Administration
801 West Union Street - Athens, Ohio 45701
Phone: 740-594-3539 - Fax: 740-593-3189
Dr. Kevin Davis, Superintendent
athenscbdd.org

Updated Policies for Review
Batch 12
Second Read

Administrative Policies

- Policy 61 – Confidentiality & Computer Security Policies: HIPAA, FERPA, IDEA & Ohio Law Compliance – Updated throughout by Eagle Consulting Partners. Renamed to better reflect content of the updated policy.

Personnel Policies

- Policy 4-2 – Probation – Updated to change probationary period from 120 to 180 calendar days, per current ORC. Additional formatting changes throughout.

ATHENS COUNTY BOARD OF DD

Confidentiality & Computer Security Policies

HIPAA, FERPA, IDEA & Ohio Law Compliance

Updated March 2021

Eagle Consulting Partners, Inc.
6779 Memphis Ave. #7
Cleveland, OH 44144
216.503.0333
© 2020, All Rights Reserved
gpritts@eagleconsultingpartners.com
www.eagleconsultingpartners.com

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

Formatting Notes

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

DRAFT

Change Log

Date	Policy	Description

Table of Contents

CONFIDENTIALITY & PRIVACY POLICIES 7
POLICIES FOR ALL STAFF 7
1000 Confidentiality, Privacy and Computer Security Definitions 7
1010 Confidentiality – General Rules 13
1020 Minimum Necessary Policy 15
1030 Confidentiality Safeguards (Oral & Written) 17
1040 Speaking with the Family and Friends of an Individual Receiving Services 19
1050 Authorizations 20
1060 Verification 22
1070 Minors, Personal Representatives and Deceased Individuals 24
1080 Duty to Report Violations 26
1090 Disclosures that do not Require an Authorization 27
INDIVIDUAL RIGHTS 32
1200 Individual's Right to Access Records 32
1210 Individual's Right to Request Amendment of Records 34
1220 Individual's Right to Receive an Accounting of Disclosures 36
1230 Individual's Right to Request Additional Restrictions 38
1240 Individual's Right to Request Confidential Communications 39
1250 Individual's Right to Notice of Privacy Practices 40
CONFIDENTIALITY POLICIES FOR SUPERVISORS 41
1300 Business Associate Contracts 41
1320 Non-intimidation and Non-retaliation 42
1330 HIPAA Assignments and Documentation 43
1340 Privacy Complaints 45
1350 Policy Updating and Staff Training 46
HIPAA SECURITY POLICIES 47
POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER 47
3000 Security Management Process 47
3005 Data Backup 49

DRAFT

3010 Disaster Recovery Plan and Emergency Mode Operation 50
3015 Facility Security and Access Control 52
3020 Annual Security Evaluation 53
3025 Audit Control and Activity Review 54
3030 Malicious Software Protection 55
3035 Breach Reporting 56
3040 Security Awareness Program 58
3050 Device and Media Disposal and Re-Use 59
3052 Encryption and Key Management 60
3054 User Account Management 62
3056 Privileged Account Management 64
3060 Technical Safeguards 66
3062 Technical Controls for Mobile Devices 68
3065 Mitigation 69
3070 Electronic Signatures 70
SECURITY POLICIES FOR HR STAFF & SUPERVISORS 72
3075 Employee System Access and Termination Procedures 72
HIPAA ADMINISTRATIVE REQUIREMENTS 74
SECURITY POLICIES FOR ALL STAFF 74
3080 Computer Usage 74
3082 Social Media Use 77
3085 Portable Computing Devices 79
3087 Employee Work at Home 81
3090 Security Incident Response and Reporting 82
APPENDICES 83
Appendix A: Identifying Business Associates 83
Appendix B: Sample HIPAA Business Associate Agreement 85
Appendix B2: Sample Service Provider Agreement 89
Appendix C: Sample Privacy & Security Officer Job Descriptions 92
Appendix D: Facility Security and Access Plan 95
Appendix E: Minimum Necessary – Workforce, Disclosures and Requests 96

DRAFT

Workforce Access to PHI and Safeguards _____ **96**

Procedures for Routine Disclosures of PHI _____ **97**

Procedures for Routine Requests of PHI _____ **98**

Types and Locations of Records for School-Age and Early Childhood _____ **98**

Names and Positions of Employees with Access to PII _____ **98**

Appendix F: Miscellaneous _____ ***99***

Athens County Board of Developmental Disabilities (ACBDD) – Authorization for Release of Information _____ ***100***

Notice of Privacy Practices _____ ***101***

Employee-Owned Mobile Device Agreement _____ ***103***

Agency-Owned Mobile Device Agreement _____ ***104***

ACBDD Disclosure Log _____ ***105***

ACBDD ACKNOWLEDGEMENT OF HIPAA POLICIES AND PROCEDURES _____ ***106***

DRAFT

CONFIDENTIALITY & PRIVACY POLICIES

POLICIES FOR ALL STAFF

1000 Confidentiality, Privacy and Computer Security Definitions

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

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

AUDIENCE
All Staff

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

DEFINITIONS
1) **Access –** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (Taken from HIPAA regulations.)
2) **Administrative safeguards –** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
3) **Agency** – means ACBDD
4) **Applicable Requirements –** Applicable requirements mean applicable federal and Ohio law and the contracts between the ACBDD and other persons or entities which conform to federal and Ohio Law.
5) **Authentication –** means the corroboration that a person is the one claimed.
6) **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.
7) **Breach –** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information.
   a) Breach *excludes*:
      i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.
      ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.
      iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
   b) Except for the exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at

DRAFT

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

8) **Business Associate (BA) –** A Business Associate, basically, is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The complete definition is included in Appendix A - Identifying Business Associates.
9) **Confidentiality –** means the property that data or information is not made available or disclosed to unauthorized persons or processes.
10) **Covered Entity –** Covered entity means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA transaction rules.
11) **Designated Record Set –** Designated record set means:
    a) A group of records maintained by or for a covered entity that is:
        i) The medical records and billing records about Individuals maintained by or for a covered health care provider;
        ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
        iii) Used, in whole or in part, by or for the covered entity to make decisions about Individuals.

    For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
12) **Directory Information** -- as defined in FERPA, means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate; full-time or part-time), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended.
13) **Disclosure –** Disclosure means the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the entity holding the information.
14) **DODD** – the Ohio Department of Developmental Disabilities
15) **Early Intervention Records**. – means all records regarding a child that are required to be collected, maintained, or used under Part C of the Act and the regulations in this part. These are essentially equivalent to FERPA Education Records
16) **Education –** Education means activities associated with operating the school including instruction, IHP/IEP preparation, administration, behavioral intervention, extra-curricular activities and other normal school functions. Education shall also include activities associated with early intervention programming.
17) **Education Records** –
    a) As defined in the FERPA regulations, means records that are:
        i) Directly related to a student; and
        ii) Maintained by an educational agency or institution or by a party acting for the agency or institution.
    b) The term does **not** include:
        i) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
        ii) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
        iii) Either of the following:
            (1) Records relating to an Individual who is employed by an educational agency or institution, that:
                (a) Are made and maintained in the normal course of business;
                (b) Relate exclusively to the Individual in that Individual's capacity as an employee; and
                (c) Are not available for use for any other purpose.

DRAFT

(2) Records relating to an Individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(iii)(1) of this definition.

iv) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
   (1) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
   (2) Made, maintained, or used only in connection with treatment of the student; and
   (3) Disclosed only to persons providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution.

v) Records created or received by an educational agency or institution after an Individual is no longer a student in attendance and that are not directly related to the Individual's attendance as a student.

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

18) **Employee –** Employee means any person employed by the Agency, volunteers, board members and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.
19) **Encryption –** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
20) **Facility –** means the physical premises and the interior and exterior of a building(s).
21) **FERPA –** FERPA means the Family Educational Rights and Privacy Act, which are federal regulations that govern the privacy of records maintained by schools, as well as the rights of parents and students to access those records. These regulations are codified in CFR Title 34 Part 99.
22) **Guardian of the Person –** Guardian of the Person means a person appointed by the Probate Court to provide consent for and make decisions for the ward
23) **Health care –** means care, services, or supplies related to the health of an Individual. Health care includes, but is not limited to, the following:
   a) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and
   b) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
24) **Health Care Clearinghouse –** A Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system or community health information system that does either of the following functions:
   a) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
   b) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
25) **Health care operations –** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
   a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
   b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
   c) Except as prohibited under 45 CFR § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care

(including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR § 164.514(g) are met, if applicable;

d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f) Business management and general administrative activities of the entity, including, but not limited to:

   i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

   ii) Resolution of internal grievances;

   iii) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

   iv) Consistent with the applicable requirements of 45 CFR § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

26) **Health Oversight Agency –** Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

27) **Health Plan –** Health plan means an individual or group plan that provides, or pays the cost of medical care. A partial list of entities that are health plans (edited based on relevance to DD Boards) includes the following, singly or in combination:

   a) The Medicaid program under title XIX of the Act, 42 U.S.C. § 1396, et. seq.

   b) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

   c) A group health plan, that is, an employee welfare benefit plan (as defined in section 3(1) of the Employment Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1), including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents, that:

      i) Has 50 or more participants; or

      ii) Is administered by an entity other than the employer that established and maintains the plan.

   d) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers

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

29) **IDEA** – Individuals with Disabilities Education Act. Part C details rights and safeguards for infants aged 0-2 involved with Early Intervention programs, and Part B details rights and safeguards for children aged 3-18.

30) **Incidental Disclosure** – An unintentional disclosure of PHI, that occurs as a result of a use or disclosure otherwise permitted by the HIPAA Privacy Rule. An Incidental Disclosure is NOT a violation of the Privacy Rule. However, in order for incidental disclosures to not be a violation, the covered entity must be in compliance with the requirement for implementation of the minimum necessary principle, and also in compliance with the requirement to implement physical, technical, and administrative safeguards to limit incidental disclosures.

31) **Individual, Individual receiving services or Individual served** – Means a person who receives services from the Agency. Note that parents or minors, guardians and other "personal representatives" may exercise any right or privilege available to an Individual served.

32) **Individually Identifiable Health Information –** is information that is a subset of health information, including demographic information collected from an Individual, and:

   a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

   b) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision

of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
   i) That identifies the Individual; or
   ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

33) **Information system –** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
34) **Integrity –** means the property that data or information have not been altered or destroyed in an unauthorized manner.
35) **Malicious software –** means software, for example, a virus, designed to damage or disrupt a system.
36) **MOU –** MOU means a Memorandum of Understanding between governmental entities, which incorporates elements of a business associate contract in accordance with HIPAA rules.
37) **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
38) **Password –** means confidential authentication information composed of a string of characters.
39) **Payment –** means, in the context of a County Board of DD:
   a) Both:
      i) Activities undertaken by the Agency to obtain reimbursement for services rendered, for example, from Medicaid of DODD, to Individuals served.
      ii) Activities undertaken by the Agency to provide reimbursement to contracted providers for services provided to Individuals served.
   b) The activities in paragraph (a) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:
      i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
      ii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
      iii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
      iv) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.
40) **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 ACBDD and the minor.
41) **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.
42) **Protected Health Information, or PHI** – means individually identifiable information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Records of Individuals deceased for more than 50 years are not PHI. For the purposes of this manual, and the Agency's compliance program, PHI shall also include "Education Records" as defined by FERPA. This creates a consistent set of policies for both types of confidential information.
43) **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.
44) **Psychotherapy Notes –** means notes recorded (in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the

DRAFT

following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

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) **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
51) **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers. This definition includes the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
52) **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.
53) **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.
54) **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.
55) **User –** means a person or entity with authorized access.
56) **Violation**, **or violate** – means, as the context may require, failure to comply with a provision of either the HIPAA Privacy or Security rules, or a provision of state law relating to privacy, confidentiality or computer security.
57) **Workforce Member –** Workforce Member means the same as Employee. See definition above.
58) **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.

DRAFT

1010 Confidentiality – General Rules

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

POLICY
All information in an enrollee's records, including electronic information, is confidential. Further, all conversations involving individually identifiable information is confidential.
The ACBDD shall conform to all requirements for privacy and confidentiality set forth by the State of Ohio, the federal HIPAA, FERPA and IDEA regulations, and any other applicable law. Safeguards will be implemented for the use, disclosure, collection, storage, retention and destruction of individually identifiable information. The ACBDD shall not use or disclose individually identifiable information except in accordance with applicable requirements.

AUDIENCE
All Staff

AUTHORITY
45 CFR Part 160 and 45 CFR § 164 (current as/of 3/27/2013)
45 CFR § 164.504(g) for entities with multiple functions
ORC § 5126.044 Ohio law on confidentiality (effective 9/22/2000)
OAC 5123-4-01(O) Records [County Boards of DD P&P required for HIPAA and FERPA compliance]
45 CFR § 164.502(a)(1)(iii) incidental uses and disclosures
OAC § 3301-51-04 Confidentiality (effective 7/1/2014), for EI/Pre-School/School Age; see also:
- 34 CFR 99 FERPA (current as of 1/2012)
- 34 CFR 300 and 301 Part B IDEA (Individuals with Disabilities Education Act, ages 3-21)
- 34 CFR 303 Part C IDEA (Individuals with Disabilities Education Act, ages 0-2)
- 34 CFR 303.402 - 416 Early Intervention Confidentiality and Family Rights Provisions
- 34 CFR 300.610 - 627 Children with Disabilities Confidentiality and Parent Rights Provisions

NOTE ON KEY LANGUAGE USED IN THESE POLICIES AND PROCEDURES
These policies specify a mixture of mandatory behaviors, behaviors which are generally expected with exceptions permitted and optional processes and procedures. The following terminology is used:

Term	Meaning
Shall, must and/or will	All these terms indicate that the behavior is mandatory
Should	This term indicates the behavior is usually expected, although in certain situations it is not absolutely mandatory
May	This term indicates that an individual is empowered to take a specific action

PROCEDURES
1) Staff of the ACBDD may use or disclose PHI only as follows:
   a) For treatment, payment, health care operations and education. This includes disclosures to service providers for their treatment, payment or education, and to contracted Business Associates. This information is to be used by employees for Agency purposes for serving Individuals. In an exception, explicit parent authorization is required for any Medicaid billing for children.
   b) In accordance with a release or authorization of the Individual in accordance with policy and procedure set forth in Policy 1050 Authorizations.
   c) As permitted in Policy 1040 Speaking with the Family or Friends of an Individual Receiving Services.
   d) As permitted in Policy 1090 Disclosures that do Not Require an Authorization.
   e) To the Individual served.
2) For all of the above, the minimum amount of information should be disclosed, and specific procedures followed as detailed in 1020 Minimum Necessary Policy.
3) All employees are responsible for safeguarding the information regarding Individuals served by ACBDD, as

detailed in

a) Policy 1030 Confidentiality Safeguards (Oral & Written)
b) Policy 3080 Computer Usage
c) Policy 3082 Social Media Use
d) Policy 3085 Portable Computing Devices
e) Policy 3087 Employee Work at Home

4) Rights of Individuals served by ACBDD may be exercised by parents, guardians and personal representatives as detailed in Policy1070 Minors, Personal Representatives and Deceased Individuals.
5) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in Policy 1080 Duty to Report Violations and Security Incidents.
6) Supervisors, managers and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.

DRAFT

1020 Minimum Necessary Policy

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

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

AUDIENCE
All Staff

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

PROCEDURES

1) **FOR ALL EMPLOYEES**
   a) **Minimum Necessary Requirement**.
      i) **Basic Requirement**. When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, employees must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
      ii) **Exceptions**. The minimum necessary requirement does NOT apply to:
         (1) Disclosures to or requests by a health care provider for treatment
         (2) Uses or disclosures made to the Individual served, including but not limited to any requests for their records or requests for an accounting of disclosure
         (3) Uses of disclosures made pursuant to an Authorization
         (4) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations
   b) **Routine Requests or Disclosures.** Staff shall be familiar with and follow procedures detailed in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests when making requests for PHI or disclosures.
   c) **Procedures for Non-Routine Disclosures or Requests**
      i) **For non-routine disclosures**, when subject to the minimum necessary provision, the person making the disclosure will apply the minimum necessary principle. He or she may seek the guidance, if necessary, of the Privacy Officer (or his/her designee).
      ii) **For non-routine requests**, the requesting party will utilize the minimum necessary principle, seeking the guidance, if necessary, of the Privacy Officer (or his/her designee).
      iii) **Good Faith Reliance** – ACBDD staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:
         (1) The disclosure is made to a **public official**, permitted to receive information, and the public official represents that the request is for the minimum necessary information;
         (2) The request is from another **covered entity**;
         (3) The request is from a **professional** at ACBDD, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary information.
2) **FOR THE PRIVACY OFFICER**
   a) **Implementation Approach**. The Privacy Officer will implement the minimum necessary requirement with the steps detailed below. Measures to limit workforce access, and procedures for both routine disclosures and requests for PHI will be created and documented as detailed below:
   b) **Limiting Workforce Access to PHI**: Access to the PHI will be granted based on the employee's role and determined by the Director and Privacy Officer of ACBDD. ACBDD will identify:

DRAFT

i) Those persons or classes of persons, who require access to PHI to carry out their duties, in the workforce, including interns and trainees, will be listed according to job classification with the minimal necessary PHI required for successful job performance to serve the Individuals, and
ii) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
iii) Safeguards will be developed and documented to restrict workforce access to the minimum necessary, especially as detailed in Policy 3015 Facility Security and Access Control.
iv) The Privacy Officer will document the results of this analysis in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests. This report will be available for public inspection.

c) **Procedures for Routine Disclosures and Requests.** The HIPAA Privacy Officer will identify all routine disclosures made by Agency employees, for which the minimum necessary requirement applies, and create procedures to implement these. The same shall be done for routine requests for PHI. [Note that minimum necessary does not apply for disclosures or requests related to "treatment"; consequently, no procedures must be created in these situations.] These results shall be documented in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests.

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

DRAFT

1030 Confidentiality Safeguards (Oral & Written)

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

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

AUTHORITY
45 CFR § 164.530(c) – Administrative, Technical, and Physical Safeguards
34 CFR 99.31(a)(1)(ii) Safeguards
ORC § 5126.044 Ohio law on confidentiality
OAC § 3301-51-04 Confidentiality (effective 7/1/2014), for EI/Pre-School/School Age

PROCEDURES

1) **General Procedures**
   a) Employees shall be familiar with Appendix D Facility Security and Access Plan regarding staff, Individuals receiving services, parent and other visitor access to the facility.
   b) Visitors shall be required to sign-in and wear a visitor badge while on the premises. Employees shall escort visitors throughout the premises.
2) **Oral Privacy**
   a) Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings and using appropriate volume when speaking to prevent others from overhearing conversations.
   b) Employees shall refrain from holding conversations in common areas where Individuals receiving services or visitors can overhear PHI.
   c) Discussions concerning Individuals should be done in a private area and discussions must be limited to "need to know" information for purposes of providing the best services.
   d) Overheard conversations are not to be shared or repeated.
   e) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.
3) **Safeguards for Written PHI**
   a) **Control of Paper Records**
      i) Case and School records shall be kept locked and secured. Employees requiring access to these records shall have a key and/or combination for the storage room or cabinet.
      ii) Paper files shall be put away promptly when not being used.
      iii) Individual records shall be retained per Policy 54 Retention of Board Records.
   b) **Other use and storage of paper records**
      i) Employees shall 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 shall be taken to address and transmit fax to the proper recipient.
      iii) Faxed documents should not be left at a common fax machine.
   d) **Printing and Copying PHI**
      i) Printers and copiers used for printing of PHI shall 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.

DRAFT

iii) The Security Officer shall monitor all printer and photocopier acquisitions. In the event that this equipment includes internal storage devices, which retain images of photocopies made, the asset shall be managed by the IT department, especially upon disposal to ensure destruction of any PHI contained in its storage.

e) **Transportation/outside use of documents with PHI**
   i) Caseworkers and other employees who remove documents from the facility, to conduct fieldwork, for example, are responsible for safeguarding these documents.
   ii) When leaving documents unattended in a personal vehicle, the vehicle shall be locked. Preferably, the documents and/or their container shall not be visible.
   iii) If any documents with PHI are lost or stolen, the incident shall 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, shall be destroyed appropriately.

i) **Clean Desk Policy.** All employees should clean their desks of PHI whenever leaving their work area for a time, especially at end-of-day.

j) **Confidentiality with Cleaning Personnel**. Cleaning personnel with access to the facility shall be placed under a confidentiality agreement.

4) **Compliance Audits/Facility Review**. Annually or on another periodic basis, the HIPAA Privacy Officer or designee may audit staff compliance with these guidelines. The audit shall consist of a walk-through of the facility, with observations recorded, such as placement of desks, location of computer equipment, any papers with PHI that would be visible to a visitor, etc. The results shall be discussed with the appropriate employee, and any appropriate actions taken.

5) **Enforcement**. All supervisors are responsible for enforcing this policy. Employees who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

DRAFT

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

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

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

AUDIENCE
All Staff

AUTHORITY
45 CFR § 164.510(b)

PROCEDURES
1) **If the Individual is present**
   a) **Permitted disclosure to family or friend present**. If a family member, or friend of the Individual is present while services are being rendered, an employee serving the Individual may disclose PHI after one of the following:
      i) verbally seeking permission for the disclosure, and the Individual agrees; or
      ii) giving the Individual the opportunity to object to the disclosure, and the Individual does not express an objection; or
      iii) the staff member reasonably infers from the circumstances, based on the exercise of professional judgment, that the Individual does not object to the disclosure.
2) **If the Individual is not present**
   a) **Communications about the Individual's care**
      i) In the event of a phone call or other discussion with a family member or one involved with the care of the Individual being served by ACBDD, 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.

DRAFT

1050 Authorizations

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

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

AUDIENCE
All Staff

AUTHORITY
45 CFR § 164.508 – HIPAA requirements for authorizations
ORC § 3701.243 – Disclosing of HIV test results or diagnosis
ORC § 5126.044 – Ohio Statute on confidentiality of records
OAC § 3301-51-04(E) and (M) – Confidentiality for EI/School Age: records of disclosures, consent; see also:
34 CFR 99.30 – FERPA requirements for prior consents to disclose information
34 CFR 99.32 – FERPA recordkeeping requirements concerning requests and disclosures
42 CFR Part 2 – Confidentiality of records from federally-funded drug and alcohol abuse treatment centers

LEGAL NOTES
- OAC 3301-51-04, FERPA and IDEA applies for records created for EI, Pre-School, and School-Age; HIPAA applies to all other records. The term used in the FERPA regulations for the Release of Information form is "consent". The HIPAA term "authorization" is used in these policies.

PROCEDURES
1) **Valid Authorization**. Unless otherwise authorized by ACBDD policy and/or state or federal law, release of an Individual's records requires specific authorization by the Individual being served or his/her legal representative. A standard authorization form is included as an Appendix. If authorizations are received on other forms, note that a valid authorization must include the following:
   a) Full Name of the Individual.
   b) A specific description of the information to be released. For example, a range of dates, or category of record.
   c) The purpose or need for the disclosure.
   d) The name of the person or agency disclosing the information.
   e) Names of the person(s), or agency to whom the disclosure is to be made.
   f) The date, event, or condition upon which the authorization expires.
   g) Statement of the Individual's right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke.
   h) Statement that ACBDD 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) ACBDD is aware authorization has been revoked.
   e) ACBDD is aware information is false.

DRAFT

f) Authorizations to release PHI is combined with other documents.

3) **For authorizations presented in person for immediate release**, the staff member shall verify the identity of the recipient according to Policy 1060 Verification, after which the information may be released.
4) **Special Situations**. All staff should be aware of certain special situations. Records personnel shall be trained and shall follow legally-required and ACBDD procedures for all special situations, including:
   a) **HIV/AIDS Records**. Ohio Revised Code ORC 3701.243 specifies special procedures for release of HIV/AIDS test results or diagnosis which requires explicit authorization to release these records, plus a disclosure to the recipient regarding the prohibition of re-disclosure.
   b) **Records with names of other Individuals served**. If an Individual's records Include the name of another Individual served by ACBDD (such as an MUI report), the other Individual's name must be redacted prior to the release of the record.
   c) **Psychotherapy Notes**. See Policy 1000 for the definition of Psychotherapy Notes. Psychotherapy Notes may only be released when explicitly authorized. Psychotherapy Notes record releases require their own Authorization, that is, a release of Psychotherapy Notes may not be combine with any other request.
   d) **Records relating to Drug and Alcohol Abuse Treatment**. Any records obtained by ACBDD from a federally-funded drug and/or alcohol abuse treatment facility are subject to 42 CFR Part 2 regulations. 42 CFR Part 2 mandates specific language on the authorization, and further requires that recipients of the records be notified regarding the prohibition of re-disclosure without the Individual's consent.
5) **Proper Completion of Authorization Form by Staff**. The staff person handling the request should complete the following steps, and annotate the bottom of the Authorization Form:
   a) The employee should write their name on the completed authorization form.
   b) The original signed authorization shall be saved in the Individual's master record, and a copy must be given to the Individual.
   c) A record of the release shall be maintained in the Individual's record, using the Disclosure Log included as an Appendix, detailing the following information:
      i) The date of the disclosure.
      ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
      iii) A brief description of the PHI disclosed.
      iv) A brief statement of the purpose of the disclosure.
      v) If the disclosure was due to a health or safety emergency, a description of the significant threat to health or safety.
6) **Retention Period for Written or Electronic Copy of Authorization**. The ACBDD 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. This may serve as the required record of access per OAC 3301-51-04(E).
7) **Revocation of Authorization.** Upon instructions of revocation of authorization, ACBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.
8) Note that information from other service providers contained in the Individual's record may be released with the Individual's written authorization.

DRAFT

1060 Verification

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

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

AUDIENCE
All Staff

AUTHORITY
34 CFR 99.31(c) Verification
45 CFR § 164.514(h) Verification

PROCEDURES

1) **REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY**
   a) **Verifying Identity and Authority**. In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI, ACBDD personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing PHI:
      i) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI.
      ii) Presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person.
      iii) A written statement on appropriate government letterhead that the person is acting under the government's authority.
      iv) Other evidence of documentation from an agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
      v) A written statement of the legal authority under which the information is requested.
      vi) If a written statement would be impracticable, an oral statement of such legal authority.
      vii) A request that is made pursuant to a court order and subpoena or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority.
   b) The following issues should be addressed before releasing PHI once a request is received:
      i) Is the requestor who she/he claims to be?
      ii) Does the requestor have the authority to request PHI. If the request involves a court order, subpoena, or other legal request, follow the procedures outlined in the Policy 1090 Disclosures that do Not Require an Authorization.

2) **REQUESTS FROM AN INDIVIDUAL RECEIVING SERVICES, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE**
   a) A properly completed, valid Authorization per the specifications in Policy 1050 Authorizations is sufficient verification of the identity and authority of the person requesting information.
   b) For requests for information other than formal record releases, staff must first verify both the identity and the authority of the person prior to releasing PHI:
      i) If the person is known to the staff person, this is sufficient verification of identity.
      ii) Identity can be verified by questioning the person regarding their knowledge of information in the record of the Individual being served, such as birth date, social security number, etc., which only an authorized person would typically know.
      iii) For requests from someone other than the Individual or the parent of a minor, the person's authority to obtain information must also be verified. For example, a healthcare Power of Attorney and/or statement from the Individual that the requestor is a HIPAA Personal Representative would

DRAFT

demonstrate proper authority. See also Policy 1040 Speaking with Family and Friends of an Individual Receiving Services for situations where it may be permissible to give information to a family member.

DRAFT

1070 Minors, Personal Representatives and Deceased Individuals

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

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

AUTHORITY
ORC 5126.044 Confidentiality
ORC 3319.321(4) Confidentiality and Parental Rights of Access to Student Records
ORC 3109.051(H) Parenting Time – companionship rights
ORC 1337.13 Authority of attorney under durable power of attorney for health care
45 CFR § 164.502(g)(1) Personal representatives
45 CFR § 164.502(g)(2) Adults and emancipated minors
45 CFR § 164.502(g)(3) Unemancipated minors
45 CFR § 164.502(f) Deceased Individuals
45 CFR § 164.510(b)(5) Uses and disclosures when the individual is deceased

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

PROCEDURES
1) **Rights of legally Consenting Minors**. Individuals being served, who are minors, and who are legally allowed to consent to treatment under Ohio Law may exercise all rights regarding access to, requests for amendment to, and release of their PHI pursuant to a written authorization.
2) **Rights of an Individual's Personal Representative**. ACBDD 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 ACBDD Authorization Form which permits release of PHI.
3) **Recognized Personal Representative**. ACBDD recognizes the following persons to be personal representatives:
   a) The parent of a child younger than 18 years old
   b) The non-custodial parent of a child younger than 18 years old (ORC 3319.321 and ORC 3109.051(H)), unless the custodial parent presents ACBDD a court order restricting the non-custodial parent's access. In the event that ACBDD is presented with such a court order, ACBDD shall adhere to the terms of that order.
   c) A person who is recognized through durable power of attorney to have authority to act on the behalf of the Individual (ORC § 1337.13)
   d) The legal guardian of the Individual
   e) Any other person authorized by law except in Abuse, Neglect, and/or Endangerment situations, or where ACBDD 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, ACBDD may elect not to recognize a person as a personal representative of an Individual. In order for ACBDD to choose not to recognize a person as a personal representative, ACBDD 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 ACBDD 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, ACBDD shall adhere to the restrictions in the court order.

4) **Deceased Individuals**

a) **Disclosure of PHI After Death**. PHI generated during the life of an Individual is protected from disclosure after death unless disclosure is for treatment or payment, quality assurance or other auditing or program review functions. ACBDD and its employees cannot release PHI regarding a deceased Individual unless a valid personal representative has been established and has requested the PHI through the proper authorization process.

b) **Disclosure of PHI to Administer Estate**. Upon request, PHI shall be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate (ORC § 5126.044).

c) **Disclosure to Guardian or next-of-kin:**. Upon request, the Agency shall release records regarding an Individual served to the guardian at time of death. Absent a guardian, records may be released to the next of kin:

i) The Individual's Spouse (if married)

ii) The Individual's children

iii) The Individual's parents

iv) The Individual's brothers or sisters

v) The Individual's uncles or aunts;

vi) The Individual's closest relative by blood or adoption

vii) The Individual's closest relative by marriage

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

DRAFT

1080 Duty to Report Violations

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

POLICY
Confidentiality of PHI is taken very seriously at ACBDD. Employees are required to follow all mandates detailed in these policies. Any employee who becomes aware of a violation of any policy in this *Confidentiality and Computer Security Policies* manual is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

AUTHORITY
HIPAA Privacy Rules, 45 CFR § 164
45 CFR § 164.530(e)(1) – Sanctions

PROCEDURES
FOR ALL EMPLOYEES
1) **Employees Duty to Report Violation**. Any employee observing a violation of any of the Confidentiality and Computer Security policies is to report the violation to his/her supervisor. Failure to report a violation is a disciplinable offense.

FOR SUPERVISORS AND THE PRIVACY AND/OR SECURITY OFFICER
2) **Investigation.** The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, Individuals receiving services, or others, and/or review of computer or paper audit trails.
3) **Procedure for Data Breach.** For potential data breaches, the Privacy and/or Security Officer will follow any procedures detailed in Policy 3035 Breach Reporting.
4) **Procedure for Privacy Violation.** For Privacy Violations, the Privacy Officer will follow procedures in Policy 3065 Mitigation.
5) **Filing of Written Report by Privacy and/or Security Officer.** A written incident report will be written by the Privacy and/or Security Officer. It will be filed in:
   a) the Privacy Officer's Privacy Violations file; and
   b) the employee's personnel file.
6) **Employee Discipline**, if appropriate, will be taken and documented in accordance with the following policy:
   - 8.1 Disciplinary Process – Unclassified Employees
   - 8.2 Disciplinary Process – Classified Employees
   - 8.5 Progressive 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.

DRAFT

1090 Disclosures that do not Require an Authorization

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

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

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

AUTHORITY
45 CFR § 164.512
34 CFR 99.31
34 CFR 99.36
ORC § 2151.421(A) Reports of Child Abuse
ORC § 2305.51 Disclosures to prevent harm to 3rd parties
ORC § 2317.02(B) Privilege for physicians, school guidance counselors, licensed social workers and licensed counselors
OAC § 3301-51-04 (E)(Q) Confidentiality (effective 7/1/2014), for EI/Pre-School/School Age; see also:
ORC § 4732.19 Privilege for psychologists
ORC § 5123.19 Licensure activities of DODD
ORC § 5123.60 OLRS
ORC § 5123.61(C)(1) Duty to report abuse/neglect of persons with DD
ORC § 5126.044 Confidentiality for DD Boards
ORC § 5126.055 LMAA functions of DD Boards
ORC § 5126.31 Case Review and Investigation
OAC § 5123:2-17-02(B) Incidents adversely affecting health/safety
OAC § 5123:2-17-02(D) Reporting MUIs
OAC § 5123:2-3-04 Monitoring of licensed facilities
Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena
ORC § 4113.52 Reporting Violations of law by employer or fellow employee
34 CFR Part 99 Subpart D May an Educational Agency Disclose Education Records
20 U.S.C. 7165(b) Section 4155(b) No Child Left Behind Act – Transfer of Disciplinary Records
OAC 3301-51-04(Q) Disciplinary Information

LEGAL NOTES

- ORC § 5126.044 does not authorize any of the excepted disclosures detailed in HIPAA and FERPA. Other Ohio regulations reference disclosures otherwise allowed by federal and state law. HIPAA preempts contrary state

DRAFT

law, except where state law offers greater privacy protections, greater rights of access to an Individual's records, or is less coercive. Consult your county prosecutor for review and approval of this policy.

- HIPAA and FERPA/IDEA maintain overlapping but different lists of disclosures permitted without authorization or parental consent. We use the term "Education Records" below to refer to FERPA/IDEA permitted disclosures, and "PHI" regarding HIPAA permitted disclosures.

PROCEDURES

ACBDD 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. [45 CFR 164.528, OAC 3301-51-04(E)] Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.
2) **When required by law**
   a) To officials at another school that an Individual served by the Agency intends to enroll in, or is already enrolled in, for the purposes of Individual's enrollment or transfer. Any such disclosures must include records of any disciplinary actions, particularly the circumstances that resulted in the disciplinary action and relevant information to the safety of the child and others. A description of the disciplinary action taken must be included if the disciplinary action was taken because the child possessed a weapon on premises, knowingly possessed controlled substances on premises, or inflicted serious bodily to another on premises. (OAC 3301-51-04(Q) Disciplinary Information)
   b) The ACBDD may use or disclose PHI or Education Records to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
   c) For compliance with mandatory disclosures related to sex offenders
3) **For public health purposes** PHI may be used or disclosed to:
   a) A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions.
   b) A public health or other government authority authorized by law to receive reports of child abuse or neglect.
   c) A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance.
   d) A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.
4) **To protect victims of abuse, neglect, domestic violence or other crime**
   a) **Reports of child abuse**
      i) Reports of child abuse shall be made in accordance with Ohio law.
      ii) The ACBDD 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 ACBDD 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 ACBDD 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 ACBDD 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 ACBDD would be informing a personal representative, and the ACBDD 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 ACBDD, in the exercise of professional judgment.

5) **For health or education oversight activities such as investigations, audits, and inspections**
   a) PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.
   b) Specifically excluded from this category are investigations of an Individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.
   c) PHI may be used and disclosed to receive and review reports of incidents, and to conduct investigations as authorized by ORC 5126.055(A)(6), 5126.31, 5126.311, 5126.312 and 5126.313.
   d) Education Records may be disclosed to the Comptroller General of the US, Attorney General of the US, Secretary of Education and/or State of Ohio Education authorities subject to the requirements of 34 CFR 99.35 or to state officials involved with juvenile justice in accordance with 34 CF 99.38.
6) **To accrediting organizations**
   a) Information in Education Records may be disclosed to accrediting organizations without parental consent. For any disclosure of PHI, a HIPAA Business Associate agreement should be in place with the accrediting organization.
7) **For judicial and administrative proceedings**
   NOTE: These policies do not detail all situations such as grand juries and other infrequent legal proceedings. Consult with legal counsel prior to disclosure for any unusual situations!
   HIPAA-specific provisions: The following provisions apply for records of adult (over 18) services:
   a) The ACBDD 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 ACBDD may comply with such legal requests only if:
      i) The ACBDD makes reasonable effort to notify the parent involved and/or receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the Individual who is the subject of the requested PHI has been given notice of the request; or
      ii) The ACBDD 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 ACBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements of HIPAA, FERPA, IDEA and/or OAC 3301-51-04.
8) **For law enforcement purposes**
   a) **Conditions Allowing for Disclosure of PHI to Law Enforcement**. PHI may be disclosed for the following law enforcement purposes and under the specified conditions:
      i) Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; or commission of a felony, subject to any exceptions set forth in applicable law.
      ii) Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.
      iii) The ACBDD may disclose to a law enforcement official protected health information that the ACBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the ACBDD.
   b) **Reporting Commission and Nature of Crime.** HIPAA and Ohio Regulations for School-Age differ in their specifications.
      i) **HIPAA specifications for reporting of crimes:** 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:
         (1) Name and address
         (2) Date and place of birth
         (3) Social security number

(4) ABO blood type and RH factor
(5) Type of injury
(6) Date and time of treatment
(7) Date and time of death, if applicable,
(8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos

ii) FERPA / IDEA Part B / OAC 3301-51-04 specifications for reporting of crimes: DD boards may report crimes committed by school-age individuals served. See FERPA 99.8(c)(1) and OAC 3301-51-04(R).

c) **Compliance/Enforcement of privacy regulations**: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

9) **To coroners, medical examiners, and funeral directors**

a) PHI may be disclosed to coroners, medical examiners and funeral directors, as necessary for carrying out their duties.

10) **Organ, eye or tissue donation**

a) PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.

11) **To reduce or prevent a serious threat to public health and safety and/or safety of person(s)**

a) The ACBDD may disclose PHI or Education Records as follows, to the extent permitted by applicable law and ethical standards:

i) **Good Faith.** PHI may be used or disclosed if the entity believes in good faith:

(1) that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat; or

(2) the disclosure is to law enforcement authorities to identify or apprehend an Individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.

b) **Disclosure of Individual's Admitted Participation in a Violent Crime**. Disclosures of admitted participation in a violent crime are limited to the Individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.

c) **Disclosure of Individual's Admitted Participation in a Violent Crime Learned in the Course of Treatment**. Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the Individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

12) **Specialized government functions**

a) **National Security and Intelligence**: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, Counterintelligence, and other activities authorized by the National Security Act.

b) **Protective Services**: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.

c) **Correctional Institution or Law Enforcement Official.** The ACBDD may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other Individual protected health information about such inmate or Individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

i) The provision of health care to such Individuals;
ii) The health and safety of such Individual or other inmates;
iii) The health and safety of the officers or employees of or others at the correctional institution;
iv) The health and safety of such persons and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
v) Law enforcement on the premises of the correctional institution; and
vi) The administration and maintenance of the safety, security, and good order of the correctional institution.

The provisions of this section do not apply after the Individual is released from custody.

DRAFT

d) **Public Benefits**: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

13) **In connection with "whistleblowing"**. In connection with "whistleblowing", or reporting of a violation of law or ethics, an employee of ACBDD may disclose PHI to his/her attorney, and to other parties specified in Ohio Revised Code § 4113.52, while following the procedures outlined in that statute. See also Policy 10.5 Protection of Whistleblowers.

14) **For workers' compensation or other similar programs if applicable**.
    a) PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

DRAFT

INDIVIDUAL RIGHTS

1200 Individual's Right to Access Records

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

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
45 CFR § 164.524(e) individual's right to access PHI
45 CFR § 164.524(b) Time limits on response to access
45 CFR § 164.524(c) Form of access
34 CFR 99.4 Rights of Parents
34 CFR 300.613(c) IDEA Rights of parents
ORC § 1347.08(A)(2) individual's right to access records
OAC § 3301-51-04 Confidentiality, for Education of Students with Special Needs

LEGAL NOTES
- State laws, HIPAA, and FERPA all provide that Individuals receiving services have access to their records.

PROCEDURES
1) **Parent Information Rights.** Per Ohio law, the following information shall be documented in Appendix E and available to parents:
   a) **Types & Locations of Education Records.** A list of the types and locations of education records collected, maintained, or used by ACBDD must be provided to the parent/guardian of an Individual served upon request, unless rights of the parent/guardian have transferred to the Individual served. [OAC 3301-51-04(G)]
   b) **Names and Positions of employees with access to Personally Identifiable Information (PII).** The agency shall maintain a current listing of the names and positions of employees who may have access to PII of children (individuals served who are under age 18). [OAC 3301-51-04(N)]
2) **Who May Access Records**
   a) An Individual served by the Agency above the age of 18, the parent/guardian of a child, the guardian of an adult not able to act on their own behalf, or any "personal representative" of an Individual served may access the records. See Policy 1070 Minors, Personal Representatives and Deceased Individuals.
   b) **3rd Party Review.** An Individual or parent may include any 3rd party of their choosing, including an attorney, to review the records.
   c) **Presumption of Parental Right to Access Records.** ACBDD 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.
3) **Procedure, form and method of access**
   a) **Requests for Access.** Requests for access to records shall be directed to the Privacy Officer or his/her designee.
   b) **Verification Procedure.** The Privacy Officer shall follow the Verification Procedure to verify the identity of the requestor. For any grant of access to someone other than the parent, the authority of the requestor to access the information shall also be verified. This might include documentation of guardianship or documentation that the person was appointed a "Personal Representative" under HIPAA.
   c) **Redaction of Confidential Information**. Prior to release, Agency staff shall redact any confidential information, including any names of other Individuals served. [OAC 3301-51-04(F)]

DRAFT

d) **Forms of Access Requested by the Individual**. The ACBDD shall provide the Individual with access to their records in any of the following ways requested by the Individual:
   i) **By inspection**. ACBDD shall provide a private room for the Individual to review the records under the supervision of a ACBDD staff member who will ensure that the record is not altered.
   ii) **Photocopy**. ACBDD shall provide a photocopy of the entire record or portion of the record requested.
   iii) **Electronic format**. ACBDD shall provide an electronic copy of the information requested if this is feasible; if not, the Security Officer or his/her designee shall negotiate an electronic format and transmission method acceptable to both parties and fulfill the request.
      1) If the Individual requests the information via email and only unsecured email is available, the Individual shall be notified that this method is subject to electronic eavesdropping. If the Individual is willing to accept the risks, the info shall be sent via email.
      2) The Agency shall honor requests for commonly used media, such as USB Flash drives.

e) **Record of Parties Accessing Records.** The Privacy Officer or his/her designee shall maintain a record of all parties who request access to records (including staff) including the name of the party, the date access was given, and the purpose of access. ACBDD shall maintain an appropriate system for maintaining these records.

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

5) **Time for response to request for access**
   a) Access shall be granted without unnecessary delay. In particular, requests should be honored prior to any scheduled IEP meeting, hearing, or administrative procedure. Requests in all cases shall be honored within 30 days.

6) **Fees for copying/electronic media**
   a) ACBDD at present has no fees for photocopies, postage or electronic media used to provide records.

DRAFT

1210 Individual's Right to Request Amendment of Records

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

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
45 CFR § 164.526(f) Individual's right to request amendment
OAC § 3301-51-04(I), (J), (K), (L) Confidentiality, for Education of Students with Special Needs
ORC § 1347.09 Disputing of Records
34 CFR 99.20 FERPA – Requesting amendment of records
34 CFR 99.21 FERPA – Rights to a Record Hearing
34 CFR 99.22 FERPA – Requirements for a Records Hearing

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

PROCEDURES
1) **REQUESTS FOR AMENDMENTS**
   a) **Amending Statements Believed to be Inaccurate, Misleading or in Violation of Individual's Rights.** An Individual 18 years or older, 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 ACBDD or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
   b) **Responsibility of Privacy Officer**. The Privacy Officer of the ACBDD is responsible for receiving requests for amendment, processing the requests, arranging for any hearings, and completing required documentation.
   c) **Time to Act on a Request for Amendment.** The ACBDD will act on a request for amendment without unnecessary delay and no later than 60 days after the date of the request.
   d) **Accepted Request for Amendments.** If the ACBDD accepts the requested amendment, in whole or in part, ACBDD must make the appropriate amendment, and inform the Individual and other persons or entities who have had access to the information.
   e) **Denied Request for Amendments**. Otherwise, if the ACBDD believes the existing record is correct as is, it may deny the amendment:
      i) **Written Notice.** If an amendment is denied, the ACBDD will give written notice in plain language which includes the following:
         (1) The basis for the denial;
         (2) The Individual's right to submit a written statement disagreeing with the denial and how the Individual may file such a statement;
         (3) A statement that, if the Individual does not submit a statement of disagreement, the Individual may request that the ACBDD provide the Individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
         (4) The Individual's right for a hearing to challenge the information.
      ii) **Statement of Disagreement.** If the Individual submits a statement of disagreement, the Privacy

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

iii) **Written Rebuttal.** The ACBDD may prepare a written rebuttal to the Individual's statement of disagreement. Whenever such a rebuttal is prepared, the ACBDD must provide a copy to the Individual who submitted the statement of disagreement.

iv) **Permanent Record.** The inserted statement of disagreement and any rebuttal become a part of the permanent record and must be included with all future disclosures of the covered records.

f) **Individual's Request for Copy of Changed Record.** At the Individual's request, ACBDD will send a copy of the changed record to any party requested by the Individual (per ORC 1347.09).

g) **Separate Transmission of Information in EDI Format**. If the disclosure which was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, the ACBDD may separately transmit the information to the recipient of the transaction in a standard EDI format.

2) **RECORDS HEARINGS**

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

a) **Hearing Procedures**

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

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

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

iv) To conduct the hearing, the Privacy Officer may appoint any person, including an official of ACBDD, who does not have a direct interest in its outcome.

v) During the hearing, the parent shall have a full and fair opportunity to present evidence relevant to their objection. The Individual or parent may obtain assistance of any person(s), including an attorney hired at their own expense, to assist them.

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

vii) The decision shall be documented in writing, within a reasonable time of the hearing, and shall include a summary of the evidence presented and the reasons for the decision.

b) **Results of Hearing**

i) If, as a result of the hearing, ACBDD decides that the information in its records is inaccurate, misleading, or otherwise in violation of the privacy or other rights of the Individual, it must amend the information accordingly and inform the Individual in writing.

ii) If, as a result of the hearing, ACBDD 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 ACBDD.

iii) Any information placed in the record as a result of this hearing, ACBDD must maintain this statement as part of its permanent record and include it with any subsequent disclosure.

DRAFT

1220 Individual's Right to Receive an Accounting of Disclosures

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

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
45 CFR § 164.528
45 CFR § 164.528(d) Individual's right to an accounting of disclosures of PHI
34 CFR 99.32 FERPA Recordkeeping requirements concerning requests and disclosures

PROCEDURES

1) **Proper Records.** The Privacy Officer shall be responsible for insuring that proper records are kept to allow for proper and complete responses to any requests for accountings of disclosures. See also procedures listed in 1090 Disclosures that do not Require an Authorization and 1050 Authorizations which detail the use of the Disclosure Log.
2) **Individual's Right to Request Accounting of Disclosures of PHI.** Generally, an Individual has the right to request an accounting of disclosures of their PHI by ACBDD and its business associates during a time period of up to six years prior to the date of the Individual's request. Most disclosures are **not** required to be included in the accounting. The types of disclosures which are **not** required to be accounted for are:
   a) For the purposes of treatment, payment and health care operations (45 CFR § 164.502);
   b) To the Individual receiving services, or to a parent, guardian or personal representative, of the Individual's own PHI (45 CFR § 164.502);
   c) Incidental disclosures, as detailed in (45 CFR § 164.502);
   d) Pursuant to an authorization (45 CFR § 164.508);
   e) To persons involved in the Individual's care or other notification purposes (45 CFR § 164.510);
   f) For national security and intelligence purposes, as detailed in (45 CFR § 164.512(k)(2);
   g) Disclosures to prisons and other law enforcement agencies regarding an Individual who is in custody, as detailed in (45 CFR § 164.512(k)(5).
3) **Employee Documentation of Disclosures.** Any employee who makes a disclosure other than listed above shall document the disclosure in the Individual File, with all information described in step 6B below. More specifically, the following types of disclosures must be documented:
   a) To public health authorities
   b) Birth and death reporting
   c) To law enforcement regarding crime on premises
   d) To law enforcement in emergencies where crime is suspected
   e) For cadaveric organ, eye, tissue donation purposes
   f) For judicial and administrative proceedings
   g) For research with an IRB waiver
   h) To military command authorities
   i) For Workers Comp purposes
   j) To correctional institutions except as detailed in 2G above
   k) About decedents to medical examiners, funeral directors, coroners
   l) For public health activities
   m) About victims of abuse
   n) Regarding child abuse or neglect
   o) To the FDA
   p) To a person who may have been exposed to a communicable disease

DRAFT

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 ACBDD does not charge a fee for accountings.
6) **The written accounting must meet the following requirements**:
   a) All disclosures of the Individual's PHI during the 6 years prior to the request (or such shorter period as is specified in the request) as stated above.
   b) As to each disclosure, the accounting must include:
      i) The date of the disclosure.
      ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
      iii) A brief description of the PHI disclosed.
      iv) A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure.
      v) If during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period, and the date of the last such disclosure during the accounting period.
      vi) If the accounting request includes school records, consult legal counsel regarding the need to obtain records of redisclosures by state or local school officials (see 34 CFR 99.32).
   c) ACBDD 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.

DRAFT

1230 Individual's Right to Request Additional Restrictions

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

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
45 CFR § 45 CFR § 164.522(a)

PROCEDURES
1) **Refer the Request to ACBDD' Privacy Officer or Designee:** All requests for additional restrictions on the use or disclosure of PHI will be referred to the HIPAA Privacy Officer, or his/her designee. Upon receiving a request, the Privacy Officer shall consider the following factors, in the decision to grant or deny the request:
   a) Whether the restriction might cause the organization to violate applicable federal or state law;
   b) Whether the restriction might cause the organization to violate professional standards, including medical ethical standards;
   c) Whether ACBDD' 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 ACBDD will agree**: The ACBDD 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:** ACBDD will notify the Individual of its final decision (whether approving or denying the request) in writing. The notice will be maintained in the Individual's record.
   a) Granting the Request: If ACBDD agrees to the restriction, the notice to the Individual will clearly state what restriction ACBDD 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 ACBDD 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 ACBDD 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 ACBDD' 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.

DRAFT

1240 Individual's Right to Request Confidential Communications

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

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

AUTHORITY
45 CFR § 164.502(h) Confidential communications
45 CFR § 164.522(b) Confidential communications requirements

AUDIENCE
Privacy Officer

PROCEDURES
1) **Individual's Right to Request Confidential Communications**. Individuals, or their personal representative, may make a request for confidential communications in writing to the Privacy Officer.
2) **Receiving a Request.** When the Privacy Officer receives a request, the Privacy Officer may not ask the reason for the request. The Privacy Officer shall contact the Individual making the request to obtain an alternate means of contacting them (e.g. cell phone, PO Box, etc.). The Individual will be informed at that time of steps ACBDD 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.

DRAFT

1250 Individual's Right to Notice of Privacy Practices

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

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

AUTHORITY
45 CFR § 164.520 Notice of privacy practices for protected health information
45 CFR § 164.502(i) Uses and disclosures consistent with Notice
OAC 3301-51-04(C) Confidentiality for EI/Pre-School/School Age; See also:
- 34 CFR 99.7 Notice (FERPA)
- 34 CFR 300.612 Notice (IDEA Part B)
- 34 CFR 303.404 Notice (IDEA Part C)

ORC § 1347.08(A)(3) (Personal Information Systems)
34 CFR 99.7 FERPA Annual Notification

LEGAL NOTES
OAC 3301-51-04(C) /FERPA / IDEA require an annual Notice. HIPAA requires a one-time Notice, with redistribution upon change. HIPAA requires signed acknowledgement of receipt.

AUDIENCE
Privacy Officer

PROCEDURES
1) **Drafting of Notice**. The Privacy Officer shall draft a Notice which is compliant with the requirements of the HIPAA, FERPA and IDEA regulations as well as OAC 3301-51-04(C). This shall include translations as necessary based on the language needs of the Individuals served. Further, the Notice shall be consistent with the Agency's privacy practices as detailed in these policies. Notice is detailed in the Notice of Privacy Practices.
2) **Updating Notice.** The Privacy Officer shall update the Notice as necessary based on changes in the Agency's privacy policies and/or the legal requirements as necessary. Upon update, the website and Notices posted at each facility (see below) shall be updated. Additionally, an updated copy will be provided to all Individuals receiving services and/or parents.
3) **Distribution of Notice.** The Privacy Officer shall ensure that Agency procedures are maintained to ensure appropriate distribution of Notice:
   a) All adults at intake will be given a copy of the Notice of Privacy Practices. At the time that the Notice is provided, the Individual or guardian shall sign an acknowledgement of his or her receipt of this Notice as part of the intake/transition of rights paperwork. This acknowledgement will be retained as part of the permanent record, for compliance with HIPAA requirements.
   b) For children (under age 18) a copy of the Notice shall be provided annually to the parent or guardian.
   c) For children (under age 18), the Agency shall coordinate with the appropriate education authority to ensure that the notice, "A Guide to Parent Rights in Special Education" (formerly "Whose IDEA Is This?"), is distributed annually.
   d) An additional copy of the Notice shall further be provided upon request by an Individual or parent.
4) **Posting of Notice.** The Privacy Officer shall ensure that the Notice is posted:
   a) **Website.** On the Agency's website.
   b) **At Each Facility.** At each facility, in a place where Individuals served can be reasonably expected to see the Notice, such as the reception areas of all Agency facilities.
   c) Copies of the Notice will be maintained for 6 years, as detailed in Policy 54 "Retention of Board Records.

REFERENCE
http://education.ohio.gov/Topics/Special-Education/A-Guide-to-Parent-Rights-in-Special-Education

DRAFT

CONFIDENTIALITY POLICIES FOR SUPERVISORS

1300 Business Associate Contracts

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

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

AUTHORITY
45 CFR 160.103
45 CFR § 164.502(e)
45 CFR § 164.504(e)
34 CFR 99.31(a)(1)(i)(B)
ORC § 5126.044 – Ohio Statute on confidentiality of records

PROCEDURES
1) **Business Associate Contract or Memorandum of Understanding.** ACBDD will have a written Business Associate Contract with every Business Associate. For a COG or other government agencies, a Memorandum of Understanding will be executed. See Appendix A Identifying Business Associates.
2) **Annual Review of all Contractual Relationships.** On an annual basis, the HIPAA Privacy Officer will review all contractual relationships to verify that up-to-date Business Associate contracts are in place.
3) **Satisfactory Assurances.** The Business Associate Contract will provide satisfactory assurances that the Business Associate will not use or disclose the PHI of ACBDD 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 ACBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, ACBDD will take steps to cure the breach or end the violation. If ACBDD is unable to cure the breach or end the violation, ACBDD will terminate the Business Associate Contract.

DRAFT

1320 Non-intimidation and Non-retaliation

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

POLICY

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

PROCEDURES

1) **ACBDD will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:**
   a) **Individuals Receiving Services**. Any Individual for the exercise by the Individual of any right under, or for participation by the Individual in any process established by the HIPAA regulations;
   b) **Individuals Receiving Services and others**. Any Individual receiving services, or other person for:
      i) Filing of a complaint with the Secretary of HHS regarding a HIPAA issue;
      ii) Testifying, assisting or participating in an investigation, compliance review, proceedings or hearing under Part C of Title XI; or
      iii) Opposing any act or practice made unlawful by the HIPAA regulations, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information.
2) **Retaliatory action is defined as doing any of the following**:
   a) Removing or suspending the employee from employment;
   b) Withholding from the employee salary increases or employee benefits to which the employee is otherwise entitled;
   c) Denying the employee a promotion that would have otherwise been received;
   d) Transferring or reassigning the employee;
   e) Reducing the employee in pay or position.
3) **Non-retaliation statement**. A person who in good faith brings a complaint will not be subject to retaliation. Retaliation against any person who falls within this definition, either Individual served or staff member of ACBDD, is strictly prohibited.
4) **Prohibition against Waiver of Rights**. No office, program, facility or employee of the ACBDD shall require Individuals to waive any of their rights under HIPAA as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits. The Agency may require parents of children under age 18 receiving services reimbursed by Medicaid to sign an authorization granting the Agency permission to bill Medicaid.
5) ACBDD will also follow Policy 10.5 Protection of Whistleblowers as appropriate.

DRAFT

1330 HIPAA Assignments and Documentation

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

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

AUTHORITY
Federal Law 45 CFR § 164.530(j) – Documentation requirement,
45 CFR § 164.520(e) – Notices of Privacy Practices;
45 CFR § 164.524(e) – Access of individuals to protected health information;
45 CFR § 164.526(f) – Amendment to protected information;
45 CFR § 164.508(b)(6) – Uses and disclosures for which an authorization is required;
45 CFR § 164.512(i)(2) – Uses and disclosures for research purposes;
45 CFR § 164.522(a)(3) – Rights to request privacy protection for protected health information;
45 CFR § 164.528(d) – Accounting of disclosures of protected health information – Implementation specification
ORC § 5126.044(E) (General records of DD Boards)
OAC 3301-51-04(N) Confidentiality Safeguards

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

PROCEDURES
1) **Designating a Privacy Officer and Other Individuals to Assist HIPAA Committee.** The superintendent shall designate a person to be the Privacy Officer, who is responsible for development, implementation, enforcement, and update of HIPAA Privacy policies and procedures. This individual shall be accountable for ensuring the confidentiality of any personally identifiable information. [per OAC 3301-51-04(N)] The superintendent may also designate other persons to assist, a HIPAA committee, which may include representatives from each department (e.g., administration, SSA, information systems, children's services).
2) **Documenting Records Covered by HIPAA and FERPA**. The records covered by HIPAA and FERPA shall be detailed and documented following the procedures for the "Designated Record Set" of the HIPAA regulations.
3) **HIPAA Mandated records**. HIPAA Mandated records include the following:
   a) HIPAA Required designations, including, Hybrid entity designation if applicable, description of records in Designated Record Set, the names of staff responsible for duties of Privacy Officer, receiving HIPAA complaints, providing access to Individual records, receiving requests for amendment of Individual records, answering questions about HIPAA policies and procedures. See Appendix F.
   b) Notice of Privacy Practices, as described in Policy 1250 Individual's Right to Notice of Privacy Practices, and signed acknowledgements that Individuals served have received a copy of the notice.
   c) Restrictions on use or disclosure of PHI agreed to by ACBDD as described in the Policy 1230 Individual's Right to Request Additional Restrictions.
   d) Records of disclosures, as required by the Policy 1220 Individual's Right to Receive an Accounting of Disclosures.
   e) Any signed authorization as described in Policy 1050 Authorizations.
   f) All privacy-related complaints received, and their disposition, if any, as described in Policy 1340 Privacy Complaints.
   g) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Policy 1080 Duty to Report Violations and Security Incidents.
   h) Incident Reports and other documentation specified by Policy 3035 Breach Reporting and Policy 3090 Security Incident Response and Reporting.

i) Records detailed in Policy 3000 Security Management Process, including the formal Security Risk Assessment, records that this was reviewed by all decision makers, and risk management actions taken.
j) Training records maintained in accordance with Policy 1350 Policy Updating and Staff Training.

4) **Policy and Procedure Audit Trail**. An audit trail of policies shall be maintained to allow identification of all policies that have been in place for the last six years.
5) **Updating Required Designations**. The Privacy Officer will maintain and update HIPAA Required Designations as necessary.
6) **Compliance Notes**. The Privacy Officer and Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, and internal audit activities.
7) **Internal Audit**. The Privacy Officer shall conduct a periodic audit, as necessary, to ensure proper maintenance of all documentation itemized in this policy.
8) See also Policy 54 Retention of Board Records for retention periods and destruction procedures.

DRAFT

1340 Privacy Complaints

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

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

AUDIENCE
All Staff

AUTHORITY
45 CFR § 164.530(d) HIPAA complaint procedures
ORC § 5123.64(A) requires establishment of a complaint procedure
OAC § 5123:2-1-12 administrative resolution of complaints involving the programs, services, policies, or administrative practices of a county board or the entities acting under contract with a county board

PROCEDURES
1) **The HIPAA Privacy Officer shall manage this complaint process**, and shall be designated in the Notice of Privacy practices as the person to receive complaints.
2) The ACBDD will extend the provisions of Policy 10.5 Protection of Whistleblowers, to all individuals who file confidentiality or privacy related complaint.
3) An employee or individual should file their complaint in writing to the privacy officer. Employees may review Policy 10.5 Protection of Whistleblowers which provides for alternate officials to receive the written complaint.
4) **Review and Investigation of Complaint.** Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Superintendent) shall review and investigate the complaint.
5) **Corrective Action.** If warranted, the Privacy Officer shall take corrective action, which may include:
   a) Change of policy and/or procedure.
   b) Intervention with an employee who is not following procedures including additional training and/or sanctions.
   c) Other action as appropriate.
6) **Communicating Results of Investigation and Corrective Action.** The Privacy Officer shall communicate the results of the investigation and any corrective action taken to the person filing the complaint.
7) **Documentation of Complaints.** The ACBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Policy 1330 HIPAA Assignments and Documentation.

DRAFT

1350 Policy Updating and Staff Training

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

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

AUTHORITY
45 CFR § 164.530(b)
45 CFR § 164.530(i)
45 CFR § 164.520
ORC § 5123.64(A) training in rights
OAC § 5123:2-5-01(E) training requirements for adult service workers
OAC § 5123:2-5-02(D) training requirements for adult service workers
OAC § 5123:2-5-05(D) training requirements for early intervention workers
OAC § 5123:2-5-07 training requirements for investigative agents

PROCEDURES
1) **Annual Review and Update of All Policies.** The HIPAA Privacy Officer shall conduct an annual review of all policies, and update policies as necessary based on new circumstances, changes in federal regulations and any changes in Ohio state laws and regulations governing DD Boards. An audit trail of policy changes will be maintained as detailed in Policy 1330 HIPAA Assignments and Documentation.
2) **Training New Staff on Confidentiality and Computer Security Policies.** The HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to ensure that all new staff will be receive training on ACBDD Confidentiality and Computer Security policies promptly after hiring. The two officers shall create an appropriate training program See Policy 4.5 Staff Training & Professional Development.
3) **Training All Staff When Policies are Substantially Changed**. The HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to ensure that staff receive training on Confidentiality and Computer Security policies when they are substantially changed. This training shall be implemented as detailed in Policy 4.5 Staff Training & Professional Development.
4) **Documentation**. Training records shall be maintained in each employee's personnel file for at least 6 years.

DRAFT

HIPAA SECURITY POLICIES

POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER

3000 Security Management Process

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

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

AUDIENCE
Executive Management

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

PROCEDURES

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

DRAFT

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

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

e) **Information System Inventory**. The HIPAA Security Officer and/or Security Team shall maintain an inventory of IT assets. This will include:
   i) IT Processing Assets
      (1) Cloud environments
      (2) Physical, virtual, and/or cloud servers or desktops
      (3) Mobile devices, including, laptops, smartphones, tablets
      (4) Physical storage devices, including NAS, external disk drives, USB flash drives, external disk drives, and any other storage device
      (5) Network gear, including firewalls, switches, access points, and any other gear
      (6) IOT devices
      (7) Any other physical or virtual device
   ii) Software Assets
      (1) Operating Systems
      (2) Application Software
   iii) Third-Party Services / Cloud Applications
   iv) Databases, Fileshares, Folders, and/or Datafiles containing ePHI
   v) A copy of this inventory shall be maintained off-site to ensure availability in the event of a fire or other disaster

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

REFERENCES

NIST SP 800-30 Guide for Conducting Risk Assessments
NIST Cyber Security Framework Project
Center for Internet Security (CIS) Top 20 Controls
The Fair Institute and FAIR Method

DRAFT

3005 Data Backup

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

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES
1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality.
2) **Multiple Backup Generations**. Backups should include as many generations as is practical to store and no fewer than daily snapshots for 30 days. Backup frequency shall be determined based on risk assessment and Recovery Point Objective specified in the Disaster Recovery Plan.
3) **Backup Software**. An appropriate backup facility/system shall be used. Configuration and/or scripting shall be reviewed and adjusted whenever infrastructure changes are made to ensure that appropriate data backup is maintained.
4) **Off-site and off-line storage**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include at least 2 backup copies: one at an off-site location, and one which is off-line (not accessible via the network).
5) **Backup Documentation**.
   a) A written description of the backup regimen must be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
   b) User documentation, for use by a system administrator, shall be maintained to allow for an alternate person to verify the daily operation of the backup.
6) **Responsibility**. The HIPAA Security Officer shall designate the employee with primary responsibility to perform daily monitoring of backup, with an alternate person if the primary employee is not working. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7) **Backup Log**. A daily electronic log of backup must be maintained.
8) **Backup Media Security**. Backup media shall be maintained in a secure location.
9) **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT**.** On at least a yearly 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.

DRAFT

3010 Disaster Recovery Plan and Emergency Mode Operation

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

POLICY
XCBDD personnel shall develop contingency plans, to include a Disaster Recovery (DR) Plan and Emergency Mode Operations (EMO) Plan to prepare for system failures, and for procedures for maintaining critical XCBDD operations in the event of system failure

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR 164.308(a)(7) Contingency Plan

PROCEDURES

1) **Disaster Recovery Team**. The HIPAA Security Officer shall ensure that appropriate Disaster Recovery (DR) and Emergency Mode Operation (EMO) plans are created, tested, documented and updated based on specifications in this policy. The Superintendent may establish a Disaster Recovery (DR) Team and/or an Emergency Mode Operations (EMO) Team to support the HIPAA Security Officer in this duty. The HIPAA Security Officer shall lead these teams and is responsible for all tasks specified in this policy.
2) **Identify Critical Business Processes**. The DR and EMO planning shall begin with identification and prioritization of business processes and IT assets/systems/capabilities that are critical to XCBDD's operations. For each of these processes and systems, a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) shall be established after consultation with System Owners and Executive Management.
3) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios shall include natural disasters, technical failures, malicious actions, and other human-caused failures. Failure scenarios shall be assessed as to likelihood and prioritized for planning.
4) **DR Planning Process**. The DR Planning Process shall include the following steps:
   a) **Preventative Measure Evaluation**. The planning effort shall identify current and potential preventative measures to reduce the likelihood of system failure. Example preventative measures to consider may include:
      i) Fault-tolerant hardware
      ii) High-availability configurations such as mirrored database clusters
      iii) Resilient data centers such as those meeting TIA standards for Tier 3 or Tier 4
      iv) Partners / third-party service providers who provide high-availability services
   b) **Mitigation Measure Evaluation**. The planning effort shall identify current and potential mitigation measures which reduce the impact of a disaster if it were to occur. Example mitigation measures to consider may include investment in incident response capability and failover capability.
   c) **Recovery Measures**. The planning effort shall create step-by-step playbooks to implement the recovery process for each of the prioritized scenarios identified above.
   d) **Disaster Recovery (DR) Plan**. A formal, written Disaster Recovery Plan shall be created which will include the following sections:
      i) Purpose and Scope of Plan
      ii) Key Information including physical locations, contact information for DR Team members and other key contacts and the location of an information repository
      iii) Plan Overview to include procedures for plan updating, plan documentation storage, data backup strategy, prevention and mitigation strategies.
      iv) Plan activation protocol and decision-making procedures during a disaster
      v) Plan for communications with key stakeholders
      vi) Playbooks for recovery, for each prioritized system, for each of the failure scenarios identified
      vii) written system and disaster recovery plan, with detailed steps for each of the scenarios identified above.

DRAFT

5) **Emergency Mode Operations (EMO) Planning Process**.
   a) **Preparation Steps**. For each prioritized system, the necessary preparation steps necessary to permit functioning in the absence of systems shall be identified. Preparation steps may include:
      i) Creation and updating of alternate, up-to-date, copies of key information
      ii) Maintenance and update of manual systems, for example, paper forms
      iii) Periodic drills to ensure adequacy of preparation
   b) **Emergency Mode Operations (EMO) Plan**. A formal, written Emergency Mode Operations Plan shall be created which will include the following sections:
      i) Purpose and Scope of Plan
      ii) Plan Overview including procedures for plan updating and plan testing
      iii) Plan activation protocol and decision-making procedures during Emergency Mode Operations
      iv) Playbooks for functioning for each system/department prioritized for inclusion in the EMO Plan
6) **Plan Location**. The location of the above plans is specified in Appendix F – Miscellaneous.
7) **Plan Testing**. The HIPAA Security Officer shall periodically test the DR Plan, and EMO Plan if it is not assigned to customers. All tests and their results shall be documented.
8) **Plan Update**. The DR Plan and EMO Plans shall be updated periodically based on changes to the organization, technology platforms, and systems, and to incorporate improvements based on plan testing.

REFERENCES

NIST SP 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems

DRAFT

3015 Facility Security and Access Control

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

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

AUDIENCE
HIPAA Security Officer

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

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

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

REFERENCES
NIST SP 800-66

DRAFT

3020 Annual Security Evaluation

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

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

AUDIENCE
HIPAA Security Officer

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

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

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

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

DRAFT

3025 Audit Control and Activity Review

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

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

AUDIENCE
HIPAA Security Officer

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

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

DRAFT

3030 Malicious Software Protection

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

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

AUDIENCE
HIPAA Security Officer

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

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

DRAFT

3035 Breach Reporting

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

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

AUDIENCE
HIPAA Security Officer, HIPAA Privacy Officer

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

PROCEDURES

1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer shall jointly determine if the incident meets the definition of a breach. If a Security Incident Response Team (Team) has not been assembled, they may assemble a Team at this point. Legal counsel and other outside expert advice shall be obtained, if appropriate, for additional guidance on the Team. An investigation should be launched, with attention to preserving evidence. The Team shall follow the following 3 step procedure:
   a) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   b) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   c) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.

      The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1330 HIPAA Assignments and Documentation. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred, and this process may stop. Otherwise, a breach has occurred, and the Team should proceed with the steps that follow in the remainder of this policy.
2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   a) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the Agency may use telephone, email or other means to immediately notify Individuals of the breach.
      ii) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         (1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
         (2) A description of the types of unsecured protected health information that were involved in the breach;

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

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

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

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

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

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

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

6) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that the Agency should have become aware if it exercised reasonable diligence. Breaches shall also be recorded in the Disclosure Log to facilitate compliance with the Accounting for Disclosures requirements.

DRAFT

3040 Security Awareness Program

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

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

AUDIENCE
HIPAA Security Officer

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

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

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

   A variety of media and avenues should be explored such as sign-in banners, security reminder cards for posting at workstations, articles in employee newsletters, posting on bulletin boards, etc. At a minimum, Computer Security Awareness will be included annually as detailed in Policy 4.5 Staff Training and Professional Development.

DRAFT

3050 Device and Media Disposal and Re-Use

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

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES
1) **Media Disposal Handled by HIPAA Security Officer**. As specified in Policy 3080 Computer Usage, Agency employees are prohibited from storing Protected Health Information of the Agency's on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.
2) **Accountability**. The Agency shall properly account for any physical media which is maintained by the Agency to store electronic PHI. A record of the movement of the media and associated hardware shall be maintained to clearly document the chain of custody.
3) **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 Rev. 1*. The Agency requires that at a minimum, data from electronic media should be "cleared", as defined in the referenced NIST documentation.
4) **Media Disposal and Re-use**. Procedures vary based on type of storage media:
   a) **Cloud Environments**. The HIPAA Security Officer shall obtain technical guidance from any cloud vendors regarding appropriate procedures for data sanitization. Protocols specified by vendor shall be followed as part of asset destruction to ensure sanitization of discarded assets is performed. Satisfactory assurances shall be obtained from vendor that the technical guidance is accurate.
   b) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
   c) **Hard Drives and floppy disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
   d) **Other Media**. See NIST SP 800-88 Rev. 1 for disposal/recycling methods for other media.
   e) **Notes**. Photocopiers, printers and other office equipment may include media subject to this provision!
5) **Records.** Records of Media disposal should be maintained for 10 years. When using third-parties to perform media sanitization, a Certificate of Destruction shall be obtained.

DRAFT

3052 Encryption and Key Management

POLICY
Encryption with appropriate key management shall be used for data at rest and data in motion. Exceptions to approved procedures must be documented by the HIPAA Security Officer.

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR §164.312 (c), (d) and (e) Integrity, authentication and transmission security
45 CFR §164.312(a)(2)(iv) Encryption and Decryption [of data at rest]

PROCEDURES

1) **Encryption of Data at Rest**. Data at rest shall be encrypted using appropriate standards:
   a) **Servers and Cloud Environments**. Servers and cloud environments storing PHI at rest shall be encrypted using current standards:
      i) Cyphers shall be compliant with ISO/IEC 19790:2012(E) Information technology – Security Techniques – Security requirements for cryptographic modules.
   b) **Desktop, Mobile Devices and Portable Media**. When encryption of end-user devices is determined appropriate based on risk analysis, ACBDD shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, the Agency:
      i) should consider solutions that use existing system features (such as operating system features) and infrastructure
      ii) should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments
   c) **Keys and Key Management**.
      i) **Encryption Keys**. The HIPAA Security Officer shall ensure appropriate management for all encryption keys including those for cloud environments, servers, DBMS, backup media, desktop and mobile devices and other data assets.
      ii) **Key Management**. Key management best practices shall be used for key assignment, backup, rotation, and destruction as detailed in NIST SP 800-57 Part 1 Rev 4, NIST SP 800-57 Part 2, and NIST SP 800-57 Part 3.
      iii) **Exceptions**. The HIPAA Security Officer may authorize exceptions to key management best practices, based on risk assessment. Any exceptions shall be documented.
2) **External Data in Motion**. For any data transmitted via the internet, ACBDD systems shall use a securely configured transmission protocol that provides both encryption and message integrity.
   a) Acceptable transmission protocols include:
      i) Web Access: TLS 1.2 (HTTPS)
      ii) File Transfer: FTPS, SFTP, SCP, WebDAV over HTTPS
      iii) Remote Shell: SSH2 terminal
      iv) Remote Desktop: radmin
   b) Secure configuration. Protocols shall be configured appropriately.
      i) Any encryption algorithms used must be compliant with ISO/IEC 19790:2012(E) Information technology – Security Techniques – Security requirements for cryptographic modules.
      ii) The Secretary of HHS's guidance (which provides a safe harbor) is may be used. The HHS guidance specifies the use of one of these standards:
         (1) NIST 800-77, *Guide to IPsec VPNs*,
         (2) NIST 800-113, *Guide to SSL VPNs*
   c) Exceptions. RDP may be used as a Remote Desktop Protocol only with the explicit approval of the HIPAA Security Officer who shall document the rationale for permitting the exception.
3) **Wireless Networks**. Wireless networks in ACBDD facilities and/or employee home offices will be implemented with the following security options:

DRAFT

a) The beacon shall be enabled
b) The SSID should be changed from the default
c) WPA2 should be enabled
d) WPS should be disabled
e) MAC filtering should be employed to allow access only to workstations owned by ACBDD and authorized to use the network.
f) These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
g) The administrator account shall be changed and protected with a strong password (see Policy 3054 User Account Management).

DRAFT

3054 User Account Management

POLICY
Identities of users with access to the Agency's information systems shall be maintained either in a centralized identity and access management system or on a decentralized basis. Multi-factor authentication shall be used whenever possible. Password policies shall use current standards when possible and shall consider the sensitivity/criticality of the asset. A password manager/password vault may be used to manage and provide access to passwords.

AUDIENCE
HIPAA Security Officer
Technical Staff

AUTHORITY
45 CFR §164.312(a)(2)(i) Unique User Identification
45 CFR §164.312(d) Person or Entity Authentication.
45 CFR §164.308(a)(5)(ii)(D) Password Management
NIST SP 800-63B Digital Identity Guidelines – Authentication and Lifecycle Management

PROCEDURES
1) **Identification**.
   a) **General Rule**. Each individual requiring access to an IT asset shall be given their own, unique account ID which serves to identify them to the application, system or device. The organization may manage user identities centrally using an identity and access management system or may use separate identity management systems.
   b) **Exceptions where Shared Accounts are Allowed**. For IT assets or vendors (e.g. a Domain Name Registrar) which do not support multiple accounts, the HIPAA Security Officer may authorize a shared account In such cases, passwords may be shared. The HIPAA Security Officer shall document these exceptions including the individuals who have access to passwords.
2) **Password Security –Rules for User Accounts**. Password security procedures will vary based on account type. These requirements apply for all User Accounts, that is, accounts used by human beings.
   a) Password length – passwords must be a minimum of six characters for handheld devices ten for network-connected devices.
   b) Password complexity. Passwords must include upper-case and lower-case letters, and digits. Passwords may also include special characters. Longer "passphrases" of 20+ characters are recommended (a passphrase is a sequence of 3 or more words).
   c) Not guessable. The password must not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.
   d) Mandatory periodic password changes shall not be required. Mandatory changes shall be required for all users if there is evidence or suspicion of compromise.
   e) When changing passwords, previously used passwords must not be recycled.
   f) Different passwords must be used for each account.
   g) When specifying answers to vendor security questions (for use with password reset requests) it is best to select questions whose answers cannot be easily discovered.
3) **Multi-Factor Authentication (MFA)**. Multi-factor authentication MUST be enabled for any sensitive systems and/or production environments. It should be enabled for any service or capability which supports MFA. The preferred method for MFA is a hardware token or authenticator app such as Google Authenticator. Text messaging-based MFA is permitted with approval of the HIPAA Security Officer.

FOR THE HIPAA SECURITY OFFICER
1) **Mandatory Password Changes with Evidence of Credential Compromise**. If there is evidence of malicious activity for an IT Asset, for example, if notified of a data breach by a cloud vendor which hosts one of the organizations applications, the HIPAA Security Officer shall ensure that all users change passwords for the application at risk.

DRAFT

2) **Password Vault / Password Manager**. The Agency may use a password vault and/or password manager for maintaining login credentials. The Password Vault / Password Manager shall be included as a critical system for the DR Plan as detailed in Policy 3010 Disaster Recovery and Emergency Mode Operations Plans.
3) **Password length**. Whenever possible for an IT asset, password length must be enforced by the system:
   a) Six (6) characters for handheld devices,
   b) ten (10) for network-connected devices,
   c) twelve (12) for user accounts with elevated privileges, for example, those with access to Production Environments (see Policy 3056 Privileged Account Management).
4) **Enforcing Password Complexity**. Whenever possible with an IT asset, password complexity must be enforced by the system:
   a) For assets which do not support NIST SP 800-63B, complexity is specified as requiring at least 1 upper case letter, 1 lower case letter, and 1 digit.
   b) NIST SP 800-63B guidelines are preferred for enforcing complexity when an IT asset supports this method. However, the Agency requires that the user supply an initial password which conforms to the length requirements above. (The NIST SP 800-63B guidelines specify a protocol for validating a user-supplied password against a database of prohibited passwords compiled from large breach corpuses, dictionaries and repetitive sequences.)
5) **Password History/Recycling Prohibited**. Whenever supported by systems, they shall maintain a history of the most recent 13 passwords. Assets shall be configured to prohibit password recycling.
6) **Maximum Login Attempts**.
   a) Whenever supported by applications, systems or devices, the asset shall be configured to permit only 5 attempts to enter a correct password, after which the User ID should be locked and/or deactivated.
   b) Both end-users and the HIPAA Security Officer shall be notified of the incident which shall then be investigated.

DRAFT

3056 Privileged Account Management

POLICY
Privileged Accounts shall be rigorously managed to protect against system compromise, including procedures for

- Approval of Privileged Accounts
- Password Rules
- The optional use of a Privileged Account Management (PAM) system
- Requirements regarding use of privileged accounts in software development
- Logging and auditing of privileged account activity

AUDIENCE
HIPAA Security Officer
Superintendent
System Administrators

AUTHORITY
45 CFR §164.308(a)(5)(ii)(D) Password Management

DEFINITIONS
User Account with Elevated Privileges – means an account used by a human being, for example a network administrator or Security Officer, with elevated privileges, such as a Windows Domain Admin.
Privileged System Account – means an account used by a non-human (e.g. an application or an operating system service) that operates with elevated privileges. Since these accounts are used by non-humans, passwords do not need to be memorized, and thus, different procedures may be used.
Privileged Account – means either a User Account with Elevated Privileges or a Privileged System Account.

PROCEDURES
1) **Approval of Privileged Accounts**. Privileged Accounts must be strictly controlled:
   a) The creation or modification of User Accounts with Elevated Privileges must be approved by at least two individuals: The HIPAA Security Officer or designee and the Superintendent or designee.
   b) The number of User Accounts with Elevated Privileges must be strictly limited to individuals with an authorized business need.
2) **Normal Privilege Accounts**. All users must be given an account without Elevated Privileges for routine work such as email access and web browsing, which must be used whenever the elevated privileges are not required.
3) **User Accounts with Elevated Privileges – Password Rules**. Requirements for passwords for User Accounts with Elevated Privileges detailed in Policy 3054 User Account Management shall apply, with the following modifications:
   a) The minimum length for a Password of a User Account with Elevated Privileges is 12 characters.
   b) Whenever possible, User Accounts with Elevated Privileges must be defined using role-based account privileges to limit privileges to the specific requirements.
   c) Any User Account with Elevated Privileges used by a 3rd party contractor must have an expiration date.
   d) Default passwords must always be changed.
4) **Privileged System Accounts—Password Rules**. Passwords for Privileged System Accounts, which are not used by humans, shall be optimized for security:
   a) The length shall be based on the maximum length for each platform (e.g. 256 for Windows)
   b) Should be a computer-generated random mix of characters including upper case, lower case, digits and symbols
   c) Shall not use passphrases and should not be memorized
   d) The computer generation must use an unpredictable seed (e.g. the low order bits of system clock time)
   e) Null passwords are always prohibited
   f) Any 3rd Party application with privileged account must have an expiration date
   g) Whenever possible, Privileged Accounts must be defined using role-based account privileges to limit privileges to the specific requirements for the task.

5) **A Privileged Account Management (PAM) solution** may be used to inventory and manage privileged accounts and their passwords. When using a PAM
   a) The PAM should maintain a central inventory of privileged accounts, which must be updated no less than quarterly.
   b) Privileged Account Passwords should be automatically changed at an interval based on risk assessment, but at least once every 90 days.
   c) PAM must be protected with 2 factor authentication.
   d) The PAM solution must use strong encryption to protect passwords.
   e) The PAM solution must be configured to ensure resiliency and for timely recovery as part of the disaster recovery plan.
6) **Software Application Development**
   a) All production applications that require privileged access must use special application accounts that are created specifically for the given application. Applications must never use default administrator accounts.
   b) Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.
   c) Passwords must never be hard-coded in software developed or modified by the Agency
   d) Test data and accounts used during development and testing must be removed before a production system becomes active.
7) **Privileged Account Logging**
   a) All privileged commands issued using User Accounts with Elevated Privileges must be traceable to specific individuals through the use of comprehensive logs.
   b) All activity on privileged accounts must be logged via session or keystroke recording.
   c) All user ID creation, deletion, and privilege change activity performed by people with User Accounts with Elevated Privileges must be securely logged.
   d) All logs recording privileged ID activity must be reviewed at least quarterly.
8) **Password Changes after Privileged User Credential Compromise**. If a User Account Password with elevated privileges is compromised by an intruder of another type of unauthorized user, all passwords on that system must be immediately changed.
9) **Acceptable Use of Privileged Accounts**
   a) Privileged Account Password Sharing. Passwords for User Accounts with Elevated Privileges may be shared among administrators only if controls are in place to know which administrator is using the account at any one time.
   b) The display and printing of Privileged Account passwords must be masked, suppressed, or otherwise obscured to prevent compromise.

DRAFT

3060 Technical Safeguards

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

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES
1) **Agency networks and hosting environments** used by ACBDD shall be secured using the following controls:
   a) **Firewalls.** Appropriate firewall technology shall be employed to protect networks and applications, and may include traditional, next-gen, and web application firewalls. These shall be configured based on best-practice recommendations from authoritative sources.
   b) **DNS Filtering** with a secure DNS service (e.g. OpenDNS) shall be employed.
   c) **Software Patching**. Hardware firewalls and network gear, hypervisors, operating systems, DBMSs, other system software and application software shall be patched on a timely basis:
      i) A written protocol specifying software and equipment to be monitored, responsible individuals, prioritization process, patching timelines, change management considerations, and management reporting shall be developed.
      ii) Third-party code. For any custom applications maintained by ACBDD, any third-party code included in the custom applications shall be monitored for security updates. Custom applications shall be updated on a timeline based on risk assessment.
   d) **Hardening**. A written protocol for asset hardening shall be developed and followed. This protocol shall specify baseline security configurations for assets in the technology stack including but not limited to cloud environments, firewalls, operating systems, DBMSs, web servers, load balancers, programming languages, end-user application software, network gear, IOT devices, and other technologies used. Configurations published by authoritative sources such as NIST, the Defense Information Systems Agency, Center for Internet Security, or other authority cited in the National Checklist Program (NCP) shall be employed.
   e) **Audit Log Collection, Review and Monitoring**. Audit logs from firewalls, servers, and key operating software will be collected, securely maintained, and monitored to maintain a high level of system availability and to detect security incidents, as detailed in Policy 3025 Audit Control and Activity Review.
   f) **Virtualization Software and environment**. Virtualization-enabling software, aka "hypervisors", shall be secured as follows:
      i) unneeded capabilities shall be disabled to reduce potential attack vectors
      ii) A strong password (see Policy 3056 Privileged Account Management).
      iii) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's
      iv) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations
      v) Use separate logon credentials for each virtual server
2) **E-mail**. The agency will maintain and properly configure both standard email and secure, encrypted email:
   a) **Standard Email**. Standard Email shall be securely configured:
      i) TLS shall be enabled to encrypt all communications between email clients and the server
      ii) Enable SMTP authentication

DRAFT

iii) Disable the "mail relay" parameter to avoid being an Open Relay
iv) Use DNSBL servers to blacklist known spammers
v) Additional anti-spam, anti-malware technology should be enabled
vi) Email shall be configured for anti-spoofing using SPF, DKIM and DMARC
vii) Maintain 2 MX records for failover
viii) Any email retention policy approved by the agency shall be implemented, which may include an email archiving capability.

b) **Secure Email**. For transmission of PHI, the agency will maintain the capability for end-to-end encryption:
   i) The solution must provide that any PHI is transmitted via a secure, encrypted method
   ii) The configuration of the system shall be approved by the HIPAA Security Officer.

3) **Workstation Security**. Workstations shall be secured with multiple levels of security:
   a) **Anti-malware software**. Anti-malware software shall be enabled as detailed in Policy 3030 Malicious Software Protection.
   b) **Patching**. Operating system and end-user application software shall be patched and included in the written protocol detailed in the "Software Patching" section above.
   c) **Timeout/Screenlock**. Automatic timeout and/or screenlock shall be enforced on all workstations. The timeout period shall be set based on risk assessment.
   d) **Hardening**. The hardening protocol for end-user workstations shall include the following controls:
      i) Operating systems, web browsers, and major application software including Adobe and Microsoft Office shall be configured with security settings from an authoritative source, and
      ii) USB ports shall be configured to disable externally mountable media for all production profiles. This may be overridden only with the express approval of either the CTO or the HIPAA Security Officer.
4) **Appropriate Audit Controls in ACBDD-Used Software**. Software used by ACBDD 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 criteria for continued use of and/or procurement of any new operating or application software.
5) **Integrity Checks**. The HIPAA Security Officer shall attend to integrity of electronic data:
   a) Periodic DBMS maintenance as recommended by the software vendor shall be performed.
   b) Message digest integrity reports shall be reviewed with corrective action taken as necessary.
6) **Software utilizing Electronic Signatures**. The HIPAA Security Officer will review and approve any software that offers electronic signature capability prior to implementation at the Agency. The HIPAA Security Officer shall be responsible for implementation and ongoing monitoring/auditing of the software as specified in Policy 3070 Electronic Signatures.

DRAFT

3062 Technical Controls for Mobile Devices

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

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

AUDIENCE
HIPAA Security Officer
IT Staff

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

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

PROCEDURES
FOR THE HIPAA SECURITY OFFICER/IT DEPARTMENT

1) **Technical Controls.** The Agency shall implement appropriate technical controls:
   a) An appropriate mobile device management system shall be used to
      i) maintain inventory of devices,
      ii) enforce security configurations,
      iii) provide remote wipe/lock capability,
      iv) perform geo-location,
      v) require encryption
      vi) mandate authentication per Policy 3054 User Account Management and Policy 3056 Privileged Account Management
      vii) implement anti-malware per Policy 3030 Malicious Software Protection
      viii) implement other configuration/safeguards as determined by risk assessment
   b) Additional technical controls may include control of third-party software, segregation of corporate from personal data, restricting the use of camera/microphone, and restricting automatic backups of the Agency's data to employee-controlled backup services (e.g. iCloud).
2) **Eligibility Criteria.** The Superintendent or designee shall approve any request for BYOD access to any agency systems.
3) **Resources Provided.** The Superintendent or designee shall establish which services/capabilities may be accessed using BYOD devices.
4) **Enrollment Procedures.** The Agency will create an Operating Procedure for enrolling mobile devices with mobile device management system. This Operating Procedure should address the processes for both Agency-owned devices and BYOD devices.

DRAFT

3065 Mitigation

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

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

AUDIENCE
Privacy Officer

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

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

DRAFT

3070 Electronic Signatures

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

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

AUDIENCE
Employees Using Electronic Signatures; Managers

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

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

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

DRAFT

c) Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of addendum to the original entry. The addendum should also be signed electronically and date/time stamped by the computer software.
d) System specific standards and procedures for use may vary by system and it will be required that the Agency must establish and maintain system specific procedures for any system which also satisfies other current policies.

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

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

DRAFT

SECURITY POLICIES FOR HR STAFF & SUPERVISORS

3075 Employee System Access and Termination Procedures

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

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

AUDIENCE
Human Resource Department, Supervisors, HIPAA Security Officer

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

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

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

DRAFT

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

Audience: Supervisors, Human Resource Department

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

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

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

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

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

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

3) **EMPLOYEE JOB CHANGES**

Audience: Human Resources Department, HIPAA Security Officer

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

4) **EMPLOYEE TERMINATION**

Audience: Supervisors, Human Resource Department, HIPAA Security Officer

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

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

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

   i) Physically escorting the person off the premises after notifying him/her of the termination.
   ii) Disabling system access and access to all shared cloud systems as specified above on a timely basis.
   iii) Requiring all staff in the former employee's workgroup to change passwords.
   iv) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the person and perceived threat.

5) **EMERGENCY SYSTEM ACCESS**

Audience: Supervisors, HIPAA Security Officer

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

DRAFT

HIPAA ADMINISTRATIVE REQUIREMENTS

SECURITY POLICIES FOR ALL STAFF

3080 Computer Usage

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

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

AUDIENCE
All Staff

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

PROCEDURES

1) **WORKSTATION USE**
   a) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the Individuals served: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related.
   b) **Personal Use of Computer Workstation, Including Internet Use**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use. "Limited use" is not easily defined so employees should contact their supervisors for clarification. In general, "limited use" means:
      i) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
      ii) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.
      iii) Workstations must never be used for any activity that would be embarrassing to the Agency if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
         (1) downloading or viewing pornographic, racist, profane or otherwise objectionable material
         (2) conducting conversations of a sexual nature of relating to an illicit affair
         (3) relating to any illegal activity
         (4) political activity
         (5) operating a business

         If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.
      iv) Personal use of Social Media, such as Facebook, Twitter, LinkedIn and others is detailed separately.
      v) Employees are prohibited from checking social media and their personal email except during their own time.
      vi) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the Agency.
   c) **E-Mail Use**. Employees with Agency e-mail accounts should check e-mail daily. Agency E-mail accounts in general are to be used for Agency purposes only. E-mail should be written in a professional manner and

DRAFT

should be courteous and respectful. Other policies when using e-mail:

i) Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and must not be used to send Protected Health Information unless it is appropriately encrypted. If employees receive PHI through standard email, it must be promptly deleted from email
ii) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in [*INSERT REFERENCE TO PUBLIC RECORDS POLICY].
iii) For personal matters, employees must use a personal account such as Gmail or Yahoo mail, on a personally-owned device
   (1) In the event that any Agency e-mail is received on a personal account, the employee must forward the email to the employee's Agency account so that it is entered into the public record.
   (2) In the event that a personal email is received on an Agency account, redirect the discussion to a personal email account.

d) **Data Storage on Network Only**. All data must be stored on the network, not on a workstation hard drive. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate shared or end-user private folder on an agency server. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions. DATA STORED ON WORKSTATION HARD DRIVES IS NOT BACKED UP, AND MIGHT BE DELETED WITHOUT NOTICE.
e) **Storage of PHI or Confidential material to Cloud or Removable Media Prohibited**. Personnel may not copy to any unauthorized cloud service or removable media, such as Flash drives, CDs, DVD or portable hard drives, any Agency confidential information or Protected Health Information on Agency computer system, except when specifically authorized by the HIPAA Security Officer for Agency purposes.
f) **Phishing and other suspicious emails**. Any employee who receives a suspected phishing email and/or other suspicious email must report it using the agency-specified procedure.
g) **Security incident reporting.** Any employee who opens a potentially malicious attachment or link, suspects a hacking incident, experiences loss or theft of a mobile device, notices any unusual computer behavior, or commits/observes a violation of any computer security policy must report the incident to the HIPAA Security Officer and/or his/her designee or help desk immediately.
h) **All Usage is Logged**. THE AGENCY MONITORS ALL USAGE OF AGENCY WORKSTATIONS BY LOGGING ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY, INCLUDING ANY PERSONAL USE OF AGENCY COMPUTERS. All logs of employee activity are property of the Agency and may subject to public disclosure.
i) **Duplication of copyrighted material prohibited**. No employee may duplicate copyrighted software or other media using Agency equipment.
j) **Agency-approved apps and cloud services only.** Employees must use only agency-approved applications (apps) on workstations, smartphones/tablets and/or cloud services for any function involving PHI or other confidential information. The use of any non-authorized software, apps or cloud services with PHI is expressly prohibited.
k) **Agency-approved hardware only**. Only Agency-approved and Agency-installed hardware may be utilized. No smart speakers (e.g. Alexa), video cameras, smart TVs, video cameras, other Internet-of-Things (IotT) devices, wireless networking equipment, smartphones, or other hardware or software may be installed or used without permission of the systems department.
l) **Electronic signatures**. Employees using software that includes Agency-approved electronic signature capabilities shall follow all procedures specified in Policy 3070 Electronic Signatures.

2) **WORKSTATION SECURITY**

a) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.
b) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.
c) Employees should logoff or lock their screen when leaving their workstation area for a period of time.
d) 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.

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

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

3) **USER IDs and PASSWORDS**

a) Each employee is assigned a unique User ID(s) for agency systems. Employees must only use their User ID to access Agency systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential and not shared with anyone else. If an employee reveals a password, or if becomes known to someone else, that employee must change the password.

b) Password length – passwords must be a minimum of six characters for handheld devices ten for network-connected devices.

c) Password complexity. Passwords must include upper-case and lower-case letters, and digits. Passwords may also include special characters. Longer "passphrases" of 20+ characters are recommended (a passphrase is a sequence of 3 or more words).

d) Not guessable. The password must not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.

e) Mandatory periodic password changes shall not be required. Mandatory changes shall be required for all users if there is evidence or suspicion of compromise.

f) When changing passwords, previously used passwords must not be recycled.

g) Different passwords must be used for each account.

h) When specifying answers to vendor security questions (for use with password reset requests) it is best to select questions whose answers cannot be easily discovered.

i) In general, passwords should be memorized and not written. Any written reminder should not be maintained near the workstation.

j) Passwords should be changed only if there is evidence or suspicion of compromise.

k) Two-factor authorization and/or Single Sign-On technology should be used, if available.

l) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

4) **EMERGENCY SYSTEM ACCESS**

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

DRAFT

3082 Social Media Use

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

POLICY
Online media can bring significant educational benefits to the community and can advance the mission of the agency, however ethical and other challenges must be balanced. Employees must strictly monitor their use of social media, including, but not limited to, Facebook, LinkedIn and Instagram, to protect the confidentiality of PHI and other confidential information of the organization. This policy applies to employee use of personal social media both while working and during their personal time as well as the use of employer-sponsored social media accounts.

AUDIENCE
All Staff

PROCEDURES
1) **Agency-Sponsored Social Media Use**.
   a) The superintendent may approve the establishment of one or more agency-sponsored social media pages or accounts.
   b) Any personnel responsible for social media management must be appropriately trained on this policy
   c) The agency should include a social media privacy policy in an appropriate location on each social media platform
   d) Prior to placing an image or other personally identifiable information on the agency website or social media,
      i) Both a properly completed HIPAA authorization and a media release shall be completed and retained by the agency.
      ii) The Privacy Officer or designee should review all images, videos, and comments prior to posting.
   e) If a Individual served discloses PHI on a agency-sponsored social media page, the agency may delete or respond to the disclosure.
      i) The Privacy Officer or designee shall review the agency social media account at the end of each day to ensure no improper disclosures have been made by the staff or Individuals served.
      ii) Individuals served are permitted to disclose their PHI on social media, and the agency, at its discretion, may allow it to remain.
      iii) Deleting comments made by Individuals served is permitted, if the comment is deleted **entirely**, at the discretion of the Privacy Officer or designee. If and when an Individual served discloses PHI, the Privacy Officer or designee may remove the information at their discretion, for example, if the comment discloses information judged inappropriate or excessive.
      iv) The agency must never **edit** the disclosure of an Individual served because doing so makes the agency a co-author of the PHI.
   f) For posts from Individuals served, the agency may respond in a general way which in no way acknowledges that the inquirer as an Individual served by the agency. If the post requires a non-general reply, the conversation should be taken offline. The agency should use one of the following three general replies to be used for positive and negative comments and inquiries from Individuals served:
      i) A "like" or favorite
      ii) ACBDD is proud to have been serving the community since [add year established] and takes the care of individuals with developmental disabilities – and their privacy – seriously. Because federal privacy laws govern protected health information, it is not the policy of ACBDD to substantively respond to negative reviews on the internet. We welcome all individuals served, and their families, to address any concerns or requests for information about services provided with us directly as we strive to continue to provide individualized and excellent service in our community. Please give us a call at [agency phone number].
      iii) ACBDD is proud to have been providing care in the community since [add year established] and takes treatment of its patients – and their privacy – seriously. Because federal privacy laws govern patients' protected health information, it is not the policy of ACBDD to substantively respond to reviews on the

DRAFT

internet, but we always appreciate kind words and recommendations.

2) **Personal use of Social Media by Employees**.
   a) **Employee Use During Work Hours**. During work hours, employees are expected to focus on work-related activities. Consequently, in general, they are expected not to open any social media to avoid distraction and/or loss of employee productivity.
   b) **Employee Use Outside of Work Hours**. Any statement or image on social media has the potential to become a public communication, so employees of ACBDD must follow the following guidelines:
      i) **Sharing of work-related activities.** Employees should limit the sharing of any ACBDD related information that they would deem acceptable to be made public, for example, on the front page of a major newspaper.
         (1) Examples of information that are appropriate to share on social media include:
            (a) The employee's excitement and satisfaction with the work and mission of ACBDD.
            (b) Sharing details of an upcoming public event sponsored by ACBDD, such as a local "Health Fair" day,
            (c) Sharing the name and/or image of a friend who is a co-worker at ACBDD
         (2) Information that is NOT appropriate to post include:
            (a) The name or image of an Individual receiving services from ACBDD, unless in compliance with a HIPAA-compliant release of information form and media release form.
            (b) A complaint about ACBDD such as displeasure with a supervisor or co-worker
            (c) Any Protected Health Information, or PHI, such as the name of an Individual served or any other PHI. This includes any information that could be used to identify someone as an Individual served by ACBDD. Note that details, such as unusual cases, could reveal an individual's identity even if the name is not used.
         (3) Employees are not prohibited from making any communication that is protected and regulated by the National Labor Relations Board. Employees are further encouraged but not required to limit communications on social media to those that would portray them in a professional manner.
      ii) **Friending/Connecting/Linking.** In general, employees should not "friend", "link", "follow", or otherwise connect, on any social media platform, to any an Individual served by ACBDD, nor a parent or guardian. ACBDD expects employees to maintain an acceptable professional boundary with patients.
      iii) **Messaging.**
         (1) Employees must not use social media for ACBDD communications, especially if they involve PHI. This is prohibited since the organization does not have a Business Associate agreement with any social media platform.
         (2) Employees who receive unsolicited communications via social media from or about an individual served, or about an individual seeking services, must not respond using social media. Any necessary response must be done in person, via phone, or secure email. If possible, the unsolicited message should be deleted from the social media platform. Any such incident should be reported to the Privacy Officer for investigation.

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

DRAFT

3085 Portable Computing Devices

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

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

AUDIENCE
All Staff

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

PROCEDURES

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

DRAFT

j) **Replacing a Device**. Prior to replacing/upgrading a device, employees must contact the agency's IT manager for instructions for remove all of the organization's data prior to returning/selling/disposing of their current device.
k) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
l) **Discovery and other Legal Processes**. In case of legal action, personal devices used for agency business are subject to e-discovery. Users are responsible for bringing or sending the mobile device to the IT Department and giving the necessary device access codes when notified that the device is needed for e-discovery purposes.
m) **Termination and/or Suspension from Employment.** Upon termination of employment, employee agrees to provide the device to the IT department who will remove all organization data and disable access to the organization's IT resources. At the discretion of the organization, employees who are placed on administrative leave will have access suspended until their return to work.

2) **AGENCY-PROVIDED MOBILE DEVICES**
a) **Eligibility Criteria and Signed Agreement**. Management will evaluate, on an individual basis, the eligibility of employees to use agency-owned mobile devices. Employees who wish to use an agency-owned mobile device must sign the Agency-Owned Mobile Device Agreement.
b) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.
c) **Text Messaging**. Any text messaging performed from an agency-owned device must be done in accordance with the requirements of this policy. Text messaging using a CCBDD-approved text messaging app is permitted and is the preferred method for any text messaging. The use of standard text messaging with individuals served and/or their parents is discouraged, but not prohibited, for "transient" messages regarding meeting dates and times. Medical, behavioral, diagnosis and similar PHI must not be transmitted with standard text messaging. If unsolicited PHI is received via text by a staff member, any response should be via an approved method such as phone call, secure email, or CCBDD-approved text messaging app.
d) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Policy 3090 Security Incident Response and Reporting.
e) **Proper Use.** Agency-owned mobile devices must generally be used for agency-related purposes. *Minimum* personal use is permitted, such as checking weather or making a brief personal call.
f) **Use While Driving**. Any use of Agency-owned mobile devices while driving must be done in accordance with the laws of the jurisdiction in which you are physically present.
g) **Use of Device by Other People Not Permitted.** Employees using agency-owned mobile devices under this policy must not allow anyone to use agency-owned mobile devices who is not permitted to use these devices under this policy.
h) **Agency-Owned Mobile Devices May Not Be Sold, Transferred, Disposed of, Recycled or Damaged.** Employees must not sell, transfer, dispose of, recycle, or intentionally or recklessly damage agency-owned mobile devices.
i) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
j) **Termination and/or Suspension from Employment.** Upon termination of employment or upon administrative leave, employee agrees to return the device to the IT department.

DRAFT

3087 Employee Work at Home

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

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

AUDIENCE
All Staff
HIPAA Security Officer and Technical Staff

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

[Adjust this policy as necessary based on organization preferences]

PROCEDURES
1) **Eligibility to Work at Home.** Agency management will evaluate, on an individual basis, the eligibility of employees to work at home.
2) **Use Agency-provided laptop**. Employees working from home must use an agency-provided laptop computer for access to the agency's electronic record system(s).
3) **Limited use or personally-owned Computer/Laptop.** Employees working at home are permitted to use personally-owned computers ONLY for accessing the agency's web-based email.
4) **VPN Required for Network Access.** Except as permitted by Policy 3085 Portable Computing Devices, Employees must use agency-specified methods such as a Virtual Private Network (VPN). The use of any unauthorized third-party service (e.g. LogMeIn) to access the agency network is prohibited.
5) **Home Network Router.** With approval of the HIPAA Security officer, employees may connect their agency-provided laptop to the internet using personally-owned home router. Employees connecting in this way must set a unique 8+ character password for router administration, and must keep their router up-to-date with any vendor-supplied security updates.
6) **Guidance.** Employees who do not understand any of the requirements of this policy must consult with the HIPAA Security Officer or designee for guidance.

DRAFT

3090 Security Incident Response and Reporting

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

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

AUDIENCE
All Staff

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

PROCEDURES

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

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

DRAFT

APPENDICES

Appendix A: Identifying Business Associates

Identifying your Business Associates

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

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

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

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

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

Common examples of Business Associates for DD Boards include

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

DRAFT

Examples of relationships which are NOT Business Associates

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

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

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

DRAFT

Appendix B: Sample HIPAA Business Associate Agreement

[Business Associate Agreement Provisions

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

Any new contracts must comply with the new specifications.

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

HIPAA BUSINESS ASSOCIATE AGREEMENT

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

RECITALS

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

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

1) **Allowed Uses and Disclosures of Protected Health Information**. BUSINESS ASSOCIATE provides services for COVERED ENTITY. BUSINESS ASSOCIATE may use and disclose protected health information only as follows:
   A) BUSINESS ASSOCIATE may use and disclose protected health information for the purposes specifically provided in Attachment A – Permitted Uses and Disclosures. In performance of the tasks specified in Attachment A – Permitted Uses and Disclosures, BUSINESS ASSOCIATE may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this Agreement.
   B) BUSINESS ASSOCIATE may further use and disclose PHI, if necessary:
      i) for the proper management and administration of BUSINESS ASSOCIATE's business, and/or

ii) to carry out the legal responsibilities of BUSINESS ASSOCIATE if the disclosure is either

a) required by law, or

b) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.

2) **Responsibilities of BUSINESS ASSOCIATE**. With regard to its use and disclosure of protected health information, BUSINESS ASSOCIATE agrees to do the following:

A) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law. No further use or disclosure is permitted.

B) BUSINESS ASSOCIATE may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by COVERED ENTITY.

C) Use appropriate physical, technical and administrative safeguards and comply with the requirements of the HIPAA Security Regulations (45 CFR § 164 Subpart C) to prevent use or disclosure of PHI other than as provided for by the Agreement.

D) Report to COVERED ENTITY any security incident, and any use or disclosure of PHI not provided by this contract, including breaches of unsecured protected health information as required by 45 C.F.R § 164.410 within 10 days. Upon notification of a security incident, BUSINESS ASSOCIATE shall provide its preliminary risk assessment, as required by 45 CFR § 164.402(2), to COVERED ENTITY. COVERED ENTITY shall make final determinations regarding the risk assessment.

E) Require that subcontractors who create, receive, maintain or transmit ePHI on behalf of BUSINESS ASSOCIATE comply with applicable HIPAA Security regulations by entering into a business associate contract with these subcontractors. The business associate contract shall meet the specifications of 45 CFR § 164.314.

F) Make available to the Individual any requested protected health information, in accordance with procedures specified by COVERED ENTITY and in compliance with 45 CFR § 164.524, "Access of individuals to protected health information".

G) Make available for amendment and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR § 164.526, "Amendment of protected health information".

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

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

J) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining BUSINESS ASSOCIATE's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

K) Return to COVERED ENTITY or destroy, as requested by COVERED ENTITY, within 30 days of the termination of this Agreement, the protected health information in BUSINESS ASSOCIATE's possession and retain no copies or electronic back-up copies of protected health information. If this is not feasible, BUSINESS ASSOCIATE will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this Agreement for as long as the protected health information is in its possession.

3) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, whose services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligations to fully comply with all provisions of this Agreement.

4) **Term and Termination**.

A) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all

DRAFT

obligations of the parties have been met, unless terminated as provided in this Agreement herein or by written mutual agreement of the parties.

B) Termination. As provided for under 45 C.F.R. § 164.504, COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that BUSINESS ASSOCIATE has breached a material provision of this Agreement. Alternatively, COVERED ENTITY may choose to: (i) provide BUSINESS ASSOCIATE with 30 days written notice of the existence of an alleged material breach; and (ii) afford BUSINESS ASSOCIATE an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

5) **Survival**. The respective rights and obligations of BUSINESS ASSOCIATE and COVERED ENTITY under the provisions of paragraph 2K above, detailing BUSINESS ASSOCIATE's return of and/or ongoing protections of protected health information, shall survive the termination of this Agreement.

6) **Amendment**. This Agreement supersedes any previously negotiated HIPAA Business Associate contracts. Further, it may be modified or amended only in writing as agreed to by each party.

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

8) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to BUSINESS ASSOCIATE _____
_____
_____
_____

If to COVERED ENTITY: _____
_____
_____
_____

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

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:_____	By:_____
Name: _____	Name:_____
Title: _____	Title:_____
Date:_____	Date:_____

Attachment A – Permitted Uses and Disclosures

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

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

Example Clauses:

MUI Investigator: BUSINESS ASSOCIATE is authorized to use and disclose protected health information for the

DRAFT

purposes of conducting MUI investigations.

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

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

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

DRAFT

Appendix B2: Sample Service Provider Agreement

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

CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement ("Agreement") is entered into by and between _____ ("SERVICE PROVIDER") and _____ ("COVERED ENTITY").

RECITALS

1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 45 CFR § 164 as amended.
2) Terms used in this agreement, including but not limited to "covered entity", "business associate", "Protected Health Information (PHI)", "unsecured protected health information", "use", "disclose", "breach", and "security incident", shall have the same meaning as defined in most current versions of the above-referenced regulations.
3) COVERED ENTITY is a covered entity under HIPAA and is regulated by the HIPAA regulations.
4) Providers of medical and related services, if they submit electronic claims on their own behalf, are also HIPAA Covered Entities. Healthcare providers who do not transmit electronic claims are not subject to the HIPAA regulations, and consequently COVERED ENTITY is requiring the confidentiality assurances detailed in this agreement.

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

1) **Covered Entities Attest to HIPAA Compliance**. If SERVICE PROVIDER is a HIPAA covered entity, SERVICE PROVIDER attests that it fully complies with all applicable HIPAA regulations.
2) **Allowed Uses and Disclosures of Protected Health Information**. The SERVICE PROVIDER provides services for the COVERED ENTITY. The SERVICE PROVIDER may use and disclose protected health information only as follows:
   A) SERVICE PROVIDER may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, SERVICE PROVIDER may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.
   B) SERVICE PROVIDER may further use and disclose PHI, if necessary:
      i) for the proper management and administration of the SERVICE PROVIDER's business, and/or
      ii) to carry out the legal responsibilities of the SERVICE PROVIDER if the disclosure is either
         a) required by law, or
         b) SERVICE PROVIDER obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the SERVICE PROVIDER of any instances of which it is aware in which the confidentiality of the information has been breached.
3) **Responsibilities of SERVICE PROVIDER**. With regard to its use and disclosure of protected health information, SERVICE PROVIDER agrees to do the following:

DRAFT

A) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.

B) Use appropriate physical, technical and administrative safeguards to protect electronic PHI. These include:

   i) Any PHI stored on any portable computer equipment owned by SERVICE PROVIDER must be encrypted.

   ii) Text messaging with any information relating to individuals served shall be strictly limited to scheduling appointments.

   iii) Records shall be removed from COVERED ENTITY's premises only with permission of COVERED ENTITY

C) Report to the COVERED ENTITY any security incident, and any use or disclosure not provided by this contract, including breaches of unsecured protected health information.

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

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

F) Return to the COVERED ENTITY or destroy, as requested by the COVERED ENTITY, within 30 days of the termination of this Agreement, the protected health information in SERVICE PROVIDER's possession and retain no copies or electronic back-up copies. If this is not feasible, SERVICE PROVIDER will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.

4) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

5) **Term and Termination**.

   A) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

   B) Termination. COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that the SERVICE PROVIDER has breached a material provision of this Agreement. Alternatively, the COVERED ENTITY may choose to: (i) provide the SERVICE PROVIDER with 30 days written notice of the existence of an alleged material breach; and (ii) afford the SERVICE PROVIDER an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

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

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

8) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to SERVICE PROVIDER _____
_____
_____
_____

If to COVERED ENTITY: _____
_____
_____
_____

DRAFT

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

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

Attachment A – Permitted Uses and Disclosures

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

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

Example Clauses:

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

DRAFT

Appendix C: Sample Privacy & Security Officer Job Descriptions

HIPAA Privacy Officer Job Description

REPORTS TO: Superintendent

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

Responsibilities:

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

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

Qualifications of Privacy Officer:

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

DRAFT

HIPAA Security Officer Job Description

REPORTS TO: Superintendent

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

DUTIES:
1) Document security policies and procedures created by the information security committee/council.
2) Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures.
3) Oversee information security awareness programs/education within the organization.
4) Perform information security risk assessments and act as an internal auditor.
5) Perform and/or oversee information security risk management activities including creating all required documentation.
6) Implement information security policies and procedures.
7) Review all system-related security planning throughout the agency and act as a liaison to information systems.
8) Monitor compliance with information security policies and procedures, referring problems to the appropriate department manager.
9) Coordinate the activities of the information security committee.
10) Advise the organization with current information about information security technologies and issues.
11) Monitor the access control systems to assure appropriate access levels are maintained.
12) Prepare the disaster prevention and recovery plan.
13) Engage top management and/or trustees as necessary regarding information security issues, risk assessments and risk management.

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

Adapted from: http://www.hipaadvisory.com/

DRAFT

Appendix D: Facility Security and Access Plan

ACBDD shall protect its facilities to ensure the confidentiality of its information resources. Safeguards include:

- An electronic access control system (card-based) is used all facilities to permit access by authorized staff and contractors. The Facilities and Transportation director and IT Manager manage the access control system.
- Visitors are interviewed via intercom system, and those admitted are required to sign in with receptionist.
- Video monitoring is used throughout school and is recorded with a DVR system for subsequent access.
- Agency servers and data communication equipment are kept in locked rooms with limited access based on need.

DRAFT

Appendix E: Minimum Necessary – Workforce, Disclosures and Requests

Workforce Access to PHI and Safeguards

Person, Classes of Persons, or Business Associates	***Categories of PHI Needed***	***Additional Safeguards(*)***
Administration		
Superintendent	All	
Business Manager	All	
Medicaid/Records Clerk	All	
Nurse	Medical notes, relevant medical information	
Administrative Assistant	Computer data	
Administrative Secretary	Computer data	
Janitor	None	No User ID will be provided
Community Employment		
Supported Community Employment Director	All Community Employment files	
Job Trainer	All Community Employment files, medical and demographic data	
Job Coordinators	All Community Employment files, medical and demographic data	
Job Developers	All Community Employment files, medical and demographic data	
Receptionists	Computer data	
Service & Support		
Service & Support Director	All	
Administrative Secretary	All	
Service & Support Coordinator	All	
Service & Support Professional (1)	All	
Service & Support Technicians	All	
Transportation/Maintenance		
Vehicle Operators	Medical needs related to transportation	No User ID will be provided; medical needs and behavioral support needs will be provided in hardcopy format by SSA
Grounds Maintenance	None	No User ID will be provided;
Mechanic	None	No User ID will be provided;

DRAFT

School		
M.H. Coordinator	records regulated under FERPA	
Classroom Instructors	records regulated under FERPA	
Instructor Assistants	records regulated under FERPA	
Language Development Specialist	Medical Needs, notes pertinent to speech/language	
Early Intervention Specialists	All Early Intervention files	
Business Associates		
Athens County Auditor's Office	records pertinent to bill payment	
Community Options	Medical needs, notes pertinent to service provision	
Medicaid Billing Solutions	Demographic and case notes for billing	
Primary Solutions, Inc.	Gatekeeper Data	For support
Intellinetics	Intellivue Data	For support

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

Procedures for Routine Disclosures of PHI

Note: Disclosures to medical, vocational, residential and other providers, and service coordination with other agencies are "treatment" and per Minimum Necessary specifications, a procedure is not needed here.

1) **Software & Network Providers** – Information in the computer system is incidentally available during system support activities.
   A) **Intellinetics.** Intellinetics provides technical support for the Intellivue imaging system.
   B) **Gatekeeper and other Support.** Primary Solutions and other support vendors will be granted access rights on an as needed basis. Technical solutions for implementing this authorization will be deployed by the 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) **Department Of Developmental Disabilities –** Information will be shared routinely with 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) **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.

DRAFT

9) **Bureau of Disability Determination –** Using the Bureau's forms, assessment information will be shared in order to determine individual's eligibility for benefits.
10) **Attorneys –** When a subpoena is presented, the protocol in Policy 1090 Disclosures that do Not Require an Authorization will be carefully followed to determine, with legal counsel assistance, if the subpoena should be honored.
11) **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.
12) **Law Enforcement –** As identified by the Director of Services & Supports, guardianship, family contact information and behavior support plans will be shared with law enforcement agencies. In addition, upon presentation of a warrant and verification of credentials if presented in person, other file information may be shared with law enforcement agencies. See Policy 1090 Disclosures that do not Require an Authorization.

Procedures for Routine Requests of PHI

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

Types and Locations of Records for School-Age and Early Childhood

Types of data:
1) Application Form for admission
2) Placement authorization from school district
3) Release of Information Consent forms
4) Case history
5) Psychological evaluation forms
6) Medical evaluation reports
7) Educational evaluation reports
8) Vocational evaluation reports (where appropriate)
9) Special evaluation reports (language, physical therapy, admission, assessment, etc.)
10) Case summary (comprehensive report)
11) Home training reports (where appropriate)
12) Individual Habilitation or Education Plans
13) Habilitation or education progress reports or notes
14) Reports of special services provided
15) Critical Incident notes (injuries, accidents, unusual occurrences)
16) Attendance records
17) Written communication with parents, guardians, or adult enrollees
18) Written communication sent to another agency or received from an agency
19) Records pertaining to change of placement, transfer, suspension or termination
20) Verification of age

Locations of Data
1) Agency's information systems
2) Beacon School Office and Classrooms

Names and Positions of Employees with Access to PII

Upon request from a parent of a child under the age of 18 exercising their rights pursuant to OAC 3301-51-04(N) to obtain a list of the names and positions of staff with access to their child's information, the agency shall create an accurate list of personnel, and their positions, with access to these records of children.

DRAFT

Appendix F: Miscellaneous

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

Designated Record Set:
All information in Gatekeeper and Intellivue software
Any paper case records prior to use of the Gatekeeper/Intellivue software

DRAFT

Athens County Board of Developmental Disabilities (ACBDD) – Authorization for Release of Information

Personnel Plus	Service and Support Administration	Beacon School
1002 East State Street #5	11 Harper Street	801 W. Union St.
Athens, OH 45701	The Plains, OH 45780	Athens, OH 45701
740/592-1645 (voice)	(740) 592-6006 (voice)	740/594-3539 (voice)

Name of Individual Served _____ Date of Birth _____

I authorize ACBDD to:

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

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

The purpose of this disclosure is
___ Coordination of care
___ Requested by Individual Receiving Services, or guardian/parent
___ Other _____

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

Expiration Date:
___ 90 days from date signed
___ other date: _____

Approved by: _____ Date: _____

If signed by someone other than the Individual being served:

Print Name_____
Authority to sign: ___ Parent or Guardian
____ Appointed by Individual as HIPAA Personal Representative
____ Other _____

For staff use (complete the following steps and indicate by a check. Name of Staff Person _____)
___ Copy of signed authorization given to Individual / Parent / Guardian
___ Copy of records released given to Individual / Parent / Guardian (if requested)
___ Disclosure logged on Disclosure Log
___ Revocation received on _____ and acted upon.

Notice of Privacy Practices

Athens County Board of Developmental Disabilities

FOR YOUR PROTECTION

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. IT ALSO DESCRIBES OUR PRACTICES ABOUT [INSERT SCHOOL NAME] SCHOOL RECORDS.

YOUR RECORDS ARE PRIVATE

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

WHO USES AND DISCLOSES MY RECORDS?

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

Our organization includes Personnel Plus, the bus garage, the Service and Supports Administration, and Beacon School.

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

In general, we use and disclose your information:

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

COULD MY RECORDS BE RELEASED WITHOUT MY PERMISSION?

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

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

DRAFT

- to coroners, medical examiners and funeral directors,
- to victims of alleged violence or sex offenses,
- For workers' compensation programs,
- For specialized government functions including national security, protecting the president, operating government benefit programs, and caring for prisoners,
- In connection with "whistleblowing" by an employee of the Agency.

All other uses not described above require that we obtain your signed permission.

WHAT IF MY RECORDS NEED TO GO SOMEWHERE ELSE

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

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

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

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

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

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

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

HIPAA Privacy Officer
Athens County Board of Developmental Disabilities
801 West Union Street
Athens, Ohio 45701
(740) 594-3539 x224
skramer@athenscbdd.org

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

OUR DUTIES

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

QUESTIONS OR COMPLAINTS?

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

Attn: HIPAA Privacy Officer
Athens County Board of DD
801 W. Union Street
Athens, Ohio 45701
740-594-3539

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

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

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

DRAFT

Employee-Owned Mobile Device Agreement

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

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

_____

Employee Name (please print)

_____

Employee signature

_____

Date

Agency-Owned Mobile Device Agreement

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

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

_____

Employee Name (please print)

_____

Employee signature

_____

Date

DRAFT

ACBDD Disclosure Log

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

DRAFT

ACBDD ACKNOWLEDGEMENT OF HIPAA POLICIES AND PROCEDURES

Name_____ Date_____

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

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

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

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

Signature:_____ Date:_____

DRAFT

ATHENS COUNTY BOARD OF DD

Confidentiality & Computer Security Policies

HIPAA, FERPA & Ohio Law Compliance

10/29/2010

ORIGINAL

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

Table of Contents

CONFIDENTIALITY & PRIVACY POLICIES 5
POLICIES FOR ALL STAFF 5
1000 Confidentiality, Privacy and Computer Security Definitions 5
1010 Confidentiality – General Rules 10
1020 Minimum Necessary Policy 11
1030 Confidentiality Safeguards (Oral & Written) 14
1040 Speaking with the Family and Friends of an Individual Receiving Services 16
1050 Authorizations 17
1060 Verification 19
1070 Minors, Personal Representatives and Deceased Individuals 20
1080 Duty to Report Violations and Security Incidents 22
1090 Disclosures that do Not Require an Authorization 23
INDIVIDUAL RIGHTS 27
1200 Individual's Right to Access Records 27
1210 Individual's Right to Request Amendment of Records 29
1220 Individual's Right to Receive an Accounting of Disclosures 31
1230 Individual's Right to Request Additional Restrictions 33
1240 Individual's Right to Request Confidential Communications 34
CONFIDENTIALITY POLICIES FOR SUPERVISORS 35
1300 Business Associate Contracts 35
1310 Notice of Privacy Practices 36
1320 Non-intimidation and Non-retaliation 37
1330 HIPAA Assignments and Documentation 38
1340 Privacy Complaints 40
1350 Policy Updating and Staff Training 41
HIPAA SECURITY POLICIES 42
POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER 42
3000 Security Management Process 42

ORIGINAL

3005 Data Backup 44
3010 Disaster Recovery Plan and Emergency Mode Operation 45
3015 Facility Security and Access Control 47
3020 Annual Security Evaluation 48
3025 Audit Control and Activity Review 49
3030 Malicious Software Protection 50
3035 Breach Reporting 51
3040 Security Awareness Program 53
3050 Device and Media Disposal and Re-Use 54
3060 Technical Safeguards 55
3065 Mitigation 57
3070 Electronic Signatures 58
SECURITY POLICIES FOR HR STAFF & SUPERVISORS 60
3075 Employee System Access and Termination Procedures 60
HIPAA ADMINISTRATIVE REQUIREMENTS 62
SECURITY POLICIES FOR ALL STAFF 62
3080 Computer Usage 62
3082 Use of Social Networking Sites including Facebook, Twitter, LinkedIn, MySpace and others 65
3085 Portable Computing Devices and Home Computer Use 66
3090 Security Incident Response and Reporting 67
APPENDICES 68
Appendix A - Identifying Business Associates 68
Appendix B: Sample HIPAA Business Associate Agreement 70
Appendix C: Sample Privacy & Security Officer Job Descriptions 73
Appendix D -Facility Security and Access Plan 76
Appendix E - Workforce Access to PHI and Safeguards 77
Appendix F – Legal Citations 79
Appendix G - Mobile Device User Agreement 82
Athens County Board of Developmental Disabilities (ACBDD) – Authorization Form 826
Notice of Privacy Practices 888

ORIGINAL

ACBDD Disclosure Log _____ ***90***9

ORIGINAL

CONFIDENTIALITY & PRIVACY POLICIES

POLICIES FOR ALL STAFF

1000 Confidentiality, Privacy and Computer Security Definitions

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

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

AUDIENCE
All Staff

AUTHORITY
The definitions below are adapted from the federal HIPAA regulations, FERPA regulations, the Ohio Revised Code, and Ohio Administrative Code. In some cases, a definition in a regulation is adjusted 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.

DEFINITIONS

1. **Access** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.)
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 ACBDD 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. An "incidental disclosure", which by definition is not a violation of the Privacy Rule
   b. A use or disclosure of protected health information from which all the identifiers specified in a Limited Data Set have been removed, and in addition, date of birth and zip code have been removed.
   c. 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 or security rules.
   d. 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 and Security rules.

ORIGINAL

e. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information
f. The loss of data which has been appropriately secured through Board approved encryption or has been destroyed

Compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

7. **Business Associate (BA)** - A Business Associate is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The requirements are set forth more fully in 45 CFR 160.103. See Appendix A - Identifying Business Associates for more details.
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 privacy 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. **Destruction** - Destruction means physical destruction of a record or removal of personal identifiers from information so that the information is no longer personally identifiable.
12. **Directory Information** - Directory Information includes the following information relating to a participant: the participant's name, address, telephone number, date and place of component of service, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, and awards received.
13. **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;
        a. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
        b. 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.
14. **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.
15. **DODD** – the Ohio Department of Developmental Disabilities
16. **Education** - Education means activities associated with operating the school including instruction, IHP/IEP preparation, administration, behavioral intervention, extra-curricular activities and other normal school functions. Education shall also include activities associated with early intervention programming.
17. **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.
18. **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.
19. **Facility** means the physical premises and the interior and exterior of a building(s).
20. **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.
21. **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
22. **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.

ORIGINAL

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 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.
25. **Health Plan** - Health plan means an individual or group plan that provides, or pays the cost of medical care. Health plan 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.
26. **HIPAA** - HIPAA means the Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 - 1320d-8.
27. **ICF/MR** - An ICF/MR is an intermediate care facility for persons with mental retardation, 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.
28. **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.
29. **Individual, or Individual receiving services** – Means a person who receives services from ACBDD. 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.
30. **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.
31. **Integrity** means the property that data or information have not been altered or destroyed in an unauthorized manner.
32. **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.
33. **Limited Data Set –** 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;

ORIGINAL

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.

34. **Malicious software** means software, for example, a virus, designed to damage or disrupt a system.
35. **MOU** - MOU means a Memorandum of Understanding between governmental entities which incorporates elements of a business associate contract in accordance with HIPAA rules.
36. **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
37. **Password** means confidential authentication information composed of a string of characters.
38. **Personally Identifiable Data** - Personally Identifiable Data" includes:
    A. The name of the enrollee, the enrollee's family member.
    B. The address of the enrollee.
    C. A personal identifier, such as the enrollee's date of birth, Social Security number, or Medicaid number.
    D. A list of personal characteristics or other information which would make it possible to identify the enrollee with reasonable certainty
39. **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 ACBDD and the minor.
40. **PHI** – PHI, short for "Protected Health Information" means individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. For the purposes of this manual, PHI shall also include "Education Records" which are records created by ACBDD or a Business Associate that are directly related to a student who is served by ACBDD
41. **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.
42. **Protected Health Information –** See **PHI** above.
43. **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.
44. **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.
45. **Security or Security measures** encompass all of the administrative, physical, and technical safeguards in an information system.
46. **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.
47. **Social Engineering --** "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" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). . . .. 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.
48. **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.
49. **Technical safeguards** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

ORIGINAL

50. **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.
51. **Unsecured protected health information –** protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology in guidance specified by the Secretary of the Department of HHS in guidance published on the HHS Web site.
52. **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.
53. **User** means a person or entity with authorized access.
54. **Violation**. There are different types of violations, with different contexts:
    a. **Privacy Violation.** Allowed uses and disclosures of PHI are described in considerable detail in policies and procedures in this manual. For the purposes of this policy, a "privacy violation" is any use or disclosure which is not explicitly allowed in these policies.
    b. **Employee Security Procedure Violation**. The failure of an employee to comply with one or more of the policies and procedures described in the HIPAA Security Policies section of the policies and procedures manual.
    c. **Minor Violation**. A minor violation is defined as a breach of policies, due to either carelessness or ignorance, which results in minimal harm
    d. **Intentional Violation**. A breach of policies done deliberately and knowingly by an employee, but which results in no personal gain and not done for malicious intent.
    e. **Grievous Violation**. A breach of policies which is done either with malicious intent or for personal gain.
55. **Workforce Member** - Workforce Member means the same as employee. See definition above.
56. **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.

APPROVAL:

_____

Superintendent

ORIGINAL

1010 Confidentiality – General Rules

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

POLICY
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 ACBDD 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 ACBDD shall not use or disclose PHI except in accordance with applicable requirements.

AUDIENCE
All Staff

AUTHORITY
45 CFR Part 160 and 164 (current as/of 8/1/2010)
45 CFR 164.504(g) for entities with multiple functions
ORC § 5126.044 Ohio law on confidentiality (effective 9/22/2000)
OAC § 5123:2-1-02(I)(7) General DD Board confidentiality requirements (3/21/2002)
OAC § 5123:2-4-01(C)(2)(b) General requirements for DD Board confidentiality policies (effective 4/12/2001)
45 CFR 164.502(a)(1)(iii) incidental uses and disclosures
OAC § 3301-51-04 Confidentiality (effective 7/1/2008), for schools
34 CFR 99 FERPA (current as of 8/13/2010)
34 CFR 300 and 301 Part B IDEA (Individuals with Disabilities Education Act, ages 3-21)
34 CFR 303 Part C IDEA (individuals with Disabilities Education Act, ages 0-2)
34 CFR 303.402 and 460 Early Intervention Confidentiality Provisions
34 CFR 300.610 - 627 Children with Disabilities Confidentiality and Parent Rights Provisions

PROCEDURES
1) Staff of the ACBDD 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 Policy 1050 Authorizations.
   C) As permitted in Policy 1040 Speaking with the Family or Friends of an Individual Receiving Services.
   D) As permitted by in Policy 1090 Disclosures that do Not Require an Authorization.
2) For all of the above, the minimum amount of information should be disclosed, and specific procedures followed as detailed in 1020 Minimum Necessary Policy.
3) All employees are responsible for safeguarding the information regarding individuals we serve, as detailed in
   A) Policy 1030 Confidentiality Safeguards (Oral & Written)
   B) Policy 3080 Computer Usage
   C) Policy 3082 Use of Social Networking Sites including Facebook, Twitter, LinkedIn, MySpace and others
   D) Policy 3085 Portable Computing Devices and Home Computer Use
4) Rights of individuals served by ACBDD may be exercised by parents, guardians and personal representatives as detailed in Policy1070 Minors, Personal Representatives and Deceased Individuals.
5) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in Policy 1080 Duty to Report Violations and Security Incidents.
6) Supervisors, managers and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.

ORIGINAL

1020 Minimum Necessary Policy

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

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.. This minimum necessary provision shall **NOT APPLY** to the following outlined uses and disclosures of PHI:

- For treatment purposes;
- For information requested by the individual (or the individual's personal representative);
- For information requested pursuant to a valid authorization by the individual;
- For compliance with standardized Health Insurance Portability and Accountability Act (HIPAA) transactions; or
- Disclosures required by law or for monitoring purposes shall be made in accordance with the authority seeking the information.

AUDIENCE
All Staff

AUTHORITY
45 CFR 164.502(b)(1) minimum necessary standard

PROCEDURES

1) **Implementation Approach**. The board will systematically examine its operations and enact protocols in order to use or disclose the minimum amount of information necessary to accomplish its work. This examination will focus on implementing minimum necessary for
   A) Uses of PHI – limiting workforce access to the minimum necessary for specific individual's jobs
   B) Disclosures of PHI
   C) Requests for PHI

   Further, in implementing the minimum necessary principle, the board will require all persons who handle PHI in any manner are expected to know and abide by the following protocols:
2) **Limiting Workforce Access to PHI**: Access to the PHI will be granted based on the individual's role and determined by the Director and Privacy Officer of ACBDD. ACBDD will identify:
   A) 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
   B) 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.
   C) Safeguards will be developed and documented to restrict workforce access to the minimum necessary, especially as detailed in Policy 3015 Facility Security and Access Control.
   D) The Privacy Officer will document the results of this analysis. See the Appendix E Workforce Access to PHI and Safeguards.
3) **Limit Uses, Disclosures and Requests of Entire Medical Records** – All personnel should take care to avoid using, disclosing, and requesting the entire record of individuals we serve unless this is absolutely necessary.
4) **Good Faith Reliance** – ACBDD staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:
   A) 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
   B) The request is from another **covered entity**;
   C) The request is from a **professional** at ACBDD, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary

ORIGINAL

Procedures for Routine Disclosures

Protocols for routine disclosures are designed to limit the information disclosed to the minimum necessary. The Privacy officer will update these protocols as necessary.

1) **Medical and Ancillary Providers** – Information required to complete orders or to develop services for individuals will be disclosed to contracted providers, using ACBDD forms, prior to any service being rendered.
2) **Software & Network Providers** – Information in the computer system is incidentally available during system support activities.
   A) **Don't Panic.** Network support vendor Don't Panic is under contract to provide 24/7 network support. Access is provided at all times.
   B) **Gatekeeper and other Support.** Primary Solutions and other support vendors will be granted access rights on an as needed basis. Technical solutions for implementing this authorization will be deployed by the board.
3) **Job and Family Services** – For services rendered, which are reimbursed by ODJFS, submit requested information to JFS.
4) **Service Coordination with Mental Health Board & Other Behavioral Service Providers -** For coordination of care, psychological assessments and progress notes will be sent under the signature of the Director of Support Services to the mental health board and other behavioral health providers
5) **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.
6) **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.
7) **Auditor's Office –** When authorizing payment of bills, fiscal files may be reviewed by the Auditor's office prior to authorization of payment.
8) **Residential Providers –** To ensure quality of care for individuals, the Director of Service and Support can release IP's related to work goals, medication history, limitations and side effects, dietary needs and guardian/family contact information will be shared with contracted providers. Other requests for information from the providers will be reviewed by the Director of Service & Support.
9) **Department Of Developmental Disabilities –** Information will be shared routinely with 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.
10) **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.
11) **Transportation Providers –** To ensure quality of care for individuals, medical needs and guardian/family contact information will be shared with contracted providers.
12) **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.
13) **Bureau of Disability Determination –** Using the Bureau's forms, assessment information will be shared in order to determine individual's eligibility for benefits.
14) **Attorneys –** When a subpoena is presented, the protocol in Policy 1090 Disclosures that do Not Require an Authorization will be carefully followed to determine, with legal counsel assistance, if the subpoena should be honored.
15) **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.
16) **Vocational Training Providers -** For coordination of services, medical assessments, limitations, progress notes and behavior support plans will be sent by the Director of Adult Services, the Director of Supported Employment, or a habilitation specialist to the vocational training provider
17) **Law Enforcement –** As identified by the Director of Services & Supports, guardianship, family contact information and behavior support plans will be shared with law enforcement agencies. In addition, upon presentation of a warrant and verification of credentials if presented in person, other file information may be shared with law enforcement agencies. See Policy 1090 Disclosures that do not Require an Authorization.

ORIGINAL

Procedures for Routine Requests

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

Procedures for Non-Routine Disclosures or Requests

1. **For non-routine disclosures**, when subject to the minimum necessary provision, the individual making the disclosure may seek guidance, if necessary, of the Privacy Officer (or his/her designee) to review the request for compliance with the minimum necessary requirements.
2. **For non-routine requests**, the requesting party will utilize the minimum necessary principle.

ORIGINAL

1030 Confidentiality Safeguards (Oral & Written)

Effective Date: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

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

REFERENCES
45 CFR 164.530(c) – Administrative, Technical, and Physical Safeguards
45 CFR 164.530(c)
ORC § 5126.044 Ohio law on confidentiality
OAC § 5123:2-1-02(I) Safeguard requirements for confidential DD Board records
OAC § 5123:2-4-01(C)(2)(b) General requirements for DD Board confidentiality policies
OAC § 5123:2-12-02(J)(2) Obsolete
OAC § 5123:2-15-01(C)(6) Obsolete
OAC § 5123:2-3-13(B) Safeguards for records in licensed facilities

PROCEDURES:
1) General Procedures
   A) Employees shall be familiar with Appendix G Facility Security and Access Plan regarding staff, individuals receiving services, parent and other visitor access to the facility.
   B) Employees shall escort visitors through the premises.
2) 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.
3) 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 should 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 PHI is discussed through teleconference or video feed, ACBDD employees must limit access to the teleconference or video to authorized personnel only.
   F) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.
4) Safeguards for Written PHI.
   A) Control of the Main Record Room and site Record Rooms
      1) The HIPAA Privacy Officer shall be responsible for administering the security controls for the Main Record Room , located in the Beacon School facility.
      2) The Main Record Room shall be kept locked and secured. Designated employees with access to these records shall have a key and/or combination for the storage room. Only these employees shall be permitted in the storage area.
      3) These files shall be put away promptly when not being used.
      4) In general, records shall not be removed from the building without the authorization of the Superintendent, Privacy Officer or designee. Exceptions to this rule will occur when chart must be used off-site, such as for the court, at a school visit or for other off-site services. While away from the office, employees with records must use appropriate safeguards, such as storage in locked trunk and/or locked briefcase. Charts removed from the premises should be logged in the Chart Disclosure Log. The log shall promptly be updated when the records are returned.
      5) Individual records shall be retained per Policy 54 Retention of Board Records.

ORIGINAL

B) Other use and storage of paper records
   1) Employees should minimize the use of hardcopy PHI
   2) 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.
   3) Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer or a secured cabinet.

C) Faxing Procedure
   1) 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
   2) Care should be taken to transmit fax to the proper recipient
   3) Faxed documents should not be left at a common or shred fax machine.

D) Printing and Copying PHI
   1) 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.
   2) Shared printers/copiers with mailbox features will be configured to provide access only to the employee who requested the print job.
   3) PHI printed to a shared printer/copier should be promptly removed.

E) Transportation/outside use of documents with PHI
   1) Caseworkers and other employees who remove documents from the facility, to conduct field work, for example, are responsible for safeguarding these documents.
   2) When leaving documents unattended in a personal vehicle, the vehicle should be locked. Preferably, the documents and/or their container should not be visible.
   3) If any documents with PHI are lost or stolen, the incident should be immediately reported to a supervisor and the Privacy Officer.

F) 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) Unneeded paper documents containing PHI shall be destroyed by shredding them or placing them in one of the locked bins to be processed by a shredding service vendor.

H) 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 incidental exposures to cleaning personnel and others who may use the facilities at night.

J) Cleaning personnel with access to the facility should be placed under a confidentiality agreement.

5) 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 supervisor, as well as any appropriate disciplinary actions taken.

6) 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.

7) Annual Review. These safeguards shall be reviewed and updated annually.

ORIGINAL

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

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

POLICY
ACBDD 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.

AUDIENCE
All Staff

AUTHORITY
45 CFR 164.510(b)

PROCEDURES

1) If the individual is present
   a) 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
      1) verbally seeking permission for the disclosure, and the individual the agrees, or
      2) giving the Individual the opportunity to object to the disclosure, and the individual does not express an objection, or
      3) 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
      1) 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 ACBDD, when the Individual is not present, the employee may use their professional judgment to determine if the disclosure is in the best interest 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
      1) 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.

ORIGINAL

1050 Authorizations

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

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

AUDIENCE

AUTHORITY
45 CFR 164.508 – HIPAA requirements for authorizations
ORC § 5126.044 – Ohio Statute on confidentiality of records
OAC § 5123:2-1-02(I)(7) – Ohio Rule on confidentiality of records
34 CFR 99.30 - FERPA requirements for prior consents to disclose information
34 CFR 99.32 FERPA recordkeeping requirements concerning requests and disclosures

LEGAL NOTES
- FERPA applies for records created for education activity; HIPAA applies to all other records

PROCEDURES
1) Unless otherwise authorized by ACBDD policy, state or federal law, disclosures require specific authorization by the Individual or his/her legal representative. A standard authorization form is included as an Appendix. 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 ACBDD will not condition treatment if the individual does or does not sign 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) 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) ACBDD is aware authorization has been revoked

ORIGINAL

e) ACBDD is aware information is false.

f) Authorizations to release PHI are not combined with other documents

3) For authorizations presented in person for immediate release, the staff member shall verify the identity of the recipient according to Policy 1060 Verification, after which the information may be released.

4) 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 and the Disclosure Log will be updated with the following information:

1) The date of the disclosure

2) The name of the entity or person who received the PHI, and, if known, the address of such entity or person

3) A brief description of the PHI disclosed

4) A brief statement of the purpose of the disclosure

5) If the disclosure was due to a health or safety emergency, a description of the significant threat to health or safety

5) The ACBDD must retain the written or electronic copy of the authorization for a period of seven (7) years from the later of the date of execution or the last effective date.

6) Upon instructions of revocation of authorization, ACBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure. The Disclosure Log will be updated.

7) Information from other service providers contained in the Individual's record may be released with the Individual's written authorization.

ORIGINAL

1060 Verification

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective; 11/23/10

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

PROCEDURES

WHEN REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY, IDENTITY AND AUTHORITY ARE VERIFIED WITH THE FOLLOWING SAFEGUARDS:

1) In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI, ACBDD personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing PHI:
   a) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI
   b) Presentation of an agency identification badge, other official credentials, or other proof of government employed status if the request is made in person
   c) A written statement on appropriate government letterhead that the person is acting under the government's authority
   d) Other evidence of documentation from an agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official
   e) A written statement of the legal authority under which the information is requested
   f) If a written statement would be impracticable, an oral statement of such legal authority
   g) A request that is made pursuant to a court order and subpoena or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority
2) The following issues should be addressed before releasing PHI once a request is received:
   a) Is the requestor who she/he claims to be
   b) Does the requestor have the authority to request PHI. If the request involves a court order, subpoena, or other legal request, follow the procedures outlined in the Policy 1090 Disclosures that do Not Require an Authorization.

WHEN REQUESTS FROM AN INDIVIDUAL RECEIVING SERVICES, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE ONLY IDENTITY IS VERIFIED WITH THE FOLLWING SAFEGUARDS:

1) In no case should any statement be made which acknowledges that an individual is receiving services from the Board. Employees must immediately indicate this policy to the requestor (if done in person or on the telephone), accept the information requested, and tell them you will get back to them if you are legally able.
2) Individuals receiving services and parents often are all known to staff. In the event that the individual or parent is not known, or a Personal Representative who is unknown requests protected health information, the employee shall verify the identity of the personal representative:
   a) Ask another employee if they know the person
   b) Question the personal representative regarding their knowledge of information in the record of the individual being served, such as birth date, social security number, etc., which only an authorized person would typically know.

ORIGINAL

1070 Minors, Personal Representatives and Deceased Individuals

Adopted Date: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

PURPOSE
Establish requirements to maintain confidentiality, permit the legal release of protected health information (PHI) to minors and personal representatives, and release of PHI of deceased individuals.

AUTHORITY
ORC 5126.044
45 CFR 164.5xx

PROCEDURES:
1) Minors who are legally allowed to consent to treatment under Ohio Law, may exercise all rights regarding access to, requests for amendment, and the release of their PHI pursuant to a written authorization.
2) ACBDD recognizes an individual's personal representative are authorized to exercise rights of access and/or inspection of PHI,request amendment of PHI, and sign the ACBDD Authorization Form for the release of PHI.
3) ACBDD 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 ACBDD has received a court order or other documentation limiting privileges of a non-custodial parent as provided below.
      1) Abuse, Neglect, and/or Endangerment Situations. Notwithstanding a state law of any requirement of this paragraph to the contrary, ACBDD may elect not to recognize a person as a personal representative of an individual. In order for ACBDD to choose not to recognize a person as a personal representative, ACBDD 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:
         a. The individual has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative.
         b. Treating such person as the personal representative could otherwise endanger the individual.
      2) Receipt of a court order limiting privileges of a non-custodial parent. In the event that ACBDD 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, ACBDD shall adhere to the restrictions in the court order.
2) Deceased Individuals:
   a) 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. ACBDD 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) 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) 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.
      1) Spouse (if married)

ORIGINAL

2) The individual's children
3) The Individual's parents
4) The Individual's brothers or sisters
5) The individual's uncles or aunts;
6) The individual's closest relative by blood or adoption
7) The individual's closest relative by marriage

ORIGINAL

1080 Duty to Report Violations and Security Incidents

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective 11/23/10

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

REFERENCES:
HIPAA Privacy Rules, 45 CFR Part 164
164.530(e)(1) –Sanctions

PROCEDURES:
1) Any employee observing a violation of any of the Confidentiality and Computer Security policies is to report the violation to his/her supervisor. Failure to report a Privacy Violation is in itself a disciplinable offense.
2) The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, individuals receiving services, or others, and/or review of computer or paper audit trails.
3) For security breaches, the Privacy and/or Security Officer will follow any procedures detailed in Policy 3035 Breach Reporting.
4) For Privacy Violations, the Privacy Officer will follow procedures in Policy 3085 Mitigation.
5) A written incident report will be written by the Privacy and/or Security Officer. It will be filed
   A) in the Privacy Officer's Privacy Violations file
   B) in the employee's personnel file
6) Employee Discipline, if appropriate, will be taken and documented in accordance with the following policies:
   - 8.1 Disciplinary Process – Unclassified Employees
   - 8.2 Disciplinary Process – Classified Employees
   - 8.5 Progressive Discipline Policy
7) A post-incident review will be conducted by the Privacy and/or Security Officer, and may recommend corrective action, such as a change in policy, additional training, or other appropriate action.

ORIGINAL

1090 Disclosures that do Not Require an Authorization

POLICY
ACBDD 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.

AUTHORITY
45 CFR § 164.512
ORC § 2151.421(A) Reports of Child Abuse
ORC § 2305.51 Disclosures to prevent harm to 3rd parties
ORC § 2317.02(B) Privilege for physicians, school guidance counselors, licensed social workers and licensed counselors
ORC § 4732.19 Privilege for psychologists
ORC § 5123.19 Licensure activities of DODD
ORC § 5123.60 OLRS
ORC § 5123.61(C)(1) Duty to report abuse/neglect of persons with DD
ORC § 5126.044 Confidentiality for DD Boards
ORC § 5126.055 LMAA functions of DD Boards
ORC § 5126.31 Case Review and Investigation
OAC § 5123:2-15-10(G) Access to documentation for CAFS payments
OAC § 5123:2-17-02(B) Incidents adversely affecting health/safety
OAC § 5123:2-17-02(D) Reporting MUIs
OAC § 5123:2-3-04 Monitoring of licensed facilities
Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena
ORC § 4113.52 Reporting Violations of law by employer or fellow employee
34 CFR Part 99 Subpart D May an Educational Agency Disclose Education Records
20 U.S.C. 7165(b) Section 4155(b) No Child Left Behind Act – Transfer of Disciplinary Records

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.

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

1) **Recordkeeping**. For all of the disclosures authorized below, the employee will document the details of the disclosure on the Disclosure Log 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.

ORIGINAL

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

4) To protect victims of abuse, neglect, or domestic violence

A) Reports of child abuse

1) Reports of child abuse shall be made in accordance with Ohio law.

2) The ACBDD 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.

1) The ACBDD 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:

a. the individual agrees; or

b. the ACBDD 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.

2) The ACBDD staff member making the disclosure must promptly inform the individual whose PHI has been released unless:

a. doing so would place the individual at risk of serious harm; or

b. the ACBDD would be informing a personal representative, and the ACBDD 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 ACBDD, 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 ACBDD receives PHI disclosed under this section in its role as LMAA, the ACBDD may use the PHI to carry out its duties.

6) For judicial and administrative proceedings

A) The ACBDD 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 ACBDD may comply with such legal requests only if:

1) The ACBDD receives satisfactory assurance from the party seeking the information that reasonable

ORIGINAL

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

2) The ACBDD 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 ACBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements.

7) For law enforcement purposes

A) PHI may be disclosed for the following law enforcement purposes and under the specified conditions:

1) 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.
2) Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.
3) The ACBDD may disclose to a law enforcement official protected health information that the ACBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the ACBDD.
4) The ACBDD providing emergency health care in response to a medical emergency, other than such emergency on the premises of the ACBDD, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

If the ACBDD believes that a medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the limitations in the previous section 6)A)4) above does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to item 4) above, “To protect victims of abuse, neglect, or domestic violence”

B) 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:

1) Name and address
2) Date and place of birth
3) Social security number
4) ABO blood type and RH factor
5) Type of injury
6) Date and time of treatment
7) Date and time of death, if applicable,
8) 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.

D) The ACBDD 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 ACBDD may disclose PHI as follows, to the extent permitted by applicable law and ethical standards:

B) 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.

C) 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

ORIGINAL

type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.

D) 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 authorize 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 authorize 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) The ACBDD 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:

1) The provision of health care to such individuals;
2) The health and safety of such individual or other inmates;
3) The health and safety of the officers or employees of or others at the correctional institution;
4) 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;
5) Law enforcement on the premises of the correctional institution; and
6) 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 ACBDD may disclose PHI to his/her attorney, and to other parties specified in Ohio Revised Code § 4113.52, while following the procedures outlined in that statute. See also Policy 10.5 Protection of Whistleblowers.

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.

ORIGINAL

INDIVIDUAL RIGHTS

1200 Individual's Right to Access Records

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

POLICY
Individuals, served by ACBDD, 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.

PROCEDURES
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) An individual or parent may include any 3rd party of their choosing, including an attorney, to review the records.
   C) ACBDD 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 to records shall be directed to the Privacy Officer or his/her designee
   B) The Privacy Officer shall follow the Verification Procedure to verify the identity of the requestor. Any grant of access to someone other than the parent
   C) The ACBDD shall provide the individual with access to their records in any of the following ways requested by the individual:
      1) By inspection. ACBDD shall provide a private room for the individual to review the records under the supervision of a ACBDD staff member who will insure that the record is not altered, or
      2) Photocopy. ACBDD shall provide a photocopy of the entire record or portion of the record requested.
      3) Electronic format. ACBDD shall provide an electronic copy of the entire record, or portion of the record requested, in PDF format to be securely transmitted to the individual PHI in the form or format requested by the individual.

ORIGINAL

D) 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) ACBDD will respond to reasonable requests for explanation and interpretation of the records.
   B) Upon request, ACBDD will provide individuals, parents and guardians a list of the types and locations of records maintained or used by ACBDD.
   C) If the ACBDD does not maintain the PHI that is the subject of the individual's request for access, and the ACBDD knows where the requested information is maintained, the ACBDD will 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
   A) ACBDD at present has no fees for copying records.

ORIGINAL

1210 Individual's Right to Request Amendment of Records

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

POLICY
Subject to the rules set forth in applicable requirements and ACBDD procedures, an individual has the right to have the ACBDD 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.

PROCEDURES
REQESTS FOR AMENDMENTS

1) 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 ACBDD or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
2) The Privacy Officer of the ACBDD is responsible for receiving requests for amendment, processing the requests, arranging for any hearings, and completing required documentation.
3) The ACBDD will act on a request for amendment without unnecessary delay and no later than 60 days after the date of the request.
4) If the ACBDD accepts the requested amendment, in whole or in part,
   A) the ACBDD must make the appropriate amendment, and inform the individual and other persons or entities who have had access to the information.

   Otherwise, if the ACBDD believes the existing record is correct as is, it may deny the amendment:
   A) If an amendment is denied, the ACBDD will give written notice in plain language which includes the following:
      1) The basis for the denial;
      2) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
      3) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the ACBDD 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
      4) The individual's right for a hearing to challenge the information
   B) 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

ORIGINAL

individual requested an amendment and the ACBDD's denial.

C) The ACBDD may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the ACBDD must provide a copy to the individual who submitted the statement of disagreement.

D) 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) At the individual's request, ACBDD will send a copy of the changed record to any party requested by the individual (per ORC 1347.09)

F) 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 ACBDD may separately transmit the information to the recipient of the transaction in a standard EDI format.

RECORDS HEARINGS

ACBDD 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) ACBDD 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 ACBDD, 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, ACBDD 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, ACBDD 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 ACBDD
   - C) Any information placed in the record as a result of this hearing, ACBDD must maintain this statement as part of its permanent record, and include it with any subsequent disclosure.

ORIGINAL

1220 Individual's Right to Receive an Accounting of Disclosures

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective 11/23/10

POLICY
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

PROCEDURES
1) 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) Generally, an individual has the right to request an accounting of disclosures of their PHI by ACBDD 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) Disclosures 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);
2) 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

ORIGINAL

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

3) Unlawful and unauthorized disclosures known by ACBDD

4) Health oversight agencies and law enforcement officials may request a suspension of an individual's rights to disclosure. If such a request is received, ACBDD will follow procedures in 45 CFR § 164.528.

5) The HIPAA Privacy Officer shall comply with an individual's request for an accounting within 45 days of the request. The ACBDD 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:
      1) The date of the disclosure
      2) The name of the entity or person who received the PHI, and, if known, the address of such entity or person
      3) A brief description of the PHI disclosed
      4) 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
      5) 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.
      6) 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) ACBDD will retain documentation (in written or electronic format) for a period of 7 years:
      (1) All information required to be included in an accounting of disclosures of PHI
      (2) All written accountings provided to individual

ORIGINAL

1230 Individual's Right to Request Additional Restrictions

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective 11/23/10

POLICY
ACBDD 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)

PROCEDURES:

1) **Refer the Request to ACBDD' 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 ACBDD' 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 ACBDD will agree**: The ACBDD 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:** ACBDD 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 ACBDD agrees to the restriction, the notice to the Individual will clearly state what restriction ACBDD 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 ACBDD 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 ACBDD 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 seven years from the date of their creation:

   a) Copies of Individual requests for restrictions
   b) Copies of any notice informing the Individual about ACBDD' 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

ORIGINAL

1240 Individual's Right to Request Confidential Communications

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

POLICY:
Individuals (or their parents) are entitled to request confidential communications not be mailed or delivered to their home address. These requests will be honored to the extent that they can be reasonably accommodated with ACBDD administrative systems.

AUDIENCE
Privacy Officer

PROCEDURES:

1. Individuals, or their personal representative, may make a request for confidential communications in writing to the Privacy Officer.
2. 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 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 ACBDD will take to implement the request.
3. 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. The Privacy Officer shall document the request, and disposition, in the Individual's Record.
5. 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.

ORIGINAL

CONFIDENTIALITY POLICIES FOR SUPERVISORS

1300 Business Associate Contracts

Adopted: 6/1/03
Revised Date: 11/23/10
Approved: 6/1/03
Effective: 11/23/10

POLICY
ACBDD 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

PROCEDURES

1) ACBDD will have a written Business Associate Contract with every identified Business Associate. For a COG or other government agencies, a Memorandum of Understanding will be executed. See Appendix A Identifying who Is a Business Associate.
2) 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) The Business Associate Contract will provide satisfactory assurances that the Business Associate will not use or disclose the PHI of ACBDD 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) In the event ACBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, ACBDD will take steps to cure the breach or end the violation. If ACBDD is unable to cure the breach or end the violation, ACBDD will terminate the Business Associate Contract.

ORIGINAL

1310 Notice of Privacy Practices

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

POLICY
ACBDD 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 re distribution upon change.

PROCEDURES

1) **Creation and Update of Notice**.

   A) The HIPAA Privacy Officer shall create the Notice of Privacy Practices to conform with requirements of HIPAA and FERPA. See Appendix F - ACBDD 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 initial on-site contact 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) Every year an updated copy of the notice will be sent to individuals and/or their parents.

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 all ACBDD websites

   C) Copies of the notice will be maintained for 6 years, as detailed in Policy 54 "Retention of Board Records"

ORIGINAL

1320 Non-intimidation and Non-retaliation

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

POLICY:
ACBDD 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 ACBDD policies are not consistent with the law, or not being implemented properly. ACBDD will not require any individual receiving services to waive any of his/her rights under HIPAA as a condition of education, treatment, or enrollment.

PROCEDURES

1) ACBDD 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:
      1) Filing of a complaint with the Secretary under HIPAA compliant
      2) Testifying, assisting or participating in an investigation, compliance review, proceedings or hearing under Part C of Title XI; or
      3) 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 ACBDD, is strictly prohibited.
4) Prohibition against Waiver of Rights -- No office, program, facility or employee of the ACBDD 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.

ORIGINAL

1330 HIPAA Assignments and Documentation

Adopted: 6/1/03
Revised Date: 11/23/10
Approved: 6/1/03
Effective: 11/23/10

POLICY:
ACBDD 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/MR)
OAC § 5101:3-40-01 (ISPs for IO Waiver)
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.
OAC § 5123:2-15-01(C)(6) (Habilitation Center/TCM records)
OAC § 5123:2-15-10(G)(2) (CAFS records)

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

PROCEDURES:
1) 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) 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 Policy 1310 Notice of Privacy Practices.
   C) Restrictions on use or disclosure of PHI by ACBDD as described in the Policy1230 Individual's Right to Request Additional Restrictions.

ORIGINAL

D) Records of disclosures, as required by the Policy 1220 Individual's Right to Receive an Accounting of Disclosures.
E) Any signed authorization as described in Policy 1050 Authorizations.
F) All privacy-related complaints received, and their disposition, if any, as described in Policy 1340 Privacy Complaints.
G) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Policy 1080 Duty to Report Violations and Security Incidents.
H) Incident Reports and other documentation specified by Policy 3035 Breach Reporting.

The above records will be maintained for 6 years

2) 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".
3) Updating Required Designations. The Privacy Officer, will maintain and update HIPAA Required Designations as necessary.
4) Compliance Notes. The Privacy Officer and Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, internal audit activities.
5) Internal Audit. The Privacy Officer shall conduct a periodic audit, as necessary, to insure proper maintenance of all documentation itemized in this policy.
6) See also Policy 54 Retention of Board Records for retention periods and destruction procedures.

ORIGINAL

1340 Privacy Complaints

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

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

AUDIENCE
All Staff

AUTHORITY
45 CFR 164.530(d) HIPAA complaint procedures
ORC § 5123.64(A) requires establishment of a complaint procedure
OAC § 5123:2-1-12 administrative resolution of complaints involving the programs, services, policies, or administrative practices of a county board or the entities acting under contract with a county board

PROCEDURES
1) The HIPAA Privacy Officer shall manage this complaint process, and shall be designated in the Notice of Privacy practices as the individual to receive complaints.
2) The ACBDD will extend the provisions of Policy 10.5 "Protection of Whistleblowers", to all individuals who file confidentiality or privacy related complaint.
3) An employee or individual should file their complaint in writing to the privacy officer. Employees may review Policy 10.5 "Protection of Whistleblowers" which provides for alternate officials to receive the written complaint.
4) Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Superintendent) shall review and investigate the complaint.
5) If warranted, the Privacy Officer shall take corrective action, which may include
    1) Change of policy and/or procedure.
    2) Intervention with an employee who is not following procedures including additional training and/or sanctions
    3) Other action as appropriate
6) The Privacy Officer shall communicate the results of the investigation and any corrective action taken to the individual filing the complaint.
7) The ACBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Policy 1330 HIPAA Assignments and Documentation.

REFERENCES

ORIGINAL

1350 Policy Updating and Staff Training

Adopted: 7/1/03
Revised Date: 11/23/10
Approved: 7/1/03
Effective: 11/23/10

POLICY:
ACBDD 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
OAC § 5123:2-7-01 training requirements for TISC Gone!

PROCEDURES:
1. 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. The HIPAA Privacy Officer shall insure that all new staff will be receive training on ACBDD Confidentiality and Computer Security policies promptly after hiring. See Policy 3.6 Staff Orientation.
3. The HIPAA Privacy Officer shall insure that staff receive training on Confidentiality and Computer Security policies when they are substantially changed. This training shall be implemented as detailed in Policy 4.4 Training.

ORIGINAL

HIPAA SECURITY POLICIES

POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER

3000 Security Management Process

Adopted: 2/1/05
Revised Date: 9/1/2010
Effective: 11/23/10

ORIGINAL

POLICY
ACBDD will appoint a Security Officer. The 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.

PROCEDURES

1) The Superintendent will designate a Security Officer. The job responsibilities for this individual are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer. The 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 Security Officer will be retained with other HIPAA-mandated designations per Policy 1330 HIPAA Assignments and Documentation.
2) The Security Officer will be responsible for security management process. This will include:
   A) **Security Team**. The 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:
      a) The county board will use the risk assessment methodology detailed in NIST SP 800-30 (July 2002)
      b) The results of this assessment shall be documented and maintained for 6 years
      c) 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
      a) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices
      b) 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.

c) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
d) Train board staff regarding compliance
e) Monitor Board compliance with the information security policies, and take action as appropriate based on this monitoring

D) **Information System Inventory**. The HIPAA Security Officer and/or Security Team shall maintain an inventory of the hardware, software and networking infrastructure.
   a) Content of Inventory:
      (i) 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 document physical location, primary user, manufacturer / model / serial number.
      (ii) Network infrastructure documentation will include network topology and all other information necessary to recreate the network in the event of a catastrophic event
      (iii) Software inventory will include hardware installed on, Software manufacturer, program name, version number, license/serial number and date.
   b) Update frequency. This inventory should be updated on an ongoing basis with a physical inventory no less frequent than annually for mobile devices.
   c) Backup copy. A copy of this inventory shall be maintained off-site to insure availability in the event of a fire or other disaster.

REFERENCES

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, 2001
NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, 2001
CERT at www.cert.org
SANS at www.sans.org

Center for Internet Security at www.cisecurity.org

ORIGINAL

3005 Data Backup

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES

1) **Data Criticality Analysis**. Data identified as either Critical or Important, as described below, shall be backed up each evening:
   A) **Critical Data**:
      a) Infallible System Data
      b) Gatekeeper Data
      c) Human Resources Data
      d) Accounting Data
   B) Important Data
      a) E-Mail system
      b) Other Administrative Data
      c) User Directories (word processing documents, spreadsheets, other data)

   Non-unique Data, identified below, is less critical since it can be recreated by reloading from vendor supplied media, and is backed up routinely.
   A) Non-unique Data
      a) Operating System, other system software, and Applications software
   B) **Multiple Backup Generations**. Three backup methodologies are employed as follows:
      a) The server uses RAID technology whereby three (3) copies of system and user data are constantly maintained on three disks. Should an individual disk fail the operating system switches to one of the other units and continues processing data.
      b) End of Day user and application data backups are created daily and retained for 30 days.
      c) An offsite backup of user and application data is created and forwarded daily to one of the other ACBDD locations.
2) **Backup Software**. Appropriate vendor-supplied backup software shall be maintained and copies are maintained at one of the other ACBDD locations.
3) **Responsibility**. The Security Officer shall designate an employee and an alternate with the responsibility to verify that each backup was successful. All individuals responsible for this critical function should be trained and familiar with how to review the log file in the backup software to verify the proper operation of each backup.
4) **Backup Log**. The server maintains a daily event log to document the daily backups and their final status. Problems shall be immediately reported to the Security Officer or the Superintendent.
5) **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT**.** On a quarterly basis, a trial restore shall be performed 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.
6) **Data Recovery Plan.** The Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

ORIGINAL

3010 Disaster Recovery Plan and Emergency Mode Operation

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
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 Security Officer

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

PROCEDURES

1) **Disaster Recovery Team**. If appropriate, the 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 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 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 RAID arrays, backup power supplies, fire suppression systems, raised floors, security systems, database transaction logging and the like.
4) **System and Data Recovery Plan**. The 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 "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. Disaster Recovery Plans may include:
      (i) Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster
      (ii) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by board management
      (iii) Contracts with hot and/or cold system sites if deemed necessary and prudent by board management
      (iv) 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 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 MUI/UI's involving health emergencies,
   B) Maintenance of Critical Individual Data will include on a second media to protect against loss of access due to technical failure,

ORIGINAL

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 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.

REFERENCES

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

ORIGINAL

3015 Facility Security and Access Control

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES

1) **Facility Security Planning**. The 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 Security Officer shall be responsible for employee training on their duties and responsibilities for facility security as described in the facility security plan.
3) **Maintenance of Physical Security Equipment**. The Director of Facilities 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 Public Access Areas, shall, in a polite manner, escort the person to a common area. Any suspicious incident shall be reported to the Security Officer and/or police.

REFERENCES

NIST SP 800-66

ORIGINAL

3020 Annual Security Evaluation

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
Annually the 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 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

PROCEDURES
1) On an annual basis, the Security Officer will review any updates to federal HIPAA and FERPA 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 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) The Security Officer shall submit their report to the Superintendent including any recommendations.
3) The results of the review will be documented, and documentation shall be retained for 6 years.
4) 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.

ORIGINAL

3025 Audit Control and Activity Review

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES
1) **System Activity Logs**. Activity logs shall be enabled at the following levels
   A) Network Software (Windows NT): 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 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 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 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 of 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.

ORIGINAL

3030 Malicious Software Protection

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES
1) The HIPAA Security Officer will insure that all computers in the facility are protected with reputable software for protection against malicious software. This software should protect against the various categories of malicious software, including viruses, Trojans, Adware, and spyware.
2) Appropriate configuration options will be established in the software to protect against malicious software contained in:
   A) Incoming e-mail and e-mail attachments
   B) Files imported or exported to any external disk or portable devices
   C) Necessary procedures will be implemented to update daily the virus protection software
3) Annual review of this policy and malicious software protection will be conducted to insure that the products, services, and configuration, and policies appropriately manage risk for this threat.

ORIGINAL

3035 Breach Reporting

Adopted: 9/1/09
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
The board will notify Individuals, 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

DEFINITIONS

PROCEDURES
1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer shall determine if the incident meets the definition of a breach. Legal counsel and other expert advice shall be obtained, if appropriate, for additional guidance.
   A) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule?
   B) Does one of the statutory exceptions apply?
   C) Finally, after completing a risk assessment process, is there a significant risk of financial, reputational, or other harm to the individual?

   The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1330 HIPAA Assignments and Documentation.
2) **Breach Notification**. In the event of a breach, the HIPAA Security Officer shall
   A) Notify Individual(s) affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      a) In the event of an urgent situation, the board may use telephone, email or other means to immediately notify individuals of the breach.
      b) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following::
         (i) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known
         (ii) A description of the types of unsecured protected health information that were involved in the breach
         (iii) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
         (iv) A brief description of the actions to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
         (v) 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
      c) Send the primary breach notification to
         (i) 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
         (ii) Parent, guardian, or Personal Representative of the Individual
         (iii) The next of kin in the event that the individual is deceased and the next of kin name and address are available
      d) 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):

ORIGINAL

(i) 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
(ii) In the event that 10 or more individuals are not reachable by first class mail,
(a) A toll-free phone number shall be established, and staffed with operators, for at least 90 days
(b) a notice shall be conspicuously placed on the board's web site home page with details of the above details on the breach plus contact information

B) Notify the news media if more 500 Individual records are involved in the breach
a) Under direction of the board superintendent, a press release shall be prepared detailing the information in section 2Ab above, and other relevant information.
b) 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
a) 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
b) 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.

3) **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.

4) **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 and includes a specific 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.

5) **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.

ORIGINAL

3040 Security Awareness Program

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
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)

PROCEDURES
1) 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) New and "hot" information from e-mail advisories, online IT security news sites, and periodicals
   C) Issues with new technologies such as the latest Smartphone

   A variety of media and avenues should be explored such as sign-in banners, security reminder cards for posting at workstations, articles in employee newsletters, posting on bulletin boards, etc. At a minimum, Computer Security Awareness will be included annually as detailed in Policy 4.5 Staff Ongoing Training.

ORIGINAL

3050 Device and Media Disposal and Re-Use

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
HIPAA Security Officer

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

PROCEDURES

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 removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee or direct supervisor shall request clearance of the HIPAA Security Officer shall be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed. If the removable device is lost or stolen, the user will notify the HIPAA Security Officer and will be required to report what type of information was stored on the device.
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 will be given to the HIPAA Security Officer and will be physically destroyed by Facility staff that will document destruction and include description and serial number if available.
   B) **Hard Drives and floppy disks**. Hard drives and floppy disks will be physically destroyed by Facility staff that will document destruction and include description and serial number if available.
   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) PHI stored on media
   E) Backup Made of Information (Yes/No)
   F) If Yes, location of backup
   G) Item Disposition (Clear/Purge/Destroy)
      a) Date Conducted:
      b) Conducted by
      c) Phone #
      d) Validated By
      e) Phone #
   H) Sanitization Method used
   I) Final disposition of media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer /Other)

ORIGINAL

3060 Technical Safeguards

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
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)

PROCEDURES
1) **Firewalls.** Hardware and/or software firewalls shall be employed to protect against network intrusions. These should be configured to enforce board policies, such as blocking of internet e-mail sites, and other safeguards.
2) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   A) The beacon shall be disabled
   B) The SSID should be changed from the default
   C) WEP should be enabled
   D) Controls shall be employed to allow access only to workstations owned by the board and authorized to use the network.
   E) These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
3) **E-mail**. For transmission of PHI, secure e-mail should be employed using one of a variety of approaches, including:
   A) PGP
   B) S/MIME
   C) Transmission over a VPN
   D) TLS/SSL
   E) Run e-mail inside of SSL
   The E-mail system should be configured to enforce board policies, such as the blocking of attachments which are executable programs.

   See also Policy 3080 Computer Usage.]
4) **Encryption of desktop, mobile devices and portable media**. Encryption of end-user devices is determined appropriate based on risk analysis. ACBDD shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, the board
   A) All portable devices will be encrypted when not in use by the assigned user.
   B) ACBDD will use centralized management for all deployments of storage encryption with exceptions cleared by the HIPAA Security Officer,
5) **Transmission Security**. For data in motion, the HIPAA Security Officer will mplement 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*

ORIGINAL

D) Other FIPS 140-2 validated processes

6) **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 criteria for continued use of and/or procurement of any new operating or application software.
7) **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.
8) **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.
9) **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.

ORIGINAL

3065 Mitigation

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
In the event of an inappropriate use or disclosure of an individual's PHI, the ACBDD 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(e)(1) – Standard Sanctions
164.308(a)(a) – Security Management Process, Sanctions Policy

DEFINITIONS

PROCEDURES
1) 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.

ORIGINAL

3070 Electronic Signatures

Adopted: 7/22/08
Revised Date: 7/22/08
Effective: 11/23/10

POLICY
Electronic signature, an automated function which replaces a handwritten signature with a system generated signature statement, will be utilized for records as a means for authentication of transcribed documents, computer generated documents and/or electronic entries. System generated electronic signatures are considered legally binding as a means to identify the author of record entries and confirm that the contents are what the author intended.

Employees and Providers will be allowed to utilize electronic signature in accordance with this policy and State and Federal regulations regarding such.

AUDIENCE
Employees Using Electronic Signatures; Managers

AUTHORITY
ORC § 304
ORC § 1306

PROCEDURES
1) APPROVAL – A separate Electronic Transaction Report or Form will be filled out for each similar transaction per state and federal laws and guidelines.
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 be at least five characters long.
   C) Personal Identification Numbers (PIN)/ Secondary Passwords – 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

ORIGINAL

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

4) AUDITING ELECTRONIC SIGNATURE PROCUDURES
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.

ORIGINAL

SECURITY POLICIES FOR HR STAFF & SUPERVISORS

3075 Employee System Access and Termination Procedures

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
Human Resource Department, Supervisors, HIPAA Security Officer

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

PROCEDURES

AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS

Audience: Security Officer, Privacy Officer

1) 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) 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) The authority to grant access to information systems rests with board of directors and is delegated to the HIPAA Security Officer. 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) 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) The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
6) 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.

ORIGINAL

SYSTEM AND FACILITY ACCESS FOR NEW HIRES

Audience: Supervisors, Human Resource Department

1) Supervisors and/or the human resources department shall direct requests for access to information systems to the HIPAA Security Officer or his/her designee. .
2) 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) 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) As described above, the HIPAA Security Officer will maintain documentation of system access rights.
5) 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) Automatic Logoff. The HIPAA Security Officer shall configure user accounts to automatically logoff after 10 minutes of inactivity. The HIPAA Security Officer may designate certain devises with a different logoff period.
7) 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.

PASSWORD MANAGEMENT

Audience: Security Officer

1) All employees change their passwords whenever they wish. The HIPAA Security Officer or designee may force a change in passwords at anytime. Employees will be notified when their password has been changed and provide a temporary password to use until they change the password themselves.

EMPLOYEE JOB CHANGES

Audience: Human Resources Department, 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.

EMPLOYEE TERMINATION

Audience: Supervisors, Human Resource Department, Security Officer

1) 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) The HIPAA Security Officer shall document the disabling of system access.
3) For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the HIPAA Security Officer so 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.

EMERGENCY SYSTEM ACCESS

Audience: Supervisors, 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

ORIGINAL

another staff person in that department) to provide the necessary access on an expedited basis.

HIPAA ADMINISTRATIVE REQUIREMENTS

SECURITY POLICIES FOR ALL STAFF

3080 Computer Usage

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

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

AUDIENCE
All Staff

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

PROCEDURES FOR THIS POLICY:

WORKSTATION (Desk Top, Laptop or Employer provided device) USE

1) **System is for Job Duties**. Computer workstations are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the individuals treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, 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 during their lunch and break periods.

   B) Workstations must never be used for any activity that is not related to their job duties. It is difficult to provide a complete list of such activities; a partial list includes:

      a) Downloading, viewing or distributing pornographic, racist, profane or otherwise objectionable material

      b) conducting conversations of a sexual nature

      c) any illegal activity

      d) political activity

      e) operating a business or other means of personal gain

      If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.

   C) Personal use of Social Networking tools, such as Facebook, Twitter, LinkedIn, MySpace and others is detailed separately.

ORIGINAL

D) Employees are not to stay logged in to social networking sites, instant messaging sites/tools, or their personal email except during their lunch or break periods

3) **E-Mail Use**. Employees with board e-mail accounts should check e-mail daily. Board E-mail accounts 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 for information containing PHI is prohibited until ACBDD provides encryption to all email transactions. Be aware that e-mail to outside parties is not secure and must not be used containing Protected Health Information unless it is 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 is considered a public record and is subject to disclosure to the general public as detailed in Policy 77 Public Records Policy.

D) For personal matters, employees must use a personal email account such as Gmail or Yahoo mail.

a) In the event that any board e-mail is received on a personal account, the employee should inform their immediate supervisor and forwarded to the HIPAA Security Officer as it will be treated as a potential breach.

b) In the event that a personal email is received on a Board account, forward it to a personal email account and inform the sender of the correct email address

4) **Storage or Transfer of PHI or Confidential Material to or from Removable Media Prohibited**. Personnel may not copy to or from any ACBDD information to or from removable media, such as Flash drives, CDs, DVD or portable hard drives that has not been authorized by the HIPAA Security Officer.

5) **All Usage is Logged**. THE BOARD MAY MONITOR USAGE OF BOARD WORKSTATIONS, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES VISITED, AND PERSONAL USE OF BOARD COMPUTERS. All logs of employee activity are property of ACBDD.

6) **Data Storage on Server Only**. All ACBDD data shall be stored on the server. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in their assigned User Directory or Folder on the server. The storage of large volumes of graphic images on the server is prohibited 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. ANY DATA FOUND ON WORKSTATIONS MAY BE REMOVED WITHOUT NOTICE.

7) **Licensed or Copyrighted software.** No employee may duplicate ACBDD licensed or copyrighted software without authorization by the HIPAA Security Officer. Software not licensed to ACBDD is not permitted to be installed ACBDD owned equipment.

8) **Board owned and approved hardware and software**. Only board owned and installed hardware or software is to be used by employees. No wireless networking equipment, smartphones, video cameras, or other hardware or software may be installed or used without authorization of the HIPAA Security Officer. Donated equipment shall be inspected by the HIPAA Security Officer or designee before any use by ACBDD employees.

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

WORKSTATION SECURITY

1) Except with specific approval of the HIPAA Security Officer, workstations or other devices processing PHI are not to be setup in a public access areas.
2) All employees shall not adjust settings on software or hardware installed on workstations. Monitors may be adjusted for ergonomic reasons to promote comfortable use of the equipment.
3) Workstation monitors that are used to access PHI shall not face in a direction that makes visual access available to unauthorized users or passersby.

ORIGINAL

4) Workstations will be configured with automatic logoff capability so that they will become inaccessible after 10 minutes of inactivity. Employees should not leave their workstation unattended for an extended period of time..
5) 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 HIPAA Security Officer
6) 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.

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.
2) Passwords should be at least 8 characters long and include both letters and numbers. 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, especially not in the vicinity of a 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.

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.)

ORIGINAL

3082 Use of Social Networking Sites including Facebook, Twitter, LinkedIn, MySpace and others

Adopted: 2/1/05
Revised Date: 11/23/10
Effective: 11/23/10

POLICY
Facebook, and other social networking sites, have become a significant communication medium in our world, especially with younger people. However their use shall monitored for professional and PHI related issues that do not support the vision and mission of ACBDD.

AUDIENCE
All Staff

DEFINITIONS
Facebook means both the Facebook site itself as well as all of the other similar sites which include MySpace, Twitter, LinkedIn and others.

PROCEDURES
1) **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 any board sponsored use of Facebook or similar social networks.
2) **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. Employees are permitted personal use of social network sites during their lunch and break periods/.
      ii) **Employee Use**. 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.
         (2) **Friending**. Employees must not "friend" any individual being served by ACBDD, or the parent/guardian of an Individual. The board expects employees to maintain an acceptable professional boundary with Individuals served.
         (3) **Messaging**. Employees must not use Facebook messaging for any board communications. Employees are reminded that all board communications including information posted on a social network site are subject to and perceived as public records. Facebook and other such networks do

ORIGINAL

not utilize encryption which is required by HIPAA for transmission of PHI over an open communications network.

3085 Portable Computing Devices and Home Computer Use

Adopted: 2/1/05
Revised Date: 07/17/13
Effective: 11/23/10

POLICY
Data on laptops and other portable devices shall be encrypted and/or subject to various security measures that protect PHI disclosures.

AUDIENCE
All Staff

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

PROCEDURES

1) **Encryption on Laptops and other mobile devices**. Encryption of laptops will be controlled by the Beacon Server. The laptop will be encrypted when user logs off the server and restored at sign-on.

2) **Lost devices**. Employees must immediately report lost, stolen or compromised devices to their supervisor and the HIPAA Security Officer or designee in accordance with the Security Incident procedure. Loss of any portable device containing PHI is a potential breach incident and should be reported per Policy 3090 Security Incident Response and Reporting. Lost or stolen mobile devices will be wiped of all data by ACBDD IT department.

3) **Employee-owned portable computing devices**. Employees may use their personal smartphones or other portable devices to perform board related functions after receiving authorization by the HIPAA Security Officer.. No PHI should be stored on the PDA (e.g. a Individual's initials but not their SS#) to minimize the impact of a lost or stolen PDA. All employee-owned devices must be capable of password protection and will be password protected at all times by the user. Prior to authorization, the mobile device will be inspected and approved by the IT department. The employee should keep the mobile device with them at all times or store in a secure location when not in use.

4) **Eligibility.** Eligibility for participation in a Bring Your Own Device (BYOD) program will be assessed by the employee's manager or director.
The following considerations will be used in determining the necessity for using a mobile device:
   A) There is a justifiable business requirement needing mobile access to ACBDD information.

   B) Employee agrees to opt in to ACBDD's management policies and procedures defined in the Mobile Device Policy.

   C) No more than two mobile devices in addition to an ACBDD-owned laptop will be permitted per user.

5) **Work at home and use of employee's home computer.** Employees shall obtain approval of their immediate supervisor to work from home. Employees are not permitted to load any data containing PHI onto a device that is not Board owned. Employees may work at home and using their home computers with direct access to the Beacon server. This will eliminate the need to store PHI on their home computer.

ORIGINAL

6) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required while using these devices.

7) **Audit.** Random audits to ensure compliance with this policy will be conducted by the Information Technologies department on a quarterly basis. Employees must surrender the device for audit. Audits will be conducted with employee and the device immediately at the employee's business location.

8) **Noncompliance.** Employees failing to comply with this policy may be subject to disciplinary action and will lose access to the ACBDD network resources through any current or future mobile device.

9) **Termination of Privileges.** Access will be terminated upon written request from the supervisor, the employee, or upon ending employment with ACBDD. Employees placed on Administrative Leave will have their user accounts disabled until such time they may return to active status. The user is responsible for removing any ACBDD data stored in the cloud.

10) **Ownership of Data.** By accepting ACBDD Network access privileges, users waive any and all rights of privacy in connection with their usage including, but not limited to, protections provided by the Federal Wiretaps Act of 1968 and the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2520. All such information, content, and files shall be and remain the property of ACBDD and users should not have any expectation of privacy regarding those materials. Any information or data stored on the mobile device is a public record.

11) **Acknowledgment.** Users of mobile devices will be required to sign a document which authorizes use of a mobile device, and details their rights and responsibilities when using a mobile device.

12) **E-Discovery.** In the event of any legal action the ACBDD needs access to the device for e-discovery purposes, the employee will surrender the device along with the necessary passcodes. It is the responsibility of the end user to back up personal applications and data prior to this event.

3090 Security Incident Response and Reporting

Adopted: 2/1/05
Revised Date: 9/1/2009
Effective: 11/23/10

POLICY
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)

PROCEDURES
Creation of Response Team, Contingency Planning and Drills
1) 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

ORIGINAL

incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services from the Board and the media.

2) 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) The incident response team may conduct security incident drills to develop skills and improve performance in the event of a serious security incident.

Security Incident Reporting and Response Procedure

1) Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer and report the incident.

2) The HIPAA Security Officer and/or Incident Response Team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Policy 3035 Breach Reporting and Policy 1080 Duty to Report Violations and Security Incidents, Policy 3065 Mitigation will be followed as appropriate. The superintendent of the Board will be notified and any contingency plans will be activated.

3) 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) 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.

ORIGINAL

APPENDICES

Appendix A - Identifying Business Associates

A "business associate" (BA) is a person or entity that performs certain functions, activities or provides services that involve the use or disclosure of PHI on behalf of an DD Board. The term is explained in 45 CFR 160.103.

A member of the ACBDD's workforce is not a BA.

A covered provider, health plan, or health care clearinghouse can be a BA of an ACBDD, but only when carrying out activities on behalf of the ACBDD which involve use or disclosure of PHI.

Business associate functions and activities include, but are not limited to: claims processing, billing or administration; data analysis, processing or administration; utilization review; quality assurance; and SSA activities or MUI investigations if not done by ACBDD workforce.

Business associate services include but are not limited to: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Most COG functions carried out on behalf of DD Boards are BA activities.

1) Examples of Business Associate Relationships.
   a) A CPA firm whose accounting services to the ACBDD involves access to protected health information.
   b) An attorney whose legal services to the ACBDD involve access to protected health information.

c) A consultant that performs utilization reviews, compliance audits or billing support for the ACBDD.
d) A health care clearinghouse.
e) An entity under contract with the ACBDD to carry out MUI investigations.
f) A COG which manages IO waiver contracts for member DD Boards.
g) An accreditation organization (such as CARF or JCAHO) for a program of the ACBDD if the accreditation organization reviews PHI as part of the accreditation process.
h) A computer contractor that provides support for board software and/or its computer network and has access to PHI as part of its support and service capacity
i)

2) Examples of relationships which are not Business Associates
   a) A contract between the ACBDD and a Provider of services which bills Medicaid under its own Provider number, such as a provider of psychological, speech, OT or PT services.
   b) A contract between the ACBDD and any Provider with a contract subject to ORC § 5126.035, such as a Provider of waiver or supported living services which bills Medicaid under its own Provider number.
   c) Transactions between the ACBDD and the DODD for payment purposes.
   d) Transfer of the Individual Data System (IDS) from the ACBDD to DODD. Note that, while this transaction does not require a BA Agreement, under ORC § 5126.044 a release is necessary for disclosure of PHI for payment purposes
   e) Accreditation activities by DODD under ORC §5126.081. Accreditation by DODD is a health oversight activity; DODD can access PHI without consent or authorization of the individual.
   f) Cleaning services, although it may be appropriate to include a clause in any contract as a reasonable safeguard if employees have physical access to PHI.
   g) Contractors who perform construction or remodeling of an individual's house for accessibility or other adaptive living

ORIGINAL

Appendix B: Sample HIPAA Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") effective on _____, 2010 ("Effective Date") is entered into by and between _____ (the "Business Associate") and _____., (the "Covered Entity").

RECITALS

1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 164. This agreement is updated to comply with the revisions enacted by statute in February 2009, the regulation changes published in August 2009 and the regulation changes scheduled to be published in 2010.
2) Becoming a party to this agreement obligates the Business Associate to specific duties specified in the Federal HIPAA Privacy and Security Regulations (45 CFR Part 164) which makes Business Associate subject to federal civil, monetary and criminal penalties for non-compliance with the applicable portions of the HIPAA regulations.
3) Terms used in this agreement, including but not limited to "Covered Entity", "Business Associate", "Protected Health Information (PHI)", "use", "disclose", "Breach", and "Security Incident", shall have the same meaning as defined in the above referenced regulations.

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

1) **Allowed Uses and Disclosures of Protected Health Information**. The Business Associate provides services for the Covered Entity. The Business Associate may use and disclose protected health information only as follows:
   a) Business Associate may use and disclose protected health information for the purposes specifically provided in Appendix A. In performance of the tasks specified in Appendix A, Business Associate may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.
   b) Business Associate may further use and disclose PHI, if necessary
      i) for the proper management and administration of the Business Associate's business
      ii) to carry out the legal responsibilities of the Business Associate

      if the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
2) **Responsibilities of Business Associate**. With regard to its use and disclosure of protected health information, the Business Associate agrees to do the following:
   a) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.
   b) Implement appropriate physical, technical, and administrative safeguards, and comply with other requirements specified for business associates in the HIPAA Security Regulations (45 CFR Part 164 Subpart C)
   c) Implement the portions of the HIPAA Privacy Regulations (45 CFR Part 164 Subpart B) that are applicable to business associates.
   d) Report to the Covered Entity any use or disclosure of protected health information of which it becomes aware that is not permitted under this agreement. This includes

ORIGINAL

i) Business Associate will notify Covered Entity, within 5 days, of any Security Incident, as defined in the HIPAA Security regulations

ii) Business Associate will notify Covered Entity's HIPAA Privacy Officer of any unauthorized use or disclosure of protected health information. In the event that the unauthorized use or disclosure does not constitute a breach, Business Associate will provide its internal documentation of the incident and its risk assessment which demonstrates that the incident was not a breach.

iii) In the event of a breach by the Business Associate, Business Associate agrees

a) To notify the Covered Entity's HIPAA Privacy Officer of the breach, in writing, within 5 days of the breach, in the manner specified in Section 164.410 of the HIPAA regulations. Business Associate shall bear all of its costs of compliance with these duties.

b) Business Associate will reimburse Covered Entity for all of Covered Entity's costs of responding to the breach including legal fees, investigation and risk assessment, notifying affected individuals, advertising, staff time, and all other costs]

e) Require all agents and subcontractors who use or who have access to Covered Entity's protected health information to agree in writing to adhere to the same restrictions, conditions and obligations on the use and/or disclosure of protected health information as specified in this agreement, and that are applicable to them under HIPAA Privacy and Security regulations 45 CFR Part 164.

f) Make available to the individual any requested protected health information, in accordance with procedures specified by Covered Entity and in compliance with 45 CFR 164.524 "Access of individuals to protected health information".

g) Make available for amendment, and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR 164.526, "Amendment of protected health information".

h) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528.

i) To the extent that Business Associate is to carry out Covered Entity's obligations under the HIPAA Privacy Regulations, 45 CFR 164 Part B, comply with the requirements of the Privacy Regulations in the performance of those obligations.

j) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the Covered Entity's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

k) Return to the Covered Entity or destroy, as requested by the Covered Entity, within 30 days of the termination of this Agreement, the protected health information in Business Associate's possession and retain no copies or electronic back-up copies. If this is not feasible, Business Associate will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.

3) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

4) **Term and Termination**.

a) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

5) Termination. As provided for under 45 C.F.R. §164.504, the Covered Entity may immediately terminate this Agreement and any related agreement if it determines that the Business Associate has breached a material provision of this Agreement. Alternatively, the Covered Entity may choose to: (i) provide the Business Associate with 30 days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

6) **Survival**. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2(k), detailing Business Associate's return and/or ongoing protections of

ORIGINAL

7) , shall survive the termination of this Agreement.

8) **Amendment**. This Agreement may be modified or amended only in writing as agreed to by each party.

9) **No Third Party Beneficiaries**. Nothing express or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

10) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Business Associate: _____
_____
_____

If to Covered Entity: HIPAA Security Officer
Athens County Board of Developmental Disabilities
801 West Union Street
Athens, OH 45701

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of the ____ day of _____, 20__.

Business Associate
By:_____
Name:_____
Title:_____
Date:_____

Covered Entity
By:_____
Name:_____
Title:_____
Date:_____

Attachment A – Permitted Uses and Disclosures

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

Business Associate is authorized to use protected health information for the purposes of providing 3rd party billing and collection services, and other related services. Business Associate may further use protected health information as necessary for the proper management and administration of its business, including staff training, quality assurance, and other tasks.

ORIGINAL

Appendix C: Sample Privacy & Security Officer Job Descriptions

HIPAA Privacy Officer Job Description

REPORTS TO: Superintendent

General Purpose:
The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the ACBDD's policies and procedures covering the privacy of, and access to, individual health information in compliance with federal and state laws and the ACBDD's information privacy practices.

Responsibilities:

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

ORIGINAL

- Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.
- Works with ACBDD administration, legal counsel, and other related parties to represent the ACBDD's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications of Privacy Officer:

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

ORIGINAL

HIPAA Security Officer Job Description

REPORTS TO: Superintendent

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

DUTIES:

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

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

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

ORIGINAL

Appendix D -Facility Security and Access Plan

ORIGINAL

Appendix E - Workforce Access to PHI and Safeguards

Person, Classes of Persons, or Business Associates	***Categories of PHI Needed***	***Additional Safeguards(*)***
Administration		
Superintendent	All	
Business Manager	All	
Medicaid/Records Clerk	All	
Nurse	Medical notes, relevant medical information	
Administrative Assistant	Computer data	
Administrative Secretary	Computer data	
Janitor	None	No User ID will be provided
Adult Services		
Workshop Director	All	
Habilitation Program Manager	All	
Production Manager	Medical Needs	
R.S.A.S.W's	Medical Needs	
Account Clerk	Medical Needs	
Secretary I	Medical Needs	
Language Development Specialist	Medical Needs, notes pertinent to speech/language	
Service & Support		
Service & Support Director	All	
Administrative Secretary	All	
Service & Support Coordinator	All	
Service & Support Professional (1)	All	
Service & Support Technicians	All	
Transportation/Maintenance		
Vehicle Operators	Medical needs related to transportation	No User ID will be provided; medical needs and behavioral support needs will be provided in hardcopy format by SSA
Grounds Maintenance	None	No User ID will be provided;
Mechanic	None	No User ID will be provided;
School		
M.H. Coordinator	records regulated under FERPA	
Classroom Instructors	records regulated under FERPA	
Instructor Assistants	records regulated under FERPA	
Language Development	Medical Needs, notes	

ORIGINAL

Specialist	pertinent to speech/language	
Early Intervention Specialists	All Early Intervention files	
Business Associates		
Doe, Jane	Medical needs, notes pertinent to service provision	
Athens County Auditor's Office	records pertinent to bill payment	
O'Blenness Hospital	Medical needs, notes pertinent to treatment	
Community Options	Medical needs, notes pertinent to service provision	
XYZ Computer	All computer data	
Doe, John	Medical needs, notes pertinent to treatment	
Doe, Jane	Medical needs, notes pertinent to service provision	
Primary Solutions, Inc.	Gatekeeper Data	
Special Olympics Coordinator	Medical needs	

*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

ORIGINAL

Appendix F – Legal Citations

Policy #	Citation
1010	45 CFR Part 160 and 164 (current as/of 8/1/2010)
1010	45 CFR 164.504(g) for entities with multiple functions
1010	ORC § 5126.044 Ohio law on confidentiality (effective 9/22/2000)
1010	OAC § 5123:2-1-02(I)(7) General DD Board confidentiality requirements (3/21/2002)
1010	OAC § 5123:2-4-01(C)(2)(b) General requirements for DD Board confidentiality policies (effective 4/12/2001)
1010	OAC § 5123:2-12-02(J)(2) Rescinded
1010	OAC § 5123:2-15-01(C)(6) Rescinded
1010	45 CFR 164.502(a)(1)(iii) incidental uses and disclosures
1010	OAC § 3301-51-04 Confidentiality (effective 7/1/2008)
1010	34 CFR 99 FERPA (current as of 8/13/2010)
1010	34 CFR 300 and 301 Part B IDEA (Individuals with Disabilities Education Act, ages 3-21)
1010	34 CFR 303 Part C IDEA (individuals with Disabilities Education Act, ages 0-2)
1010	34 CFR 303.402 and 460 Early Intervention Confidentiality Provisions
1010	34 CFR 300.610 - 627 Children with Disabilities Confidentiality and Parent Rights Provisions
1020	45 CFR 164.502(b)(1) minimum necessary standard
1030	45 CFR 164.530(c) – Administrative, Technical, and Physical Safeguards
1030	45 CFR 164.530(c)
1030	ORC § 5126.044 Ohio law on confidentiality
1030	OAC § 5123:2-1-02(I) Safeguard requirements for confidential DD Board records
1030	OAC § 5123:2-4-01(C)(2)(b) General requirements for DD Board confidentiality policies
1030	OAC § 5123:2-12-02(J)(2) Obsolete
1030	OAC § 5123:2-15-01(C)(6) Obsolete
1030	OAC § 5123:2-3-13(B) Safeguards for records in licensed facilities
1040	45 CFR 164.510(b)
1050	45 CFR 164.508 – HIPAA requirements for authorizations
1050	ORC § 5126.044 – Ohio Statute on confidentiality of records
1050	OAC § 5123:2-1-02(I)(7) – Ohio Rule on confidentiality of records
1050	34 CFR 99.30 - FERPA requirements for prior consents to disclose information
1070	ORC 5126.044
1070	45 CFR 164.5xx
1080	HIPAA Privacy Rules, 45 CFR Part 164
1080	164.530(e)(1) –Sanctions
1090	45 CFR § 164.512
1090	ORC § 2151.421(A) Reports of Child Abuse
1090	ORC § 2305.51 Disclosures to prevent harm to 3rd parties
1090	ORC § 2317.02(B) Privilege for physicians, school guidance counselors, licensed social workers and licensed counselors
1090	ORC § 4732.19 Privilege for psychologists
1090	ORC § 5123.19 Licensure activities of DODD
1090	ORC § 5123.60 OLRS
1090	ORC § 5123.61(C)(1) Duty to report abuse/neglect of persons with DD
1090	ORC § 5126.044 Confidentiality for DD Boards
1090	ORC § 5126.055 LMAA functions of DD Boards
1090	ORC § 5126.31 Case Review and Investigation
1090	OAC § 5123:2-15-10(G) Access to documentation for CAFS payments
1090	OAC § 5123:2-17-02(B) Incidents adversely affecting health/safety
1090	OAC § 5123:2-17-02(D) Reporting MUIs
1090	OAC § 5123:2-3-04 Monitoring of licensed facilities

ORIGINAL

1090	Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena
1090	ORC § 4113.52 Reporting Violations of law by employer or fellow employee
1200	45 CFR 164.524(e) individual's right to access PHI
1200	45 CFR 164.524(b) Time limits on response to access
1200	45 CFR 164.524(c) Form of access
1200	ORC § 1347.08(A)(2) individual's right to access records
1200	OAC § 3301-51-04 Confidentiality, for Education of Students with Special Needs
1200	OAC § 5123:2-1-02(I)(7)(d) County Board Administration – Record Policy – Right of Access
1200	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
1210	45 CFR 164.526(f) individual's right to request amendment
1210	OAC § 3301-51-04 Confidentiality, for Education of Students with Special Needs
1210	ORC § 1347.09 Disputing of Records
1210	34 CFR 99.20 FERPA - Requesting amendment of records
1210	34 CFR 99.21 FERPA - Rights to a Record Hearing
1210	34 CFR 99.22 FERPA - Requirements for a Records Hearing
1220	45 CFR §164.528
1220	45 CFR 164.528(d) individual's right to an accounting of disclosures of PHI
1220	ORC § 5126.044(C) obligation to maintain record of disclosures
1230	45 CFR § 164.522(a)
1300	45 CFR 160.103
1300	45 CFR § 164.502(e)
1300	45 CFR § 164.504(e)
1300	ORC § 5126.044 – Ohio Statute on confidentiality of records
1310	45 CFR 164.520
1310	ORC § 1347.08(A)(3) (Personal Information Systems)
1310	OAC § 5123:2-1-02(I) County Board Administration – Records, Informing individuals about policies
1310	34 CFR 99.7 FERPA Annual Notification
1330	Federal Law 45 CFR 164.530(j) – Documentation requirement,
1330	164.520(e) – Notices of Privacy Practices;
1330	164.524(e) – Access of individuals to protected health information;
1330	164.526(f) – Amendment to protected information;
1330	164.508(b)(6) – Uses and disclosures for which an authorization is required;
1330	164.512(i)(2) – Uses and disclosures for research purposes;
1330	164.522(a)(3) – Rights to request privacy protection for protected health information;
1330	§164.528(d) – Accounting of disclosures of protected health information – Implementation specification
1330	ORC § 5126.044(E) (General records of DD Boards)
1330	OAC § 5101:3-3-20(L) (ICFs/MR)
1330	OAC § 5101:3-40-01 (ISPs for IO Waiver)
1330	OAC § 5123:1-2-02(J)(8) (Waiver records)
1330	OAC § 5123:1-2-08(R) (IO waivers)
1330	OAC § 5123:1-2-11(P) (HCBS waivers for licensed providers)
1330	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.
1330	OAC § 5123:2-15-01(C)(6) (Habilitation Center/TCM records)
1330	OAC § 5123:2-15-10(G)(2) (CAFS records)
1340	45 CFR 164.530(d) HIPAA complaint procedures
1340	ORC § 5123.64(A) requires establishment of a complaint procedure
1340	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
1350	45 CFR 164.530(b)
1350	45 CFR 164.530(i)
1350	45 CFR 164.520
1350	ORC § 5123.64(A) training in rights

ORIGINAL

1350	OAC § 5123:2-3-08 staff training in licensed facilities
1350	OAC § 5123:2-5-01(C)(12) training requirements for adult service workers
1350	OAC § 5123:2-5-02(C)(12) training requirements for adult service workers
1350	OAC § 5123:2-5-05(C)(13) training requirements for early intervention workers
1350	OAC § 5123:2-5-07(C)(9) training requirements for investigative agents
1350	OAC § 5123:2-7-01 training requirements for TISC Gone!
3000	HIPAA Privacy and Security Rules, 45 CFR Part 164
3000	164.308(a)(2)
3000	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.
3005	HIPAA Privacy and Security Rules, 45 CFR Part 164
3005	164.308(a)(7)
3010	HIPAA Privacy and Security Rules, 45 CFR Part 164
3010	164.308(a)(7)
3010	164.312(a)(1)
3015	HIPAA Privacy and Security Rules, 45 CFR Part 164
3015	164.310(a)(1)
3020	HIPAA Privacy and Security Rules, 45 CFR Part 164
3020	164.308(a)(8)
3020	ORC § 5123:2-1-02(I) County Board Administration, Records, Annual Review of Safeguards
3025	**Audit Control and Activity Review**
3025	HIPAA Privacy and Security Rules, 45 CFR Part 164
3025	164.312(b)
3025	164.308(a)(1)
3030	HIPAA Privacy and Security Rules, 45 CFR Part 164
3030	164.308(a)(5)
3035	HIPAA Privacy and Security Rules, 45 CFR Part 164, Subpart D
3035	164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, 164.414
3040	HIPAA Privacy and Security Rules, 45 CFR Part 164
3040	164.308(a)(5)
3050	HIPAA Privacy and Security Rules, 45 CFR Part 164
3050	164.310(d)(1)
3060	HIPAA Privacy and Security Rules, 45 CFR Part 164
3060	164.312(c)
3060	164.312(d)
3060	164.312(e)
3065	HIPAA Privacy and Security Rules, 45 CFR Part 164
3065	164.530(e)(1) – Standard Sanctions
3065	164.308(a)(a) – Security Management Process, Sanctions Policy
3070	ORC § 304
3070	ORC § 1306
3075	HIPAA Privacy and Security Rules, 45 CFR Part 164
3075	164.308(a)(3)
3075	164.308(a)(4)
3075	164.312(a)(1)
3075	164.314(d)
3075	164.308(a)(5) Password Management
3080	HIPAA Privacy and Security Rules, 45 CFR Part 164
3080	164.310(b) Workstation Use
3080	164.310(c) Workstation Security
3080	164.308(a)(5) Log in Monitoring
3090	HIPAA Privacy and Security Rules, 45 CFR Part 164
3090	164.308(a)(6)

ORIGINAL

APPENDIX G – MOBILE DEVICE USER AGREEMENT

Purpose/Reason for Policy

The purpose of the attached policy, 3085 Portable Computing Devices and Home Computer Use, is to define accepted practices, responsibilities and procedures for the use of mobile devices (i.e, smartphones, tablets, etc.) that the Athens County Board of Developmental Disabilities (ACBDD) are authorized to connect to the ACBDD enterprise network. This policy defines the commitment requirement, provides guidance for secure use of end-user mobile devices and provides reimbursement guidelines for all mobile devices.

Scope

This standard applies to all agency-provided or employee owned mobile devices, other than laptops, which are configured to connect to the ACBDD network and to access resources therein. The employee, through meeting eligibility requirements, must follow the requirements listed below in exchange for access to ACBDD network resources. It is important that the obligations and consequences of this arrangement are understood. A signature is required on the last page of this policy confirming that it has been read and understood. These obligations include, but are not limited to:

- Employee(s) will hold ACBDD harmless (not liable) for any damage to personal mobile computing or telecommunications devices, regardless of its use for ACBDD or personal business at the time the damage occurred.
- Employee(s) must agree to allow the Information Technology department (IT) to load manageability software on personally owned devices.
- Acceptance that a personal device may be remotely wiped (i.e., erasing all data and applications) by the ACBDD if it is deemed to pose a security risk.
- Understanding that the employee is solely responsible for backing up any personal content on the device.
- Agreement from the employee that the device will be kept updated and in good working order and password protected.
- Acknowledgement that the ACBDD will in no way be responsible for lost or stolen personal devices.
- The decision to be eligible to use a personally owned mobile device for ACBDD business will be based on a documented business need and appropriate management approval.

ORIGINAL

Guidelines for Eligibility for BYOD

Eligibility for participation in a Bring Your Own Device (BYOD) program will be assessed by the employee's manager or director.

Criteria:

- There is a justifiable business requirement needing mobile access to ACBDD information.
- Employee agrees to opt in to ACBDD's management policies and procedures defined in the *Mobile Device Policy*.
- No more than two mobile devices in addition to an ACBDD-owned laptop will be permitted per user.

User Responsibilities

Users shall not use the Network for any personal commercial activities, such as buying, advertising or selling goods or services Users shall not conduct any work or communication relative to their privately-owned or third-party business using ACBDD networks.

The features that make mobile devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to ACBDD employees and the ACBDD network. Features such as small size (easily lost, stolen or misplaced); weak user authentication which can be easily compromised or disabled by the user (non-authorized person?); and ease of interconnectedness increase the employee's and ACBDD's risk level.

Any information or data stored on the mobile device is a public record. In case of legal action, personal devices used for ACBDD communications are subject to e-discovery. Users are responsible for bringing or sending the mobile device to the IT department and giving the necessary device access codes when notified that the device is needed for e-discovery purposes.

Every employee of ACBDD who uses a computing device can make ACBDD's network environment more secure by following these best practices. The Information Technologies department can be contacted to determine if appropriate protections are already in place or assist with enabling the security measures required for personally owned mobile devices.

General Security/Safety

- Each device in use must be granted access through the authorization outlined in this policy and signature acceptance of this policy and approval of the IT department.
- Keep mobile devices with you at all times or store them in a secured location when not in use. Do not leave your devices unattended in public locations (airport lounges, coffee shops, libraries, restaurants, conferences, unattended vehicles).
- Mobile devices must be password protected. The password should block all access to the device until a valid password is enabled.

ORIGINAL

- Passwords must never be shared or revealed to others.
- Authorization to access ACBDD network resources will require employee agreement to load manageability software (MDM) on personal device.
- If you are going to dispose a mobile device, wiping or secure deletion of data must be confirmed by IT. Any data or information stored in a cloud environment or other remote location from the mobile device must also be destroyed and confirmed by the IT department.
- Lost, stolen, misplaced or replaced mobile devices should be reported to the IT department with 24 hours of discovery. Mobile devices replacing a current device (i.e., new smartphone or tablet) must also be reported to the IT department so that the previous model can be removed from network access.
- If you lose the device, your data will be wiped.
- Users should not talk, text or otherwise communicate via a mobile device while driving.
- Personally owned devices are prohibited from connecting to the ACBDD network without prior approval from their manager and the IT department. Failure to comply may result in loss of network privileges and possible disciplinary action.

E-Discovery

In the event of any legal action the ACBDD needs access to the device for e-discovery purposes, the employee will surrender the device along with the necessary passcodes. It is the responsibility of the end user to back up personal applications and data prior to this event.

Audit

Random audits to ensure compliance with this policy will be conducted by the Information Technologies department on a quarterly basis. Employees must surrender the device for audit. Audits will be conducted with employee and the device immediately at the employee's business location.

Employees failing to comply with this will lose access to the ACBDD network resources through any current or future mobile device.

Termination of Privileges

Access can be terminated and all agency data wiped from a device upon written request from an employee's supervisor submitted to the Human Resources department.

Access will be terminated and all agency data wiped after termination from the ACBDD. It is both the employee and the supervisor's responsibility to notify the Information Technologies department to terminate this access.

Employees placed on Administrative Leave will have their user accounts disabled until such time they may return to active status.

ORIGINAL

A user may have mobile device access terminated for any violations of this Policy committed by someone else who, with the user's expressed or implied permission or by the user's negligence, accesses the Network or other ACBDD resources with the user's password.

By accepting ACBDD Network access privileges, users waive any and all rights of privacy in connection with their usage including, but not limited to, protections provided by the Federal *Wiretaps* Act of 1968 and the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2520. All such information, content, and files shall be and remain the property of ACBDD and users should not have any expectation of privacy regarding those materials.

Acknowledgement

I have read and understood my responsibilities and conditions outlined in this policy related to mobile device access to the ACBDD network and resources.

_____

Employee Signature

_____ _____

Printed Name Date Signed

ORIGINAL

Athens County Board of Developmental Disabilities (ACBDD) – Authorization Form

Atco Adult Services	Service and Support Administration	Beacon School
21 S. Campbell St.	9033 Lavelle Rd.	801 W. Union St.
Athens, OH 45701	Athens, OH 45701	Athens, OH 45701
740/592-6659 (voice)	(740) 592-6006 (voice)	740/594-3539 (voice)
740/594-7814 (fax)	(740) 594-5048 (fax)	740-593-3189 (fax)

AUTHORIZATION FOR RELEASE OF CONFIDENTIAL INFORMATION

Name of Individual Served _____ Date of Birth _____

I authorize ACBDD to:

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

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

The purpose of this disclosure is
___ Coordination of care
___ Requested by Individual Receiving Services, or guardian/parent
___ Other _____

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

Expiration Date:
___ 90 days from date signed
___ other date: _____

Approved by: _____ Date: _____

If signed by someone other than the Individual being served:

Print Name_____
Authority to sign: ___ Parent or Guardian
____ Appointed by Individual as HIPAA Personal Representative
____ Other _____

For staff use (complete the following steps and indicate by a check. Name of Staff Person _____)
___ Copy of signed authorization given to Individual / Parent / Guardian
___ Copy of records released given to individual / Parent / Guardian (if requested)
___ Disclosure logged on Disclosure Log

ORIGINAL

___ Revocation received on _____ and acted upon.

ORIGINAL

Notice of Privacy Practices

Athens County Board of Developmental Disabilities

FOR YOUR PROTECTION

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

YOUR RECORDS ARE PRIVATE

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

WHO SEES AND SHARES MY RECORDS?

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

Our organization includes ATCO, the bus garage, the Service and Supports Administration, and Beacon School.

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

In general, we use and disclose your information:

- For teaching, behavioral and medical support, transportation and school administration,
- To provide the full range of services we provide: early intervention, habilitation, supported employment, and other services. For example, your service and support coordinator will review your records to recommend an individual service plan,
- To get payment for services provided: for example, the billing clerk uses service records to submit bills to the Ohio Department of Developmental Disabilities, and
- For other operations to operate and manage the board: these include improving quality of care, training staff, managing costs, and conducting other business duties. For example, a quality assurance reviewer may audit your records to determine whether appropriate services were provided,
- To remind you or a guardian or an appointment for services,
- To solicit funds.

WHAT IF MY RECORDS NEED TO GO SOMEWHERE ELSE

You may be asked to sign a separate permission form allowing your records to go somewhere else if:

1. One of our employees who serves you needs it sent to other places;
2. You want us to send it to another person, school or agency

The permission form tells us what, where, why and to whom the information must be sent. Your signed permission form is good until the date you put on the form. You can cancel your permission at any time or limit the amount of information sent by letting us know in writing.

COULD MY RECORDS BE RELEASED WITHOUT MY PERMISSION?

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

- Record transfers to other schools your child enrolls in,
- Reports to public health authorities to prevent or control disease or other public health activities,
- To protect victims of abuse, neglect, or domestic violence,

ORIGINAL

- For oversight including investigations, audits, accreditation and inspections, such as are conducted by the Ohio Department of Developmental Disabilities and federal agencies,
- When a court order, subpoena or other legal process compels us to release information,
- Reports to law enforcement agencies when reporting suspected crimes, when responding to an emergency, or in other situations when we are legally required to cooperate,
- In connection with an emergency, or to reduce or prevent serious threat to public health and safety,
- to coroners, medical examiners and funeral directors,
- to victims of alleged violence or sex offenses,
- For workers' compensation programs,
- For specialized government functions including national security, protecting the president, operating government benefit programs, and caring for prisoners,
- In connection with "whistleblowing" by an employee of the Board.

All other uses not described above require that we obtain your signed permission.

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

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

1. If you request, we will show you your records, or give you a copy.
2. If you think some of the information is wrong, you may ask that it be changed, or that new information be added.
3. If you request, we will mail all communications to a confidential address.
4. If you request, we will provide a list of any places where your records have been sent.
5. You may request that we make additional limits on how we use or disclose your information, although we are not obliged to honor these requests.
6. You may receive a paper copy of this notice.

To exercise any of these rights, mail or email your request to:

HIPAA Privacy Officer
Athens County Board of Developmental Disabilities
801 West Union Street
Athens, Ohio 45701
(740) 594-3539 x224
cblackstone@athenscbdd.org

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

POLICY CHANGES

We are required by law to abide by the terms of this notice. From time to time we may make changes to our policies, and if and when we do, your records will be protected by our new, changed policies. Our current notice will always be available on our website.

QUESTIONS OR COMPLAINTS?

If you have any questions about this notice, or you think that we have not protected your records and you wish to complain about any privacy or records access matter, please contact:

Attn: HIPAA Privacy Officer
Athens County Board of DD
801 W. Union Street
Athens, Ohio 45701
740-594-3539

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

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

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

Original Notice effective 4/14/2002; Current Revision effective 1/1/2011.

ORIGINAL

ACBDD 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)

ORIGINAL

4-2 PROBATIONARY PERIODS – CLASSIFIED EMPLOYEES

Adopted	10/15/1996
Status	PENDING APPROVAL
Historical Versions	3/18/1997; 4/18/2006; 11/24/2015
Initiated by:	Gwen Brooks, Director of Human Resources
Approved by:	Board of the Athens County Board of Developmental Disabilities (ACBDD)

Policy

The ACBDD shall establish probationary periods for newly appointed, newly promoted and newly transferred classified appointments in accordance with Ohio Revised Code 124.27 and Ohio Administrative Code 123:1-19. Probationary period is the period of time at the beginning of an original appointment or the period of time immediately following a promotion, which constitutes a trial or testing period for the employee, during which the employee may be terminated.

Probation for Newly Appointed and Newly Promoted Classified Staff

A. Each newly appointed or promoted employee in a classified regular full or part time position shall serve a probationary period of one hundred eighty (180) calendar days beginning on the date of appointment.

B. Intermittent employees are unclassified and serve at the pleasure of the superintendent, therefore, do not serve a probationary period.

C. Probationary periods are not served:
   - When a position is reclassified;
   - Upon demotion;
   - Upon reinstatement or re-employment within one year of separation of service to the former classification for which the employee is certified;
   - Upon reinstatement from disability separation to the same classification.

D. Probationary periods for appointments that are covered by a labor contract shall follow the respective negotiated contract.

E. Time spent on paid leave that exceeds two weeks, and on non-paid status leaves of absence shall not be counted as part of the probationary period.

F. An employee serving a probationary period is not eligible to apply as an internal candidate for other ACBDD positions.

G. An employee who resigns during a probationary period is not eligible for reinstatement, but may be considered for new appointment and serve a new probationary period if hired into a new appointment.

DRAFT

H. Supervisors shall use the probationary period to closely observe and evaluate the employee's performance and aptitude for the job and provide training, coaching and feedback. The employee is encouraged to bring problems to the supervisor for resolution in order to enhance his/her performance.

    1. Supervisors shall complete probationary evaluations by day ninety (90) and by day one hundred seventy (170).
    2. Supervisors shall recommend retention of only those employees who meet acceptable work standards during the probationary period.

Probationary Termination

Initial probationary employees may be removed at any time during the probationary period by submitting a written request, justification for probationary termination and a completed performance evaluation to the human resources representative no more than 10 days before the end of the probationary period.

If a classified employee accepts a promotion and is found to be unsatisfactory during the probationary period, the employee may be demoted in accordance with Ohio Administrative Code section 123:1-23-03.

DRAFT

Section: 4.2
Adopted: 10/15/96
Revised: 3/18/97, 4/18/06, 11/24/15
Effective: 3/18/97, 4/18/06, 11/24/15

4.2 PROBATION - Classified Employees

1. INITIAL PROBATIONARY PERIOD

   a. Each newly hired or promoted employee in a classified position shall serve a probationary period.

      The minimum probationary period shall be 120 calendar days. The length of the probationary period for each classification shall be specified on the position descriptions, management contracts and on all work agreements.

   b. The probationary period for full-time employees and scheduled part-time and seasonal employees shall be based on calendar days from the date of original appointment. Employees who work irregular shifts shall have their probationary periods determined by the number of hours worked. The probationary period for non-bargaining unit administrative staff is listed below. Bargaining unit employees will follow their negotiated contract.

      Length of Probationary Period

      120 days

      Time spent on non-paid status approved leaves of absence shall not be counted as part of the probationary period.

   c. Supervisors shall use the probationary period to closely observe and evaluate the employee's performance and aptitude for the job. The employee is encouraged to bring problems to the supervisor for resolution in order to enhance his/her performance. Supervisors have a responsibility to recommend retention of only those employees who meet acceptable work standards during the probationary period.

   d. Probationary employees will be evaluated at midpoint and within ten (10) calendar days prior to the end of their probationary period. Full and appropriate records will be maintained. Should the employee be given a probationary removal within the second half of the probationary period but before the end of the probationary period, the final evaluation will be made at the time of removal. Although the primary purpose of a probationary evaluation is to rate an employee's job performance uniformly and objectively, the evaluation serves several other purposes as well:

ORIGINAL

1. By acting as a means of communication between employee and supervisor, it can reveal conditions which are contributing to poor morale or low productivity.

2. It gives an employee an opportunity to identify and correct specific performance problems of which he/she may not have been aware.

3. It serves as the means of determining job efficiency for probationary removal.

e. The employee must sign the evaluation as an acknowledgement that he/she has seen and discussed the document with the supervisor. Employees should always be made aware that the signature does not signify agreement with the evaluation, but is only an acknowledgement that it has been seen and discussed. Any points of disagreement should be expressed in writing by the employee in the space reserved for employee comments. No change in the rating is to be made after the form is signed by the employee. If the employee refuses to sign the evaluation, the supervisor must record the reasons and the employee's refusal should be verified in writing by a witness. If an employee has not been on the job for some time and is, therefore, not available for signature, the supervisor must clearly indicate this absence on the evaluation form. While the employee signs the evaluation after the supervisor's rating, he/she must receive a copy of the rating in its final form after all other reviewers have made their comments.

f. Probationary employees may be removed at any time during the the probationary period if the service is considered unsatisfactory. The removal cannot be effective after the final day of the probationary period. Whenever a probationary appointee is removed, the Superintendent shall provide a letter to the employee stating the reasons for the removal.

2. PROMOTION AND DEMOTION AND LATERAL TRANSFER DURING PROBATIONARY PERIOD

If any employee's service is found to be unsatisfactory during the probationary period following promotion, a reduction is made to the classification held prior to the promotion. A probationary removal may not be given in this case. However, an order of removal may be issued in accordance with the provisions of the O.R.C. Section 124.34.

No probationary period is required following a demotion.

An employee may not be promoted during his original new hire probationary period. If an employee accepts a position in a different, lateral classification during his original probationary period, the employee must resign his current position in order

ORIGINAL

to accept the new position and must serve an original probationary period in the new classification.

An employee who resigns during a probationary period is not eligible for reinstatement. The employee may be considered for new appointment. A new probationary period must be served if the person is hired by the Board a second time.

No lateral transfer of an employee may occur during his probationary period.

3. PROBATION OF A TRANSFERRED EMPLOYEE

The employee will serve a probationary period. The employee will not be removed if his job performance in the new positions is found to be unsatisfactory but may be returned to the former position if available.

ORIGINAL