CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION POLICY

This policy establishes that the Erie County Board Developmental Disabilities (Board) is committed to protecting each employee or individual's right to confidentiality. All information contained in an employee or individual's record is considered confidential. The Board recognizes an employee, individual, parent or guardian as the person responsible for providing authorization for use and disclosure of information when authorization is required.

The Board also recognizes that the content of these records is a proper subject for access or discussion only for certain persons engaged in official duties relative to that employee or individual. Contract providers or independent contractors engaged in official duties relative to that employee or individual may have access in the same manner. Volunteers will only be permitted access to records as deemed appropriate by the Department Director/designee.

It is understood that circumstances may require the Board to release information to ensure health, safety, and provision of services to individuals supported or employee welfare in emergency situations. If so warranted, the Board will only release necessary information in strict accordance to all legal requirements and procedures for confidentiality of individual information including their protected health information as defined in the Health Insurance Portability and Accountability Act (HIPAA).

The Superintendent shall establish, revise and keep current the procedures to be utilized in the implementation of this policy. The superintendent/ designee shall ensure compliance with these procedures. All revisions and changes will be shared with the Board when made.

Superintendent Signature: ______________ Date: 12/16/21

Implemented: 7/2011

Board Approval: 7/2011, 7/16/2015, 8/17/17, 11/21/19, 12/16/21

Revised: 7/2015, 5/8/17, 11/19/19, 12/16/21

Reviewed: 7/2015, 5/8/17, 11/19/19, 12/16/21

CROSS REFERENCE:
Ohio Revised Code (ORC) 149.43, 5123.61, 5123.89
ORC 5126.044 Ohio law on confidentiality policies and standards
45 Code of Federal Regulations (CFR) Part 160 and 164 generally
45 CFR Subpart E Privacy of Individual Identifiable Health Information
45 CFR 160.103 Definitions
45 CFR 164.504(g) for entities with multiple functions
45 CFR 164.302 Applicability
45 CFR 164.304 Definitions
45 CFR 164.306 Security Standards: General Rules
45 CFR 164.308 Administrative Safeguards
45 CFR 164.310 Physical Safeguards
45 CFR 164.312 Technical Safeguards
45 CFR 164.314 Organizational Requirements

Sensitivity: Internal

45 CFR 164.316 Policies and Procedures and Documentation Requirements
45 CFR 164. 318 Compliance Dates for the Initial Implementation of the Security Standards
45 CFR 164. 402-410 Breach/Notice of Breach to Individuals
45 CFR 164.502(b)(1) minimum necessary standard
45 CFR 164.502(a)(1)(iii) incidental uses and disclosures
45 CFR 164.514 (a-e), 45 CFR 164.502 (d)
45 CFR 164.528
National Institute for Stands and Technology (NIST) Special Publication (SP) 800-53
NIST SP 800-171
NIST CSF

Attachments: Consent to Release Information, Notice of Privacy Practices and Sign off sheet

POLICY: Administrative Resolution of Complaints for Individuals, Information Technology General Operations and Security Policy, Civil Rights Policy, Document Management, Retention and Destruction of Administrative Records Policy, Building Security and usage Policy.

Sensitivity: Internal

ERIE COUNTY BOARD OF DEVELOPMENTAL DISABILITIES
CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION PROCEDURE

I. DEFINITIONS

A. Applicable Requirements: Applicable Federal and Ohio Law contract between the Board and other persons or entities which conform to Federal and Ohio Law.

B. Authorization: An 'authorization' allows for the use and disclosure of Protected Health Information (PHI) for purposes other than Treatment, Payment, and Health Care Operations (TPO).

C. Board: The Erie County Board of Developmental Disabilities.

D. Breach: means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR Subpart E of this part which compromises the security or privacy of the protected health information, except when following exceptions apply: unintentional acquisition, inadvertent disclosure, reasonable believe that information was not retained

E. Business Associate (BA): 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 (45 CFR 160.103). For the purposes of this procedure this would include any individual or agency under contract with the Board to deliver services on behalf of the Board.

F. Confidential Information: shall mean private or otherwise sensitive information (not classified as protected health information (PHI)) that must be restricted to those with a legitimate business need. Examples of Confidential Information includes: personal identifiable information (PII), personnel information, system access passwords, file encryption keys, etc.

G. Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form. For the purpose of this procedure this includes the Board or any workforce member defined by procedure.

H. Council of Government (COG): A group of developmental disability (DD) Boards or other governmental entities which have entered into an agreement under ORC Chapter 167 and are operating in accordance with that agreement.

I. Guardian: A person who has the authority by law to act on behalf of an individual. This includes parents or properly appointed agents, such as those identified in documents like Durable Power of Attorney for Healthcare, or persons designated by state law.

J. EHR: An electronic record of health-related information on an individual.

K. Home and Community-Based Services Waiver Program (HCBS): Medicaid-funded home and community-based services waiver program available to individuals with a developmental disability granted to the Ohio Department of Jobs and Family Services by The Center for Medicaid and Medicare Services as permitted in 1915c of the Social Security Act, with day-to-day administration performed by the Ohio Department of Developmental Disabilities (DODD).

L. Health Care Clearinghouse: 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.

M. Health Care Operations: Any one of the following activities to the extent the activities are related to providing health care:

Sensitivity: Internal

1. Conducting quality assessment and improvement activities.
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. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
4. Business planning and development.
5. Business management and general administrative activities:
    a) Management activities related to HIPAA compliance;
    b) Customer service;
    c) Resolution of internal grievances;
    d) Due diligence;
    e) Activities designed to de-identify health information and fundraising activities for the benefit of the agency;
    f) DD operations includes transportation services.

N. 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.

O. Health Plan: An individual or group plan that provides or pays the cost of medical care. Health plan includes the following, singly or in combination:
1. The Medicaid program under Title XIX of the Act, 42 United States Code (U.S.C.) 396, 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.

P. HIPAA: The Health Insurance Portability and Accountability Act of 1996, codified in 42 USC 1320 – 1320d-8.

Q. Incidental Disclosure: An unintentional disclosure not specifically authorized which occurs during the normal course of business, such as an overheard conversation.

R. Individual: An individual applying for services, receiving services and supports, or terminated from services from the Board or a contracted entity or person under the Board's authority.

S. Individual File: A group of records maintained by or for the Board that is:
1. The medical records and billing records about individuals maintained by or for a covered health care provider.
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.
3. Used, in whole or in part, by or for the covered entity to make decisions about individuals.
4. For purposes of this definition, the term file means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for the Board.

T. Information Security Officer: An employee assigned responsibility for assuring

Sensitivity: Internal

Confidentiality, Integrity and Availability (CIA) of data and systems, assuring organization compliance with HIPAA Privacy and Security Standards. These responsibilities will include risk analysis coordination, risk management plan implementation, monitoring, policies interpretation, review and modifications as needed.

U. Minimum Necessary: "When using or disclosing the protected health information or when requesting protected health information from another covered entity, the Board must make reasonable efforts to limit the protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." (45 C.F.R. 164.502(b) and 45 C.F.R. 164.514(d)).

V. Minor: An individual under the age of 18 and has not been legally emancipated by a court.

W. Mitigation: Diminishing any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirement of HIPAA rules by the covered entity or its business associate.

X. MOU: Memorandum of Understanding between governmental entities which incorporates elements of a business associate contract in accordance with HIPAA rules.

Y. 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 (18) the individual must act on his or her own behalf, unless he/she has a court appointed guardian. This term does not include the state, if a child is a ward of the state.

Z. Payment: Payment includes all activities involved in billing and reimbursement.

AA. Privacy Officer: An employee appointed by the Superintendent responsible for assuring organization compliance with HIPAA Privacy and Security Standards. These responsibilities will include development and implementation of privacy policies and procedures, policies monitoring, interpretation, review and modifications, ensuring implementation and adherence to privacy practices.

BB. Personal Identifiable Information (PII): is the information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The term includes, but is not limited to:

1. The individual's/student's name;
2. The name of the individual's/student's parent or other family members;
3. The address of the individual/student or student's family;
4. A personal identifier, such as the individual's/student's social security number, student number, or biometric record;
5. Other indirect identifiers, such as the individual's/student's date of birth, place of birth, and mother's maiden name;
6. Other information that, alone or in combination, is linked or linkable to a specific individual/student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the individual/student with reasonable certainty; or
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates (CFR 34 99.3)

Sensitivity: Internal

CC. Protected Health Information (PHI): Individually identifiable health information that is or has been electronically held, maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is:
   1. Created or received by a health care provider, health plan, employer, or health care clearinghouse;
   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;
   3. Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (a)(4)(B)(iv); and (iii) Employment records held by the Board in its role as employer, regarding a person who has been deceased for more than 50 years.

DD. 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.

EE. Safeguards: Appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. Safeguards must be adequate to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the HIPAA rules.

FF. Sanctions: A penalty or disciplinary action taken against workforce members who fail to comply with the privacy policies and procedures of the covered entity or the requirements of HIPAA rules.

GG. Service Coordinator: A Service Coordinator performs the role as the single point of contact with individuals that live either in their own home, in their family's home, nursing home, or enrolled on an Individual Options Waiver or a Level 1 Waiver, and for families and guardians. The Service Coordinator may act in concert with another agency or individual in coordinating services (for example, may work with the school district for an eligible child who attends school), or will be the lead coordinator for county board DD services.

HH. TPO: Treatment, Payment or Health care operations under HIPAA rules.

II. Treatment: Is broadly defined and includes traditional health care services (nursing, Physical Therapy (PT), Occupational Therapy (OT), Speech Therapy (ST), psychological), as well as habilitation services, delegated nursing and case management/service coordination.

JJ. Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology (i.e., encrypted). Unsecured PHI can include information in any form or medium, including electronic, paper, or oral form.

KK. Use: 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.

LL. Workforce Member: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Board, is under the direct control of the Board, whether or not they are paid by the Board.

Sensitivity: Internal

II. PRIVACY MANAGEMENT PROCESS

Assign Privacy Responsibility

The Board will identify and assign privacy responsibilities to designated individual(s) responsible for privacy safeguards and rule compliance. The individual's position description should be updated to reflect assigned duties. Specific responsibilities of the Privacy Officer shall include:

A. Ensuring privacy policies, procedures, and standards are in place and adhered to by the Board.
B. Providing basic privacy support for all systems and users.
C. Providing on-going employee privacy education.

III. CONFIDENTIALITY

All information contained in an employee or individual's record is considered confidential. The content of these records is a proper subject for access or discussion only as an official member of an interdisciplinary team who is engaged in official duties relative to that employee or individual. Contract providers or independent contractors who are members of an interdisciplinary team may have access in this same manner. Volunteers will only be permitted access to records as deemed appropriate by the Department Director/designee.

IV. SAFEGUARDS

A. All Board personnel collecting, maintaining, using, or otherwise having access to personally identifiable data shall be informed of the confidentiality policies and procedures of the Board and are responsible for implementing them.
B. Each Department Director/designee, as a data owner, is responsible for assuring the confidentiality of any PHI, PII and other confidential information created or used by their program or department.
C. Each Department shall maintain, for public inspection, a current list of the names and positions of those employees within the department who may have access to confidential information and what PHI they may have access to.
D. When appropriate the Board will take the necessary measures to de-identify the protected health information of individuals in accordance with 164.514 (a-e) and 164.502 (d). A record has been de-identified when health information does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. To de-identify you must remove any number or element that will identify the individual.

V. RIGHTS TO ACCESS

A. The parent has the right to inspect and review any Board record related to his/her minor son or daughter enrolled in any program of the Board; a court-appointed guardian has the same right with respect to the records of his/her appointee; an employee or individual has the same rights regarding his/her own records.
B. The Board may presume that the parent has authority to inspect and review records relating to the individual unless the Board has been advised that the parent does not have the authority under state law related to guardianship, separation, and divorce.
C. Any program department shall comply with the employee, individual, parent or guardian requests for access to confidential material within ten (10) days. Requests occurring before an Individual Family Service Plan/ Individual Service Plan (IFSP/ISP) meeting or a hearing related to identification, evaluation, or placement of the individual shall have immediate response.
D. The Board is required to give an employee, individual, parent or guardian access to

Sensitivity: Internal

protected health information (under most circumstances) but is required to take reasonable steps to verify the identity of the individual making the request. No particular identification requirements are mandated (e.g., drivers license, photo ID); it is left up to the discretion of the Board.

E. The Board may charge a fee for copies of records which are made for the employee, individual, parent or guardian under this rule if the fee does not effectively prevent that person from exercising the right to inspect and review those records.

F. The Board may not charge a fee to search for or to retrieve information.

VI. EMPLOYEE, INDIVIDUAL, PARENT, OR GUARDIAN AUTHORITY

A. The Board recognizes an employee, individual, parent or guardian as the person responsible for providing authorization for use and disclosure of information for an individual.

B. Employees or Individuals who are not minors and who do not have a legal guardian are recognized by the Board as their own guardian.

C. A person who has the authority by law (such as a legal guardian) to act on behalf of an individual will be recognized by the Board unless it is decided that it is not in the best interest of that individual because the Board has reason to 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 or guardian.
   2. Treating such person as the guardian/parent could endanger the individual.

D. The parent of a minor will be recognized by the Board as the individual's guardian except as provided in Section IV above. Once a minor reaches the age of eighteen (18) or becomes married, whichever occurs first, the parent will no longer be recognized as the guardian of the individual, unless this authority is designated by law.

E. In the event an individual is deceased the following provisions apply:
   1. PHI generated during the life of an individual is protected from disclosure after death unless disclosure is for treatment, payment, or health care operations. The Board 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. Records of a person who has been deceased for more than 50 years can be released.
   2. If under applicable law, an executor, administrator, or other person has the authority to act on behalf of a deceased individual or of the individual's estate, the Board will recognize such person as a personal representative of the individual.
   3. 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 information 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:
      a) Spouse;
      b) Adult children;
      c) Adult grandchildren;
      d) Parents;
      e) Adult descendants of parents (brothers and sisters);
      f) Brothers and sister's adult children;
      g) Brothers and sister's adult grandchildren;

Sensitivity: Internal

h) Grandparents;
i) Adult descendants of grandparents (uncles and aunts).

VII. PERMITTED USES AND DISCLOSURES WITHOUT A WRITTEN AUTHORIZATION

Personally identifiable information from the records of an employee or individual may be disclosed without the written consent of the employee, individual, parent or guardian in some instances. The Board may use and disclose in the following situations without an authorization:

A. Use and disclosure during emergency situations.
   1. For the purposes of this procedure, an emergency situation shall be defined as an incident that puts the employee or individual's health and/or safety in immediate risk.
   2. In the event of an emergency disclosure of information, the person disclosing the information shall report the disclosure to an immediate supervisor. A good faith effort to report the disclosure to the employee, individual, parent or legal guardian and to obtain written acknowledgment shall be made as soon as is practicable following stabilization of the situation.
   3. To determine whether disclosure to a family member, relative, personal representative is in the best interest of the employee or individual and, if so, disclose only the personal information that is directly relevant to the individual's care related to the situation.
   4. To use and disclose personal information about victims of crime to law enforcement officers if they are unable to obtain the employee or individual's agreement because of incapacity or other emergency circumstances, including those situations that occur in locations other than on the premises of the agency.
   5. To use or disclose the restricted personal information if the employee or individual is in need of emergency treatment, even when the employee or individual previously requested restriction of uses and disclosures.

B. Use and disclosure to other staff who are acting in the capacity of an official member of an interdisciplinary team who are engaged in official duties relative to that employee or individual. In addition, the Board may disclose to the individual's team as identified by the individual/parent/guardian or as indicated in their individual services plan, the information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

C. Use and disclosure for treatment, payment, and operations.

D. Use and disclosure to other providers when necessary for the provider's treatment and payment.

E. Use and disclosure when reporting child abuse. Information may be disclosed by the Board to a public health authority or other appropriate government authority authorized to receive reports of abuse, neglect or domestic violence about a child whom the Board reasonably believes to be a victim of abuse, neglect or domestic violence, without consent or authorization. The Board is not required to inform the victim of the disclosure.

F. Use and disclosure related to abuse, neglect and domestic violence.
   1. Information may be disclosed by the Board to any governmental authority authorized to receive reports of abuse, neglect or domestic violence about an individual whom the Board reasonably believes to be a victim of abuse, neglect or domestic violence. There are three circumstances in which the Board may disclose information about these victims:

Sensitivity: Internal

a) Law requires disclosure related to abuse and the disclosure must comply with and is limited to the relevant requirements of such law;

b) The individual has agreed to such disclosure;

c) The disclosure is expressly authorized by statute or regulation and either the Board believes that disclosure is necessary to prevent serious harm to the individual or to other potential victims, or that individual is unable to agree due to incapacity, and the law enforcement or public official authorized to receive the report represents that the information sought is not intended to be used against the individual, and that an immediate enforcement activity would be materially and adversely affected by waiting.

2. The Board is required to promptly inform the victim/parent/guardian that it has disclosed information to report abuse, neglect or domestic violence unless the victim's safety would be placed in jeopardy due to the receipt of this information. The Board may provide this information orally, written notification is not required, and may be undesirable due to the potential for further harm to the individual by the abuser. The Board is not required to inform a parent/guardian if it is believed that the parent/guardian is responsible for the abuse, neglect or other injury, and that informing this person would not be in the individual's best interest.

G. Use and disclosure about an individual who is a victim of crime.

1. Health information may be disclosed for victims of a crime. State or other law may mandate disclosure.

2. The Board is required to obtain employee, individual, parent or guardian agreement, except for disclosures required by law. The agreement may be obtained orally or in writing. The agreement requirement is waived if any of the following conditions apply:

a) The covered entity is unable to obtain the agreement because of the employee or individual's incapacity or other emergency circumstance;

b) The law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred, and the information is not intended to be used against the victim;

c) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be harmed by waiting until the employee or individual is able to agree;

d) The Board believes the disclosure is in the best interest of the employee or individual.

3. The Privacy Rule does not allow the Board to initiate disclosures of information, the disclosure must be in response to a request from law enforcement, and the minimum necessary standard applies to all disclosures.

4. The Board is required to promptly inform the victim, parent or guardian that it has disclosed information to report abuse, neglect or domestic violence unless the victim's safety would be placed in jeopardy due to the receipt of this information.

H. Use and disclosure related to crime perpetrated by an individual served by the Board.

1. Staff members who are victims of a crime perpetrated by an individual

Sensitivity: Internal

served by the Board may disclose certain information about the individual to a law enforcement agency.

2. If a staff member or a business associate of the Board is the victim of a crime perpetrated by an individual served by the Board, they may disclose information to the appropriate law enforcement agency for the purposes of reporting the crime. The information which may be disclosed is limited to the individual's:
    a) Name and address;
    b) Date and place of birth;
    c) Social security number;
    d) ABO blood type and ph factor;
    e) Type of injury;
    f) Date and time of treatment;
    g) Date and time of death, if applicable;
    h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

I. Uses and disclosures required by other laws.

J. Use and disclosure during judicial proceedings.

K. Use and disclosure to Federal, State, and other legal or regulatory officials in connection with the audit and evaluation of federally supported program, or in connection with the enforcement of or compliance with the Federal legal requirements which relate to these problems.

L. Use and disclosure to a law enforcement officer or official of the courts engaged in investigations.

M. Use and disclosure approved by the employee, individual, parent or guardian through verbal agreement. The Board may use and disclose certain information without the written consent or authorization if the employee, individual, parent or guardian has been informed in advance of the use or disclosure and has the opportunity to agree, prohibit, or restrict the disclosure. The Board may orally inform the employee, individual, parent or guardian of the permitted uses and disclosures permitted by this procedure. The Human Resource Department is responsible for documenting the agreement, prohibition or restriction of an employee. The primary person responsible for the coordination of services for the individual, as identified by the Board, must document the agreement, prohibition, or restriction through field-notes or other appropriate means. If the employee or individual is present for or otherwise available prior to a use or disclosure and has the capacity to make health care decisions, the Board may use or disclose the information if it:
    1. Obtains verbal agreement;
    2. Provides the employee or individual with the opportunity to object to the disclosure, and the individual does not express an objection;
    3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the employee or individual does not object to such disclosure.

VIII. SUBPOENAS AND SEARCH WARRANTS

Records maintained by the Board regarding individuals supported by the Board are confidential, are not public records and can only be disclosed under certain circumstances. All Board personnel will abide by the following procedure if someone presents a subpoena or search warrant. If a proper subpoena has not been issued, or the person is not a law

Sensitivity: Internal

enforcement officer, or the law enforcement officer does not have a search warrant, the Board will not furnish any confidential information to the person. Employee records are considered public records as long as they do not contain protected health information.

A. Subpoenas
   1. If a subpoena is issued to an employee of the Board, which requests that the employee produce documents maintained by the Board regarding individuals supported by the Board, or employees employed by the board, the employee shall immediately notify the Department Director/designee or the Superintendent. The Board shall contact the Prosecuting Attorney or other legal counsel to address the validity of and obligation to respond to the subpoena.
   2. No employee has authority to, shall not agree to disclose, and shall not disclose any records maintained by the Board regarding individuals supported by the Board, or employees of the board unless approved by the Department Director/designee or Superintendent.

B. Search Warrants
   1. Board personnel who are approached by anyone alleging to be a law enforcement officer should immediately contact the applicable Department Director/designee. Until approved by the Department Director/designee or Superintendent, Board personnel shall not disclose any information. Board personnel shall refer the person to the Department Director/designee.
   2. The Department Director/designee shall ask for the officer's identification and the search warrant. The Department Director/designee shall photocopy the ID and contact the applicable law enforcement agency to verify the identity of the law enforcement officer. The Department Director/designee should initially review the search warrant to determine the scope of the search warrant.
   3. If presented with a search warrant, Board personnel will not interfere with the search and seizure. If this happens at night or on a weekend, Board personnel shall contact the Department Director/designee at home.
   4. Board personnel shall always cooperate with law enforcement agents who have shown appropriate identification and authorization for the search. Interfering with or impeding a lawful search may also constitute a criminal offense under State and Federal law.
   5. Upon presentation of a search warrant, the Board shall immediately contact the Erie County Prosecuting Attorney.

IX. USES AND DISCLOSURES WITH AN AUTHORIZATION

A. When a request for disclosure of information of an employee or individual is received by any Department that information will be sent within ten (10) days of receipt of the request provided that appropriate consent is obtained.

B. The employee, individual, parent or guardian will be given the opportunity to agree or object to the release of all protected health information, in a manner that is understandable to that person, prior to the release of the information.

C. The Privacy Officer shall implement procedures to obtain written consent of the employee, individual, parent or guardian before disclosing information from records or when the Board is requesting information from another agency. The written consent must be signed and dated by the employee, individual, parent or guardian giving the consent and shall specify the records to be disclosed, the purpose or purposes of the disclosure, and the party or class of parties to whom the disclosure

Sensitivity: Internal

may be made and the time period for which permission is granted.

D. Consent must also be obtained in accordance with the Family Education Rights and Privacy Act (FERPA), prior to disclosing information:
   1. To officials of another school, school district, or other educational agency in which a school-aged student is to be enrolled.
   2. When the transfer of records is initiated by the parent served through the educational component.
   3. When a school district or other educational agency includes a notice in its policies and procedures that it forwards education records on request to a school district or other educational agency in which a student is to be enrolled.

E. When a disclosure is made, a department shall, upon request, provide a copy of the record which is disclosed to the employee, individual, parent or guardian.

F. Disclosure of information authored by a party or agency other than staff or consultants of the Board requires authorization of that party/agency.

G. Disclosure of information also includes verbal sharing (meetings, telephone conversations, etc.) which requires written consent as outlined above. Record of such disclosure shall be recorded.

H. Reports of abuse, neglect, and other major unusual incidents made under Section 5123.61 of the ORC are not public records as defined in Section 149.43 of the code.

X. REQUESTING AUTHORIZATIONS

A. In situations when an authorization is required, Board employees should complete the form, Consent to Release Information (Attachment A).

B. The receiving party can be an individual, an organization, or classes of individuals or organizations.

C. The authorization should be completed including all required elements being specific with the portion of the information to be released. Avoid specifying the entire individual's file unless absolutely necessary.

D. The expiration date in general should be no more than one year from the date of the authorization.

E. The employee, individual, parent, or guardian should be asked to approve the authorization.

XI. CORE ELEMENTS OF A VALID AUTHORIZATION

Authorizations for the release of information may be received on forms prepared by other organizations. These forms are acceptable if they contain at least the following elements and are written in plain language. <u>If any of the following elements are exempt, authorization will be denied:</u>

A. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

B. The name or other specific identification of the person or class of persons authorized to make the requested use or disclosure.

C. The name or other specific identification of the person or class of persons to whom the Board may make the requested use or disclosure.

D. An expiration date.

E. A statement of the employee, individual, parent, and guardian's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the employee, individual, parent or guardian may revoke the authorization.

F. A statement that the information used or disclosed pursuant to the authorization

Sensitivity: Internal

may be subject to re-disclosure by the recipient and no longer be protected by the HIPAA Privacy Regulations.

G. A statement that the Board is not allowed to require the employee, individual, parent or guardian to sign the authorization in order to receive services from the Board.

H. Signature of the employee, individual, parent or guardian and the date.

I. If a surrogate decision maker of the individual signs the authorization form, a description of such surrogate decision maker's authority to act for the individual is required.

J. The authorization form may contain elements or information in addition to the required elements, provided that such additional information or elements are not inconsistent with the required elements.

XII. DEFECTIVE AUTHORIZATIONS

An authorization form is considered defective and invalid if any material information in the authorization is known to be false by the Board or its employees or if any of the following defects exist:

A. The expiration date has passed or the expiration event is known by the covered entity to have occurred;

B. The authorization form has not been filled out completely;

C. The authorization form is known by the covered entity to have been revoked;

D. The authorization form lacks any one of the core elements previously described;

E. The authorization form is combined with another document.

XIII. PROCESSING AUTHORIZATIONS

A. The Department Director/designee should review the authorization against the criteria above (Core Elements for a Valid Authorization and Defective Authorizations) to verify the validity of the authorization. For any defects, contact the employee, individual, parent or guardian so that it can be corrected.

B. Verify the identity of the person requesting the information.

C. Send the information as requested from the official file.

D. Save a copy of the authorization in the individual's file, and give or send a copy to the employee, individual, parent or guardian upon request.

XIV. VERIFICATION OF THE IDENTITY OF PERSON REQUESTING THE INFORMATION

A. The Board must verify the identity of a person requesting information and the authority of any such person to have access to information if the identity or any such authority of such person is not known to the Board. To verify the requestor of information, the Board employee responding to the request may verify the person through:

1. A known place of business;
2. A known address;
3. A known phone or fax number;
4. A known human being.

B. The Board must obtain verification of the identity prior to the disclosure of the requested information. Documentation of the verification must be maintained in the official file.

C. When the person requesting the information is a public official, the Board may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of information is to a public official or a person

Sensitivity: Internal

acting on behalf of the public official.

1. If the request is made in person, presentation of agency identification badge, other official credentials, or other proof of government status.
2. If the request is in writing, the request is on the appropriate government letterhead.
3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of 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.
4. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.
5. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

D. When the person requesting the information is a person assisting in the individual's care, the Board is required to verify the identity and authority of the person before disclosing information and assure that the information requested falls within the normal area of support the person provides to the individual. Staff receiving a request for information in this situation shall obtain verification from the individual/agency by:

1. Having personal knowledge of the person's role with the individual (i.e., social worker, nurse, service coordinator, etc.);
2. By confirming the person's role through written verification from employer or relationship with the individual;
3. By confirming through other county board staff having knowledge of the requestor's role with the individual.

E. Verification is not required if there is an imminent threat to safety. It is lawful to disclose information to prevent or lessen a serious and imminent threat to the health or safety of a person or the public if disclosure is made to a person reasonably able to prevent or lessen the threat. If these conditions are met, no further verification is needed. In such emergencies, the Board is not required to demand written proof that the person requesting the information is legally authorized. Reasonable reliance on verbal representations is appropriate.

F. Disclosure to the Secretary of the Department of Health and Human Services is required for purposes of enforcing Security and Privacy regulations. When information is requested by the Secretary of the Department of Health and Human Services for compliance purposes, the Board must verify the identity of the requestor and their authority to access protected health information as would be required for any other law enforcement or oversight agency request for disclosure.

XV. RIGHT TO REVOKE AN AUTHORIZATION

A. An employee, individual, parent or guardian may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

1. The Board has taken action in reliance thereon; or
2. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

Sensitivity: Internal

B. An authorization which has been revoked is no longer valid.

C. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the office, facility, program or employee has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law.

XVI. MINIMUM NECESSARY USE AND DISCLOSURE

All persons who handle individual information in any manner are expected to know and abide by the following:

A. Access to the information will be granted based on the individual's role and determined by each Department Director/designee of the Board. The Board will identify:

1. Those persons or classes of persons, who require access to individual information to carry out their duties, in the workforce, including interns and trainees, according to job classification with the necessary minimal necessary information required for successful job performance to serve the individual, and
2. For each such person or class of persons, the category or categories of information to which access is needed and any conditions appropriate to such access.

B. Whenever requesting information from another entity, the Board personnel shall limit the request to the minimum necessary.

C. All personnel should take care to avoid requesting the entire individual file unless this is absolutely necessary.

D. The Department Director/designee may rely on the belief that the information 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 the minimum necessary information;
2. The request is from another covered entity;
3. The request is from a professional at the Board, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary.

E. The Board will implement controls/measures to limit access for minimal necessary use and disclosure including but not limited to:

1. Computer access levels and passwords;
2. Limited access to files, sign-out procedures;
3. Securing file cabinets and file rooms at night.

XVII. EXEMPTIONS FROM THE MINIMUM NECESSARY PROVISIONS

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

A. For treatment purposes;

B. For information requested by the employee, individual, parent or guardian;

C. For information requested pursuant to a valid authorization by the individual/parent/guardian;

D. For compliance with standardized Health Insurance Portability and Accountability Act (HIPAA) transactions;

E. For required disclosures to the Department of Health and Human Services (DHHS)

Sensitivity: Internal

for enforcement purposes;

F. For instances required by other law;

G. When ordered by the court (only information directly requested by such an order is to be provided).

XVIII. NON-ROUTINE DISCLOSURES OR REQUESTS

A. For non-routine disclosures, when subject to the minimum necessary provision, the Privacy Officer (or his/her designee) shall review the request for compliance with the minimum necessary requirements.

B. For non-routine requests, the requesting party will utilize the minimum necessary principle.

XIX. ROUTINE DISCLOSURES OR REQUESTS

A. Procedures for Routine Disclosures: Will follow the minimum necessary standards and document on the Consent to Release information form.

B. Procedures for Routine Requests: Will follow the minimum necessary standards and procedures for requesting information.

XX. DISPOSAL OF RECORDS

The Department Director/designee shall make varied attempts to obtain prior written permission from the individual/parent/guardian in the event that official personally identifiable information collected, maintained, or used is destroyed. Copies of these records shall be made available to the individual/parent/guardian upon request. Records will only be disposed of in accordance with the Document Management Policy and Schedule of Records Retention and Disposition (Form RC-2).

XXI. MAINTENANCE OF RECORDS

A. Employee and Individual records are maintained in both paper and electronic paperless format(s) dependent on department procedures. All electronic data will be recorded within forty-five (45) days of receipt, paper records will be recorded within ten (10) days of receipt.

B. No records will be physically removed from the premises, copies will be provided in accordance with disclosure requirements.

XXII. ACCOUNTING OF DISCLOSURES

Individuals have the right to ask how the Board has shared their PHI on and after April 14th, 2003. They may request this accounting of all disclosures for a period of time up to six years from the date of the request. The disclosures legally permitted and described in the Board's Notice of Privacy Polices do not have to be included in the disclosure report.

A. The Board will ask the requestor to complete the "Request for Accounting of PHI Disclosure" form, and will explain the process:

1. The Board is required to give an individual an accounting or the summary of disclosures, or tell the individual if the Board needs more time to respond to the request within sixty (60) days after the request is received.
2. The first accounting of disclosures or summary in any 12-month period is free. If an individual requests more than one accounting or summary in a 12-month period, the Board can charge a fee for the costs of the copies of the PHI or the cost of preparing the summary.
3. The Board must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement

Sensitivity: Internal

official, if such agency or official requests such suspension, if such disclosure would impede agency activities.

4. The requests will be reviewed and considered by Privacy Officer.

B. Upon review and approval Privacy Officer accounting of disclosures will be provided to individual.

C. Reportable disclosures are subject to accounting of disclosures requests and shall be tracked in individual's file using the "Organization Accounting of Disclosures" form.

D. Disclosures subject to accounting of disclosures reporting are:

1. Disclosures for law enforcement regarding crime on premises or in emergencies when crime is suspected;
2. Disclosures for public health purposes;
3. Disclosures of student immunization;
4. Birth and death reporting;
5. For cadaveric organ, eye and tissue donation;
6. For judicial and administrative proceedings;
7. For research with an Institutional Review Board (IRB) Waiver;
8. To military command authorities;
9. For Workers Compensation purposes;
10. To correctional institutions except as detailed in (45 CFR 164.5129k)(5);
11. About decedents to medical examiners, coroners, funeral directors;
12. About victims of abuse or when regarding child abuse or neglect;
13. To the Food and Drug Administration (FDA).

E. Disclosure NOT subject to accounting of disclosures:

1. Authorized (authorization form on file) (45 CFR 164.508);
2. Treatment payment and operations (TPO) related disclosures (45 CFR 164.502), individual own disclosures to parent, guardian etc. incidental disclosures;
3. To persons involved in the individual's care or other notification purposes (45 CFR 164.510);
4. For national security and intelligence purposes, as detailed in (45 CFR 164.512(k)(2));
5. Disclosures to prisons and other law enforcement agencies regarding an individual who is in custody, as detailed in (45 CFR 164.512(k)(5));
6. Healthcare operations related disclosures when payment is received for disclosed PHI have to be accounted for.

XXIII. AMENDMENT OF RECORD AT PARENT/GUARDIAN/INDIVIDUAL REQUEST

A. An individual/parent/guardian who believes that information in their record is inaccurate or misleading or violates the privacy or other rights of the individual may make a request to their Service and Support Administrator (SSA)/Service Coordinator of that component, which maintains the information, to amend the information. The procedure to request information is outlined below:

1. The Request should be in writing and made either by the individual/parent/guardian or with the individual/parent/guardian's consent.
2. The request should be given to the individual's SSA/Service Coordinator and a copy forwarded to the Privacy Officer.
3. The individual's Service Coordinator will consult with their supervisor and they will collaboratively evaluate how to efficiently process the request.
4. The supervisor shall present the request with recommendation on how to

Sensitivity: Internal

fulfill the request to the Department Director/designee who will decide whether or not to amend the information.

5. The request will be processed no later than sixty (60) days after the date of the request. The Board may extend the time by not more than thirty (30) days if the Board gives the individual/parent/guardian written notice of the extension.
6. The Service Coordinator will provide a copy to the Privacy Officer and implement the necessary steps to process the request within the indicated timelines.
7. The Privacy Officer of the Board shall be notified of all requests for amendments and ensure that the Board retains documentation relating to the amendments for at least six (6) years or as otherwise required by applicable requirements and Board procedures.

B. If the Board accepts the requested amendment, in whole or in part, the Board will make the appropriate amendment, and inform the individual and other persons or entities who have had access to the information. This includes the release of this information to outside entities as the result of a written request.

C. If a decision is made not to amend the information in accordance with the request, the Department Director/designee shall inform the individual/parent/guardian of the refusal in writing, which includes the following:
1. The basis for the denial;
2. The individual/parent/guardian's right to submit a written statement disagreeing with the denial and how the individual/parent/guardian may file such a statement;
3. A statement that, if the individual/parent/guardian does not submit a statement of disagreement, the individual/parent/guardian may request that the Board provide the individual/parent/guardian's request for amendment and the denial with any future disclosures of the individual information that is the subject of the amendment;
4. A description of how the individual/parent/guardian may complain to the Board or the Secretary of Health & Human Services. The description must include the name, or title, and telephone number of the contact person or office.

D. The Board will permit the individual/parent/guardian to submit to the Board a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

E. The Board may prepare a written rebuttal to the individual/parent/guardian's statement of disagreement. Whenever such a rebuttal is prepared, the Board must provide a copy to the individual/parent/guardian who submitted the statement of disagreement.

F. With regards to future disclosures of covered records the following applies:
1. Records must include the statements of disagreement and rebuttals.
2. Future disclosures of covered records must include relevant amendments and rebuttals.
3. If an individual/parent/guardian has not submitted a statement of disagreement, the Board must include the following with all subsequent disclosures:
   a) The individual/parent/guardian's request for an amendment;
   b) The Board notice of denial;
   c) If the disclosure which was the subject of amendment was

Sensitivity: Internal

transmitted using a standard Electronic Document Imaging format and the format does not permit including the amendment or notice of denial, the Board may separately transmit the information to the recipient of the transaction in a standard Electronic Digital Imaging format.

G. The Board that is informed by another entity of an amendment to an individual's information must amend the information in designated record sets.

H. The individual/parent/guardian may exercise their due process rights as outlined in the Complaint Resolution Policy/Procedure at any time during this process.

XXIV. INDIVIDUAL REQUESTED RESTRICTIONS OF THEIR INFORMATION

Individuals/parents/guardians have the right to request restrictions over and above the standard protections offered by Board policies. Granting these requests will be done at the Board's discretion, which shall include consideration of whether the restriction can be administered. Any request granted will be honored, except in emergency situations, or until terminated. Procedures to request a restriction are outlined below:

A. Requests shall be in writing and made either by the individual/parent/guardian or with the individual/parent/guardian's consent. The request should be given to the Service Coordinator and a copy forwarded to the Privacy Officer.

B. The individual's Service Coordinator will consult with their supervisor and they will collaboratively evaluate:
   1. The Boards ability to administer such a restriction, and the costs involved;
   2. The health/safety/welfare needs of the individual requesting the restriction.

C. Based on this evaluation, a recommendation shall be made to the Department Director/designee who will either approve or deny the request.

D. The Service Coordinator shall inform the individual/parent/guardian of the decision, and document the decision in the individual's file, provide a copy to the Privacy Officer and implement the necessary steps to ensure proper enforcement of the restriction.

E. These restrictions will not apply during an emergency. In the event these restrictions are broken in the course of an emergency, and information is disclosed to a health care provider, a request shall be made to that provider to not further use or disclose the information.

XXV. TERMINATION OF THE RESTRICTION

A. In the event that the Board wishes to terminate the restriction, the request will be discussed with the individual/parent/guardian. The individual/parent/guardian's written agreement to terminate the restriction must be filed in their master file, or if it is received verbally, that verbal agreement must be documented in the file and a copy given to the Privacy Officer.

B. The Board may unilaterally terminate the restriction. Such a termination without the individual/parent/guardian's agreement must be documented in the individual's file and the individual/parent/guardian must be notified. Such a termination will apply only to information created after the date of the termination.

XXVI. INDIVIDUAL REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Individuals/parents/guardians are entitled to request confidential communications, including for example, not sending information to their home address or telephoning their home number. These requests will be honored to the extent that they can be reasonably accommodated with our administrative systems by following the steps outlined below:

A. Requests for confidential communications should be made in writing by the

Sensitivity: Internal

individual/parent/guardian.

B. The request should be given to the Service Coordinator and a copy forwarded to the Privacy Officer.

C. When the Service Coordinator receives a request, they may not ask the reason for the request.

D. The Service Coordinator will work in conjunction with their supervisor to develop a plan to implement the request if appropriate.

E. The Service Coordinator shall contact the individual/parent/guardian making the request to obtain an alternate means of contacting them (e.g. cell phone, PO Box, etc.).

F. The individual/parent/guardian will be informed at that time of steps the Board will take to implement the request.

G. If existing systems are capable of administering the request, the Service Coordinator shall make sure that necessary steps are taken to implement the request, such as adjusting phone numbers or addresses in computer files or mailing lists.

H. The Service Coordinator shall assure that the request is documented, and disposition is filed in the individual's file.

I. 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.

XXVII. BREACH

A. Upon the discovery of a security incident the Department Director/designee will take immediate action in an effort to minimize the misuse of the information in question. The Privacy and Security Officer's will be notified, will determine if the incident is a breach and will work in conjunction with the responsible department to ensure that appropriate notice is given, and will track and report the Board's breaches in accordance with applicable requirements.

B. The Department Director/designee will work with the Privacy and Security Officers, Human Resources Department to determine the appropriate sanctions to be taken against the workforce member(s) responsible for the breach in accordance with the Corrective Action for Management Employees & Corrective Action for Civil Service Employees procedures and Union contracts.

C. The Board will determine if additional safeguards need to be put into place based upon the nature of the breach and risk of further exposure to the individuals involved. These safeguards may include but are not limited to; performing credit checks, purchasing identity theft insurance, revising procedures on how PHI is secured, etc.

XXVIII. NOTICE OF A BREACH TO EMPLOYEES AND INDIVIDUALS

A. The Board will provide notice in the event of a breach of unsecured PHI, PII or other confidential information as required by State and Federal Laws. Notifications will be sent to the affected person(s), the Secretary of Health and Human Services (HHS) and under some circumstance the media. Breaches Subject to Notification: Notification requirements only apply to breaches of unsecured PHI and confidential information as required by State and Federal Laws.

B. Data breach is generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information,

Sensitivity: Internal

unless organization or business associate can demonstrate that there is a low probability that the protected health information has been compromised, or one of the exceptions to the data breach definition applies. Breach definition includes following exceptions:

1. Unintentional acquisition, access or use by employee (acting under authority);
2. Accidental disclosure between authorized employees; and
3. When there is a good faith believe that information could not have been retained by unauthorized individual, to whom impermissible disclosure was made.

C. While the above definition of PHI data breach comes from the HIPAA Omnibus rule, the same concepts can be applied to personally identifiable information (PII). Organizations' serving individuals from various States shall also be aware of State data protection laws that may be more stringent than federal data protection laws. Massachusetts defines the data breach as unauthorized acquisition or use of unencrypted personal information (can be PHI or PII data), that creates substantial risk of identity theft or fraud for the individual. Other States' data breach definitions are similar (201 CMR 17.00 Standards for the protection of personal information of residents of the Commonwealth). Texas, California and other States impose specific rules as well.

D. This procedure describes steps to be taken in case of security incident likely resulting in data breach. After escalating security incident to data breach status Security Officer will:

1. Identify timelines for meeting investigation and notification requirements (time sensitive project plan).
2. Use SECURITY INCIDENT RESPONSE REPORT SharePoint database to document and identify actions necessary to mitigate data breach results, actions necessary to comply with HIPAA Rules, and individuals to be included in addressing the incident. Organization shall consider at least including Legal Counsel and Privacy and Security expert in developing plan to address data breach.
3. Use eSECURITY_INCIDENT_RESPONSE.xlsx DECISION CHART to investigate and document, factors to consider in assessing the probability of PHI being compromised, including:
   a) What type of data has been compromised, what are the data elements involved and how likely data can be re-identified;
   b) Who is the unauthorized person who used the protected health information or to whom the disclosure was made;
   c) Was the protected health information actually acquired or viewed only; and
   d) The extent to which the risk to the protected health information has been mitigated (what were the immediate mitigation steps).
4. Complete incident risk assessment using eSECURITY_INCIDENT_RESPONSE.xlsx DECISION MATRIX(Attachment C). Considering the above factors will help identify the high or low probability of data being compromised and will determine need for data breach notification.
5. Retain the copy of the security incident report (SIR), risk assessment (Decision Matrix) and all supporting documentation in all situations, even when level of information compromise is low and no breach notification is

necessary. Organization must maintain supporting documentation sufficient to meet their burden of proof regarding the breach assessment – and if applicable, notification - process including:

a) Documentation of the risk assessment demonstrating the conclusions reached;

b) Documentation of any exceptions determined to be applicable to the impermissible use or disclosure of the PHI; and

c) Documentation demonstrating that all notifications (including notifications to individuals) were made, without unreasonable delay and in no case later than within 60 days of discovery of a breach, if a determination was made that the impermissible use or disclosure was a reportable breach.

E. Before issuing any data breach notification and following HHS Breach Notification rule http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html the organization leadership and Security Official shall conduct thorough investigation verifying that data breach in fact occurred, and account for number of individuals affected by data breach, as reporting responsibilities differ based on number of individuals affected (500+). **Ask for second opinion.**

F. After notification requirements determination (item C above) and using information in eSECURITY INCIDENT RESPONSE form, prepare, deploy and distribute, as required per specific situation:

1. Mitigation strategy e.g. credit monitoring for affected individuals;
2. Communications strategy about data breach and mitigation efforts e.g. website posting;
3. Notice to individuals and notice to the Secretary;
4. Notice to media

G. The notification required by this section shall be written in plain language and shall include, to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

XXIX. COMPLAINT RESOLUTION

A. Any employee, individual, parent, guardian that has a concern about their privacy rights, that their privacy rights have been violated, or disagree with a decision that has been made by the Board concerning their privacy rights should contact their Service Coordinator and make their concern known, or contact one of the following:

Sensitivity: Internal

1. Erie County Board Privacy Officer:
   4405 Galloway Rd. Sandusky, Ohio 44870
   (419) 626-0208
2. The Secretary of the U.S. Department of Health and Human Services at:
   200 Independence Ave. SW, Washington D.C. 20201
   1-877-696-6775
3. The Office for Civil Rights (OCR), U.S. Department of Health and Human Services at:
   200 Independence Ave. SW, Room 509 F, HHH Building,
   Washington D.C., 20201
   Call Office for Civil Rights' (OCR) hotline – 1-800-368-1019
   E-mail – orcmail@hhs.gov

B. The Board will assist an employee, individual, parent, guardian in making a complaint to any of the above listed offices if the individual/parent/guardian requests assistance.

C. If any workforce member receives a complaint from an employee, individual, parent, guardian about their privacy rights they should:
   1. Forward that complaint in writing to the Privacy Officer.
   2. The Privacy Officer will notify the Superintendent that a complaint has been filed.
   3. The Privacy Officer will work to resolve the complaint. as outlined in the Administrative Resolution of Complaints Policy/Procedure.

D. The Board will retain all documentation of complaints related to the uses and disclosures of related PHI, and the dispositions of these complaints, in accordance with the HIPAA documentation policy as defined under the HIPAA Privacy Rules CFR 164.530 (J).

E. If it has been determined that an employee is in violation of this procedure, corrective action may be taken against that employee as outlined in the Corrective Action for Management Employees & Corrective Action for Civil Service Employees procedures as applicable. Appropriate action will also be taken for other workforce members in violation of the Confidentiality of Protected Health Information Held by the Board policy and this procedure.

F. If a workforce member is found to have incidentally disclosed employee or individual information, that workforce member will be trained on the confidentiality policy and the proper methods for disclosing individual information. If there are reoccurring offenses, the employee will be subject to corrective action in accordance with the ECBDD Personnel Policy- Discipline and Corrective Action, section 709 and the Information Technology, General Operations and Security Policy section II.D. Appropriate actions will also be taken for other workforce members found to have reoccurring offenses of incidentally disclosing PHI. The Board recognizes that incidental disclosures occur, however, measures will be taken to minimize incidents (i.e.... training, information systems security, file security, etc). All incidents of incidental disclosure of information will be reported to the Privacy Officer.

G. The Board will not take any retaliatory measure against the complainant during or following this process as specified under HIPAA rules 45 CFR 160.310 (b).

XXX. NOTICE

The Board shall give adequate notice of the uses and disclosures of PHI that may be made by the Board, and of the employee, individual, parent, guardian's rights and the

Sensitivity: Internal

Board's legal duties with respect to PHI.

A. An employee, individual, parent, guardian has a right to adequate notice of the uses and disclosures of the PHI that may be made by or on behalf of the Board, and of the employee, individual, parent, guardian's rights and the Board's legal duties with respect to the individual's PHI. The Board will provide notice:
   1. No later than April 14, 2003 to individuals enrolled in Board services;
   2. Thereafter, at the time of enrollment, to individuals who are new enrollees;
   3. In an emergency treatment situation, as soon as reasonably practicable after the emergency situation;
   4. Within sixty (60) days of a material revision to the notice to individuals enrolled in Board services;

B. Except in an emergency situation, the Board shall make a good faith effort to obtain a written acknowledgment of receipt of the initial notice provided, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained.

C. An acknowledgment is not required for revised notices or periodic notices on availability of notice and how to obtain notice.

D. The Notice of Privacy Practice shall be available at all sites operated by the Board for individuals to request to take with them.

E. The Board shall post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the Board to be able to read the notice. e.g. posted on the Board's website.

F. Whenever the notice is revised, the Board shall make the notice available upon request on or after the effective date of the revision and shall promptly post as required in this paragraph.

G. The notice of privacy practices (Attachment B) must be written in plain language and must contain the following elements:
   1. The following statement in a header or otherwise prominently displayed: "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".
   2. A description, including at least one example, of the types of uses and disclosures that the Board is permitted to make for purposes of treatment, with sufficient detail to place an individual/parent/guardian on notice of the uses and disclosures permitted or required. The description should clarify that any disclosure outside of the Board requires prior authorization;
   3. A description, including at least one example, of the types of uses and disclosures that the Board is permitted to make for purposes of payment and health care operations, with sufficient detail to place an individual/parent/guardian on notice of the uses and disclosures permitted or required;
   4. A description of each of the other purposes for which the Board is permitted or required to use or disclose PHI without an individual/parent/guardian's consent or authorization, with sufficient detail to place an individual/parent/guardian on notice of the uses and disclosures permitted or required;
   5. A statement that other uses or disclosures will be made only with the individual/parent/guardian's written authorization, and that the authorization may be revoked in accordance with the procedure on authorizations;

Sensitivity: Internal

6. If the Board intends to contact the individual/parent/guardian for appointment reminders, treatment alternatives or other health related benefits, a separate statement describing such contacts;
7. A statement of the individual/parent/guardian's rights with respect to the individual's PHI, and a brief description of how the individual/ parent/ guardian may exercise those rights, including: the right to request restrictions on certain uses/disclosures of PHI, and the fact that the Board does not have to agree to such restrictions; the right to receive confidential communications of PHI; the right to inspect and copy PHI upon written request; the right to amend PHI; the right to receive an accounting of disclosures of PHI, and; the right to receive a paper copy of the privacy notice (each of the above in accordance with relevant procedures);
8. A statement of the Board's duties with respect to PHI, including statements: that the Board is required by law to maintain the privacy of PHI and to provide individuals/parents/guardians with notice of its legal duties and privacy policies; that the Board is required to abide by the terms of the currently effective privacy notice;
9. A statement that the Board reserves the right to change the terms of the notice and make the new notice provisions effective for all PHI that is maintained, along with a description of how the Board will provide individuals/parents/guardians with the revised notice;
10. A statement that individuals/parents/guardians may complain to the Board and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual/ parent/ guardian will not be retaliated against for filing a complaint;
11. The name, or title, and telephone number of the person or office to contact for further information;
12. The effective date of the notice, which may not be earlier than the date printed or published.

H. When there is a material change to the uses or disclosures, the individual/ parent/ guardian's rights, the Board's legal duties, or other privacy practices described in the notice, the Board shall provide a notice of such change.
   1. Notice of material changes shall be made no later than 60 days after the change is effective.
   2. The notice shall incorporate all material changes and shall be distributed in accordance with this procedure within the time period required in this procedure.
   3. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.
   4. The Board is not required to obtain acknowledgment of a revised notice.

I. The Board will maintain the web site; the notice will be posted on the web site and be made available electronically through the web site.

J. The Board shall retain copies of the notices issued by the Board and any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment. Copies of such notices shall be retained for a period of at least six years from the later of the date of creation of the notice or the last effective date of the notice. Acknowledgments or documentation of good faith efforts to obtain acknowledgment shall be retained for a period of at least six years from the date of receipt.

Sensitivity: Internal