shared, upon written request on School District letterhead, if the request for services originated in the school district.
10) **Bureau of Disability Determination –** Using the Bureau's forms, assessment information will be shared in order to determine individual's eligibility for benefits.
11) **Attorneys –** When a subpoena is presented, the protocol in Disclosures that do Not Require

an Authorization will be carefully followed to determine, with legal counsel assistance, if the subpoena should be honored.

12) **Other Outside Agencies –** In order to ensure continuity of services to individuals, the Director of SSA or the Director of Adult Services will share IP, medical limitation and incident reports with authorized contacts from Family Services.
13) **Law Enforcement –** As identified by the Director of Services & Supports, guardianship, family contact information and behavior support plans will be shared with law enforcement agencies. In addition, upon presentation of a warrant and verification of credentials if presented in person, other file information may be shared with law enforcement agencies. See Disclosures that do not Require an Authorization.

Procedures for Routine Requests of PHI

1) **Eligibility Inquiry** – Individual insurance eligibility will be verified by using procedures provided by the Ohio Department of Developmental Disabilities.

Policy Number: HC APPENDICES	Page: 1	Of: 1
Title: Appendix C: UCBDD Disclosure Log		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 1/20/16		
Reviewer/Job Title: Director of Operations		

UCBDD Disclosure Log

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