PICKAWAY COUNTY BOARD OF DEVELOPMENTAL DISABILITIES

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

CHAPTER 9

Content

Page 2	**POLICY: 9.0~~2~~ Definitions for Confidentiality and Computer Security Policies**
Page 15	**POLICY: 9.1 HIPAA/FERPA/IDEA Privacy and Confidentiality Policy**
Page 19	**POLICY: 9.2 HIPAA Security**

PICKAWAY COUNTY BOARD OF DEVELOPMENTAL DISABILITIES

POLICY: 9.02 ~~2~~ Definitions for Confidentiality and Computer Security Policies

I. Purpose:

To establish a common set of definitions for use in Confidentiality, Privacy, and Computer Security Policies.

II. Discussion:

A. 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 generally include both the information protected by the HIPAA regulations and the information protected by the FERPA regulations.

III. Definitions:

A. **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.)

B. **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

C. **Applicable Requirements –** Applicable requirements mean applicable federal and Ohio law and the contracts between the PCBDD and other persons or entities which conform to federal and Ohio Law.

D. **Authentication –** means the corroboration that a person is the one claimed.

E. **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.

F. **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*:

1. 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 rule;

2. 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; and

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

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

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

G. **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 complete definition is included in Appendix A - Identifying Business Associates.

H. **Confidentiality –** means the property that data or information is not made available or disclosed to unauthorized persons or processes.

I. **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.

J. **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.

K. **Designated Record Set –** Designated record set means:

1. A group of records maintained by or for a covered entity that is:

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

3. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

4. 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.

L. **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.

M. **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.

N. **DODD** – means the Ohio Department of Developmental Disabilities.

O. **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

P. **Education –**means activities associated with operating the school including instruction, IEP preparation, administration, behavioral intervention, extra-curricular activities and other normal school functions. Education shall also include activities associated with early intervention programming.

Q. **Education Records** – As defined in the FERPA regulations, means records that

are:

1. Directly related to a student; and

2. Maintained by an educational agency or institution or by a party acting for the agency or institution.

    a. 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.

3.

    a. Records relating to an individual who is employed by an educational agency or institution, that:

        i. Are made and maintained in the normal course of business;

        ii. Relate exclusively to the individual in that individual's capacity as an employee; and

        iii. Are not available for use for any other purpose.

    b. 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 (2)(a) of this definition.

4. Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:

    a. 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;

    b. Made, maintained, or used only in connection with treatment of the student; and

    c. Disclosed only to individuals providing the treatment. For the purpose of this definition, “treatment” does not include remedial educational activities or activities that are part of the program of

instruction at the agency or institution.

5. 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.

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

R. **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.

S. **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.

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

U. **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.

V. **Guardian of the Person –**means an individual appointed by the Probate Court to provide consent for and make decisions for the ward.

W. **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.

X. **Health Care –** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. 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

2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Y. **Health Care Clearinghouse –** means 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:

1. 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.

2. 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.

Z. **Health Care Operations –** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. 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;

2. 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;

3. Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

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

5. 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

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

a. Management activities relating to implementation of and compliance with the requirements of this subchapter;

b. Resolution of internal grievances;

c. 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

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

AA. **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.

BB. **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:

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

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

3. 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:

   a. Has 50 or more participants; or

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

4. 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.

CC. **HIPAA –** means the Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 - 1320d-9 and at 42 CFR Parts 160, 162 and 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.

DD. **ICF/DD –** An ICF/DD is an intermediate care facility for persons with developmental disabilities, certified to provide services to individuals with DD or a related condition in accordance with 42 CFR part 483, subpart I, and administered in accordance with OAC § 5101:3-3.

EE. **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.

FF. **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.

GG. **Eligible Individual** – means a person who receives services from the County Board. In the event that the eligible individual is a minor, the term "individual" in these policies may also include the parent or guardian of the eligible individual. In addition, in regard to any privacy rights, individuals may also mean an individual's "personal representative" as it is defined under HIPAA regulations.

HH. **Individually Identifiable Health Information –** means information that is a subset of health information, including demographic information collected from an individual, and:

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

2. 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

    a. That identifies the individual; or

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

II. **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.

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

KK. **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.

LL. **Limited Data Set –** means protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town or city, state and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social Security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

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

NN. **MOU –**means a Memorandum of Understanding between governmental entities, which incorporates elements of a business associate contract in accordance with HIPAA rules.

OO. **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

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

QQ. **Payment –** means, in the context of a County Board:

1. Both:

   a. Activities by the Board required to determine if an individual is eligible for services, and

   b. Activities of the Board either to reimburse contracted providers for services rendered to individuals served or seeking reimbursement, for example from Medicaid or DODD, for services rendered to an individual served.

2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

   a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

   b. 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;

   c. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

   d. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

RR. **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 PCBDD and the minor.

SS. **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.

TT. **Protected Health Information, or PHI** – means individually identifiable information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Records of individuals deceased for more than 50 years are not PHI. For the purposes of this manual, and the Board's compliance program, PHI shall also include "Education Records" as defined by FERPA. This creates a consistent set of policies for both types of confidential information.

UU. **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.

VV. **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.

WW. **Security or Security measures –** encompass all of the administrative, physical, and technical safeguards in an information system.

XX. **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.

YY. **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.

ZZ. **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.

AAA. **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.

BBB. **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

CCC. **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

DDD. **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

EEE. **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.

FFF. **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.

GGG. **User –** means a person or entity with authorized access.

HHH. **Violation**, **or violate** – means, as the context may require, failure to comply with a provision of either the HIPAA Privacy or Security rules.

III. **Workforce Member –** Workforce Member means the same as Employee. See definition above.

JJJ. **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.

References: **45 CFR Part 160 and 164** (current as/of 3/27/2013)

45 CFR 164.504(g) for entities with multiple functions
ORC § 5126.044 Ohio law on confidentiality (effective 9/22/2000)
OAC § 5123:2-1-02(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 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

POLICY: 9.1 HIPAA/FERPA/IDEA Privacy And Confidentiality Policy

I. Purpose:

To establish appropriate policy for compliance with multiple regulations, including HIPAA, FERPA, IDEA and Ohio Revised Code, which specify privacy and confidentiality requirements.

II. Definitions:

A. All definitions used for the Policy and corresponding procedures are detailed in Policy 9.0

B. Definitions for Confidentiality and Computer Security Policies and Procedures.

III. Policy:

A. Minimum Necessary

1. 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.

2. The Privacy Officer shall implement safeguards and protocols required by HIPAA to implement this policy.

B. Confidentiality Safeguards (Oral & Written)

1. The Board shall utilize appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

C. Speaking with an Individual's Family and Friends

1. Board personnel are allowed to verbally disclose protected health information to family, friends, caregivers and other individuals 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.

D. Authorizations

1. All disclosures of PHI beyond those permitted or required by law require a signed authorization.

2. The Board will use an authorization form that conforms to Ohio Laws, and the federal FERPA, IDEA and HIPAA regulations.

E. Verification of Identity Prior to Release of Information.

1. Board employees will take reasonable steps to verify the identity and/or the authority of the person requesting protected health information (PHI) of an individual.

F. Minors, Personal Representatives and Deceased Individuals.

1. 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.

G. **Duty to Report Violations and Security Incidents**.

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

2. Any employee who becomes aware of a violation of either confidentiality or computer security rules is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

H. **Disclosures Permitted Without an Authorization Form**

1. Board employees may use and disclose PHI and/or Education Records 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 situations:

   a. When required by law.
   b. 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.
   c. To protect victims of abuse, neglect, or domestic violence.
   d. For health oversight activities such as investigations, audits, and inspections.
   e. To accrediting organizations.
   f. For judicial and administrative proceedings.
   g. For law enforcement purposes.
   h. To coroners, medical examiners, and funeral directors.
   i. For organ, eye or tissue donation.
   j. To reduce or prevent a serious threat to public health and safety.
   k. For Specialized government functions.
   l. In connection with "whistleblowing".
   m. For workers' compensation or other similar programs if applicable.

I. **Individuals, Parents and Guardians may Access Their Records**

1. Individuals served by the Board, and their parents, guardians and/or 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.

J. **Individual/Parent Right to Request Correction of Erroneous Records**

1. Individuals receiving services and their parents/guardians have the right to request that the Board amend PHI in the designated record set, or Education Records, that they believe are erroneous.

K. **Right to an Accounting of Disclosures**

1. The Board will provide, upon request, an "Accounting of Disclosures," in accordance with HIPAA Regulations, to individuals who receive services from the Board.

L. **Individual's Right to Request Additional Restrictions**

1. While the Board believes that its established safeguards will be acceptable to most individuals served, it supports individual's HIPAA right to request restrictions on the use or disclosure of protected health information which are more stringent than the restrictions defined in organizational policy.

M. **Individual's Right to Request Confidential Communications**

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

N. **Notice of Privacy Practices**

1. Individuals (or their parents) are entitled to a notice detailing the privacy practices of the Board. PCBDD will provide such notice to each individual (or their parents), in a manner compliant with both the HIPAA and FERPA regulations.

O. **Business Associate Contracts**

1. The Board 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.

P. **Non-intimidation and Non-retaliation**

1. The Board will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals receiving services who exercise any HIPAA-related right.

2. The Board will not intimidate or retaliate against staff or other individuals who express the opinion that PCBDD policies are not consistent with the law, or not being implemented properly, or who file a whistleblower action.

3. The Board will not require any individual receiving services to waive any of his/her rights under HIPAA as a condition of education, treatment, or enrollment.

Q. **HIPAA Assignments and Documentation**

1. The Board will maintain written Policies and Procedures required by HIPAA, including a 6-year audit trail. In addition, all documentation required by HIPAA regulations will be maintained for 6 years.

2. The HIPAA Privacy Officer shall be responsible for insuring the proper maintenance of all required documentation.

R. **Policy Updates and Staff Training on Confidentiality and Computer Security**

1. The Board's HIPAA Privacy Officer and HIPAA Security Officer shall collaborate to insure 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.

POLICY: 9.2 HIPAA Security

IV. Purpose:

To establish appropriate policy for compliance with multiple regulations, including HIPAA and Ohio Revised Code, which specify computer security requirements.

V. Definitions:

A. All definitions used for the Policy and corresponding procedures are detailed in Policy 9.0 Definitions for Confidentiality and Computer Security Policies and Procedures.

VI. Policy:

A. **Computer Security Management Process**

1. The Superintendent will appoint a HIPAA Security Officer. The HIPAA Security Officer, will orchestrate the Board's security management process.

B. **Data Backup**

1. The HIPAA Security Officer will insure that a robust data backup regimen is in place and operational at all times.

2. The HIPAA Security Officer shall insure that the principles, operating procedures and other processes specified in procedure.

C. **Disaster Recovery Plan and Emergency Mode Operation Plan**

1. 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.

D. **Facility Security**

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

E. **Annual Security Evaluation**

1. Annually, the HIPAA Security Officer shall conduct an evaluation of the Board's security policies and procedures, its compliance with its policies and all applicable regulations, and will update these policies, procedures and safeguards as necessary in response to environmental or operational changes affecting the security of electronic protected health information.

F. **Audit Control and Activity Review**

1. System capabilities for maintaining audit trails of system use by employees and/or any other activity on the systems shall be enabled to permit auditing, forensic analysis, and periodic activity reviews. Periodic audits and reviews shall be conducted to identify inappropriate activity so that appropriate corrective action is possible.

G. **Malicious Software Protection**

1. Appropriate measures will be taken by the HIPAA Security Officer to protect against malicious software. This will include centrally managed anti-malware software as one component of a multi-layered defense strategy.

H. **Breach Reporting**

1. The Board will fully comply with HIPAA breach notification requirements and will notify individuals receiving services, the Secretary of HHS and, when appropriate, the news media regarding breaches of protected health information.

I. **Security Awareness Program**

1. In recognition that properly trained employees are essential to computer security, the Board will conduct an ongoing computer security awareness training program.

2. Implementation details including curriculum for new employees as well as ongoing training for existing employees.

J. **Device and Media Disposal and Re-Use**

1. Electronic storage media and devices shall be cleaned of protected health information and other confidential information prior to disposal and/or re-use. Details including responsible parties, technical methods and recordkeeping are specified in procedures.

K. **Technical Safeguards**

1. Best practice technical safeguards will be employed as necessary to maintain the confidentiality, integrity and availability of the Board's information assets.

L. **Mitigation**

1. In the event of an inappropriate use or disclosure of an individual's PHI (that is, a violation of the HIPAA Privacy Rule and/or improper disclosure under FERPA/IDEA), the Board will take reasonable steps to mitigate the harmful effects upon individuals served. The Privacy Officer, in conjunction with the management staff, will determine mitigation appropriate to the severity of the violation.

M. **Employee System Access and Termination Procedures**

1. 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.

N. **Computer Usage**

1. Each staff member is responsible for understanding and following the Board's rules and guidelines regarding workstation and information system use and security.

O. **Social Media Use**

1. Social networking sites, notably Facebook but including many others, have become a significant communication medium in our world.

2. The Board mandates specific guidelines for the use of these sites 1) to limit activities in order to protect confidentiality and privacy of individuals being served, and 2) to permit other uses that advance the mission or the Board.

P. **Portable Computing Devices**

1. Mobile computing devices used by Board employees (laptops, smartphones and other devices) must be properly encrypted.

2. Employees are prohibited from using personally-owned computers for Board business, except for the purpose of accessing Board email. This includes smart phones, tablets, USB flash drives, laptop computers, home computers and any other electronic equipment.
3. Smart phones and personally owned computers are permitted only for the purpose of accessing Board email. Devices must be password protected. Passwords must never be shared or revealed to others.
4. All employees must receive appropriate training regarding using these safeguard and reporting lost or stolen devices.

Q. **Security Incident Response and Reporting**

1. The Board will monitor all electronic information systems for breaches of security, promptly respond to contain and mitigate security incidents, and employ continuous improvement principles so as to learn from and improve security after events.

Approved:
Board Policy, Chapter 9, 9/24/15, Board Action #15-61