JEFFERSON COUNTY BOARD OF DEVELOPMENTAL DISABILITIES

Privacy and Security Standards

HIPAA, FERPA, IDEA & Ohio Law Compliance Using the NIST Cybersecurity Framework (CSF)

Updated November 2025

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

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

Disclaimer
These sample standards are provided as a compliance aid to county DD boards in Ohio. These policies address privacy and computer security and are drafted for compliance with HIPAA, FERPA, IDEA and Ohio state law. Regarding Ohio State law, in particular ORC § 9.64, these standards use the NIST CSF 2.0 as the cybersecurity framework. Legal counsel should be consulted prior to adopting these or any policies required for compliance with federal and state regulations. There are no warranties or guarantees of any kind regarding the appropriateness, accuracy, or completeness of this sample standards manual.

Assumptions and Notes
1) FERPA and IDEA permit schools to maintain and freely publish a "Directory" which includes basic information including student name, address, photograph, sports participation, and certain other information. HIPAA similarly permits covered entities (e.g., hospitals) to publish directories using specific procedures. These policies do include any language regarding a Directory. Ohio law does not expressly authorize a Directory. We recommend that you consult legal counsel prior to publishing a Directory.
2) These policies assume that the Agency is not involved with any research or studies. FERPA and HIPAA both have special requirements regarding these.
3) These policies assume that the Agency will not be involved with deidentification of individually identifiable data. Both HIPAA and FERPA have requirements regarding deidentification.
4) These policies detail the most common requirements regarding uses and disclosures for legal proceedings. Note that not all circumstances are specified as there are unusual situations that most Agencies are unlikely to experience. Please consult legal counsel for unusual legal proceedings.

About the Board's employee group health plan
HIPAA regulates health plans, clearinghouses, health care providers, and "Business Associates". County boards, in executing their duties to ensure care for individuals with developmental disabilities, act at times as a health care provider, and at times as a health plan. This is all handled by this standards manual.

If the Board maintains a self-insured group health plan for its employees, the employee group health plan is a separate and distinct covered entity under HIPAA. Your self-insured group health plan may require its own HIPAA policies, which would require a different, shorter, specialized HIPAA manual. Contact Eagle Consulting and/or your County Prosecutor for assistance.

Change Log

Date	Standard	Description

Table of Contents

STANDARDS FOR ALL STAFF 6

1000 Privacy & Security Definitions 6

1010 Privacy and Security – General Rules 12

1020 Minimum Necessary 14

1030 Confidentiality Safeguards (Oral & Written) 16

1040 Speaking with the Family and Friends of an Individual Receiving Services 18

1050 Authorizations 19

1060 Verification 21

1070 Minors, Personal Representatives and Deceased Individuals 22

1080 Reporting Security Incidents and Violations 24

1090 Disclosures that do not Require an Authorization 25

1100 Acceptable Use of IT Assets 29

1150 Acceptable Use & Governance of Artificial Intelligence (AI) Tools 32

1110 Social Media Use 35

1120 Portable Computing Devices 37

1130 Employee Work at Home 39

INDIVIDUAL RIGHTS 40

2000 Individual's Right to Access Records 40

2010 Individual's Right to Request Amendment of Records 42

2020 Individual's Right to Receive an Accounting of Disclosures 44

2030 Individual's Right to Request Additional Restrictions 46

2040 Individual's Right to Request Confidential Communications 47

2050 Individual's Right to Notice of Privacy Practices 48

PERSONNEL SECURITY 49

3000 Onboarding and Offboarding – IT and Facility Access 49

3010 Access Control 50

3020 Staff Training 51

3030 Investigation and Response to Privacy/Security Violations 52

COMPLIANCE AND THIRD-PARTY MANAGEMENT 53

4000 Regulatory Compliance 53

4010 Data Governance 55
4020 Third Party Management 56
4030 Breach Reporting 57
4040 Mitigation 60
4050 Non-intimidation and Non-retaliation 61
4060 Privacy Complaints 62
COMPUTER SECURITY 63
5000 Security Program 63
5010 IT Asset Management and Data Flow Mapping 65
5020 Data Backup 66
5030 Disaster Recovery and Business Continuity Plans 67
5040 Security Incident Response 69
5050 Facility Security and Access Control 71
5060 Vulnerability Management and Evaluations 72
5070 Audit Control and Activity Review 73
5080 Malicious Software Protection 74
5090 Change Management 75
5100 Device and Media Management 76
5110 Encryption and Key Management 77
5120 User Account Management 79
5130 Privileged Account Management 81
5140 Control of Remote Access 83
5150 Technical Safeguards 84
5160 Technical Controls for Mobile Devices 86
5170 Electronic Signatures 87

STANDARDS FOR ALL STAFF

1000 Privacy & Security Definitions

STANDARD
The following definitions apply throughout these *Privacy and Security Standards*, for Standards numbered 1000 through 6000.

AUDIENCE
All Staff

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

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

iv) The extent to which the risk to the PHI has been mitigated.

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

    For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
13) **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.
14) **Disclosure –** Disclosure means the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the entity holding the information.
15) **DODD** – the Ohio Department of Developmental Disabilities
16) **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
17) **Education –** Education means activities associated with operating the school including instruction, IHP/IEP preparation, administration, behavioral intervention, extra-curricular activities, and other normal school functions. Education shall also include activities associated with early intervention programming.
18) **Education Records** –
    a) As defined in the FERPA regulations, means records that are:
        i) Directly related to a student; and
        ii) Maintained by an educational agency or institution or by a party acting for the agency or institution.
    b) The term does **not** include:
        i) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
        ii) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
        iii) Either of the following:
            (1) Records relating to an Individual who is employed by an educational agency or institution, that:
                (a) Are made and maintained in the normal course of business;
                (b) Relate exclusively to the Individual in that Individual's capacity as an employee; and
                (c) Are not available for use for any other purpose.
            (2) Records relating to an Individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(iii)(1) of this definition.
        iv) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
            (1) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or

paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
(2) Made, maintained, or used only in connection with treatment of the student; and
(3) Disclosed only to persons providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution.

v) Records created or received by an educational agency or institution after an Individual is no longer a student in attendance and that are not directly related to the Individual's attendance as a student.
vi) Grades on peer-graded papers before they are collected and recorded by a teacher.

19) **Employee –** Employee means any person employed by the Agency, volunteers, board members and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.
20) **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.
21) **Facility –** means the physical premises and the interior and exterior of a building(s).
22) **FERPA –** FERPA means the Family Educational Rights and Privacy Act, which are federal regulations that govern the privacy of records maintained by schools, as well as the rights of parents and students to access those records. These regulations are codified in CFR Title 34 Part 99.
23) **Guardian of the Person –** Guardian of the Person means a person appointed by the Probate Court to provide consent for and make decisions for the ward
24) **Health care –** means care, services, or supplies related to the health of an Individual. Health care includes, but is not limited to, the following:
    a) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and
    b) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
25) **Health Care Clearinghouse –** A Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system or community health information system that does either of the following functions:
    a) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
    b) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
26) **Health care operations –** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
    a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
    b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
    c) Except as prohibited under 45 CFR § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR § 164.514(g) are met, if applicable;
    d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
    e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f) Business management and general administrative activities of the entity, including, but not limited to:
   i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
   ii) Resolution of internal grievances;
   iii) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
   iv) Consistent with the applicable requirements of 45 CFR § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

27) **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.
28) **Health Plan –** Health plan means an individual or group plan that provides or pays the cost of medical care. A partial list of entities that are health plans (edited based on relevance to DD Boards) includes the following, singly or in combination:
   a) The Medicaid program under title XIX of the Act, 42 U.S.C. § 1396, et. seq.
   b) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.
   c) A group health plan, that is, an employee welfare benefit plan (as defined in section 3(1) of the Employment Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1), including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents, that:
      i) Has 50 or more participants; or
      ii) Is administered by an entity other than the employer that established and maintains the plan.
   d) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
29) **HIPAA –** HIPAA means the Health Insurance Portability and Accountability Act of 1996, cited in Pub.L. 104–191 and 110 Stat. 1936 and its regulations in 45 CFR Parts 160, 162 and 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.
30) **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.
31) **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.
32) **Individual, Individual receiving services or Individual served** – Means a person who has completed an eligibility determination, is receiving services, or who has received services from the Agency. Note that parents of minors, guardians and other "personal representatives" may exercise any right or privilege available to an Individual served.
33) **Individually Identifiable Health Information –** is information that is a subset of health information, including demographic information collected from an Individual, and:
   a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
   b) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
      i) That identifies the Individual; or
      ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.
34) **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.

35) **Integrity –** means the property that data or information have not been altered or destroyed in an unauthorized manner.
36) **Malicious software –** means software, for example, a virus, designed to damage or disrupt a system.
37) **May –** means the individual or entity is empowered, but not required, to perform the specified task.
38) **MOU –** MOU means a Memorandum of Understanding between governmental entities, which incorporates elements of a business associate contract in accordance with HIPAA rules.
39) **Must –** means the individual or entity is required to perform the following action. See also "Shall".
40) **Parent –** Parent means either parent. If the parents are separated or divorced, "parent" means the parent with legal custody of the child. "Parent" also includes a child's guardian, custodian, or parent surrogate. At age eighteen, the participant must act in his or her own behalf, unless he/she has a court-appointed guardian
41) **Password –** means confidential authentication information composed of a string of characters.
42) **Payment –** means, in the context of a County Board of DD:
    a) Both:
        i) Activities undertaken by the Agency to obtain reimbursement for services rendered, for example, from Medicaid for services provided to Individuals.
        ii) Activities undertaken by the Agency to provide reimbursement to contracted providers for services provided to Individuals served.
    b) The activities in paragraph (a) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:
        i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
        ii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
        iii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
        iv) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.
43) **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 JCBDD and the minor.
44) **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.
45) **Protected Health Information, or PHI** – means individually identifiable health information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Records of Individuals deceased for more than 50 years are not PHI. For the purposes of this manual, and the Agency's compliance program, PHI shall also include "Education Records" as defined by FERPA. This creates a consistent set of policies for both types of confidential information.
46) **Protected from Malicious Deletion --** means that one or more safeguards are in place to prevent deletion of the backup as part of a ransomware attack. Various technologies and strategies exist, including
    a) Isolation of backup, for example, by omitting a backup server from the domain or using a cloud backup service
    b) Rigorous access control and authentication, for example restricting access to the backup facility, omitting access credentials from password managers, and/or enabling MFA for the backup facility
    c) Backing up to removable media (e.g., magnetic tape) which is physically detached
    d) Saving the backup to unmodifiable media (e.g., Write-once, read-many (WORM))
    e) Cloud vendor anti-ransomware features which retain backups after deletion and permit recovery via an authenticated phone call
    f) Mandating dual authorization for configuration changes
47) **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.

48) **Psychotherapy Notes –** means notes recorded (in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
49) **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.
50) **Security or Security measures –** encompass all the administrative, physical, and technical safeguards in an information system.
51) **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.
52) **Shall –** means the individual or entity is required to perform the following action. See also "Must".
53) **Should** – means the individual or entity is recommended to perform the specified task, even though the task may not be required.
54) **Social Engineering –** means a hacker's use of psychological tricks on another person to obtain information he needs to gain access to a system or cause a person to perform an action. Common examples include tricking a person to reveal their password, tricking a person to click a malicious link in an email, or tricking a person to permit the hacker to enter a facility.
55) **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.
56) **System Owner** – means the individual in an organization with primary accountability for the use and operation of a software application. The specific duties of the System Owner may be defined in the organization's system and data governance standard.
57) **Technical safeguards –** means the technology, standards and procedures for its use that protect electronic protected health information and control access to it.
58) **Treatment –** means the provision, coordination, or management of services by the County Board or other provider to an Individual. This definition includes the coordination or management of support services; consultation between the County Board and support service provider relating to an Individual; or the referral of a Individual from one service provider to another.
59) **TPO –** TPO means treatment, payment, or health care operations under HIPAA rules. For the purposes of this standards manual, TPO shall also include "Education" as defined above.
60) **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.
61) **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.
62) **User –** means a person or entity with authorized access.
63) **Violation**, **or violate** – means, as the context may require, failure to comply with a provision of either the HIPAA Privacy or Security rules, or a provision of state law relating to privacy, confidentiality, or computer security.
64) **Workforce Member –** Workforce Member means the same as Employee. See definition above.
65) **Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

1010 Privacy and Security – General Rules

STANDARD
All information in an Individual's records is confidential. All conversations involving individually identifiable information are confidential.

The JCBDD shall conform to all requirements for privacy and confidentiality set forth by the State of Ohio, the federal HIPAA, FERPA and IDEA regulations, and any other applicable law. Safeguards will be implemented for the use, disclosure, collection, storage, retention, and destruction of individually identifiable information. The JCBDD shall not use or disclose individually identifiable information except in accordance with applicable requirements.

AUDIENCE
All Staff

AUTHORITY
45 CFR Part 160 and 45 CFR § 164 (current as/of 3/27/2013) Health Insurance Portability and Accountability Act Standards for Privacy of Individually Identifiable Health Information
45 CFR § 164.504(g) Health Insurance Portability and Accountability Act Standards for Privacy or Individually Identifiable Health Information -Uses and Disclosures: Organizational Requirements.
ORC § 5126.044 Ohio law on confidentiality (effective 9/22/2000)
OAC § 5123-04-01(O) County Boards of DD P&P required for HIPAA and FERPA compliance
45 CFR § 164.502(a)(1)(iii) incidental uses and disclosures
OAC § 5180-10-01Confidentiality (effective 7/1/2014), for EI/Pre-School/School Age; see also:
34 CFR 99 FERPA (current as of 1/2012)
34 CFR 300 and 301 Part B IDEA (Individuals with Disabilities Education Act, ages 3-21)
34 CFR 303 Part C IDEA (Individuals with Disabilities Education Act, ages 0-2)
34 CFR 303.402 - 416 Early Intervention Confidentiality and Family Rights Provisions
34 CFR 300.610 - 627 Children with Disabilities Confidentiality and Parent Rights Provisions

NOTE ON KEY LANGUAGE USED IN THESE STANDARDS AND PROCEDURES
These policies specify permitted behaviors, mandatory behaviors, and behaviors generally expected but not mandatory. The following terminology is used:

Term	Meaning
Shall, must, or will	The behavior is mandatory
Should	The behavior is usually expected, although not absolutely mandatory
May	An individual is permitted or empowered to take a specific action

PROCEDURES
1) Staff of the JCBDD may use or disclose PHI only as follows:
   a) For education, treatment, payment, and health care operations, including to contracted Business Associates. This information is to be used by employees who are official members of a habilitation/educational team, with the goal of serving the enrollee. Two exceptions:
      i) Explicit parent authorization is required for any Medicaid billing for children.
      ii) Explicit authorization is required to release information to another professional outside of the agency
   b) In accordance with a release or authorization of the Individual in accordance with the procedures set forth in Standard 1050 Authorizations.
   c) As permitted in Standard 1040 Speaking with the Family or Friends of an Individual Receiving Services.
   d) As permitted in Standard 1090 Disclosures that do Not Require an Authorization.
   e) To the Individual served.
2) For all the above, the minimum amount of information shall be disclosed, and specific procedures followed as detailed in 1020 Minimum Necessary.
3) All employees are responsible for safeguarding the information regarding the Individuals we serve, as detailed in

a) Standard 1030 Confidentiality Safeguards (Oral & Written)
b) Standard 1100 Acceptable Use of IT Assets
c) Standard 1110 Social Media Use
d) Standard 1120 Portable Computing Devices
e) Standard 1130 Employee Work at Alternative Locations

4) Rights of Individuals served by JCBDD may be exercised by parents, guardians and personal representatives as detailed in Standard 1070 Minors, Personal Representatives and Deceased Individuals.
5) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in Standard 1080 Reporting Violations and Security Incidents.
6) Supervisors, managers, and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.

1020 Minimum Necessary

STANDARD
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. All employees shall follow those protocols. The Privacy Officer is accountable to ensure implementation of this standard.

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.502(b)(1) Uses and Disclosures-Minimum Necessary Standard
34 CFR 300.623(d) IDEA Part B
34 CFR 303.415(d) IDEA Part C
34 CFR 99.31(a)(1)(i)(A) FERPA
OAC 3301-51-04(N)(4) OAC Confidentiality Safeguards

PROCEDURES
1) **FOR ALL EMPLOYEES**
   a) **Minimum Necessary Requirement**.
      i) **Basic Requirement**. When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, employees must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
      ii) **Exceptions**. The minimum necessary requirement does NOT apply to:
         (1) Disclosures to or requests by a health care provider for treatment
         (2) Uses or disclosures made to the Individual served and/or the guardian of the Individual, including but not limited to any requests for their records or requests for an accounting of disclosure
         (3) Uses of disclosures made pursuant to an Authorization
         (4) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations
   b) **Routine Requests or Disclosures.** Staff shall be familiar with and follow procedures detailed in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests when making requests for PHI or disclosures.
   c) **Procedures for Non-Routine Disclosures or Requests**
      i) **For non-routine disclosures**, when subject to the minimum necessary provision, the person making the disclosure will apply the minimum necessary principle. He or she may seek the guidance, if necessary, of the Privacy Officer (or his/her designee).
      ii) **For non-routine requests**, the requesting party will utilize the minimum necessary principle, seeking the guidance, if necessary, of the Privacy Officer (or his/her designee).
      iii) **Good Faith Reliance** – JCBDD staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:
         (1) The disclosure is made to a **public official**, permitted to receive information, and the public official represents that the request is for the minimum necessary information;
         (2) The request is from another **covered entity**;
         (3) The request is from a **professional** at JCBDD, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary information.
2) **FOR THE PRIVACY OFFICER**
   a) **Accountability.** The Privacy Officer is accountable for implementation of appropriate authorization and access control procedures, creation of procedures for routine requests and disclosures, and other implementation of the minimum necessary principle.
   b) **Authorization and Access Control**: Authorization to access a computing resource and specific PHI is granted to a user by an agency department head and/or System Owner based on the user's role and duties. JCBDD will identify:
      i) Those persons or classes of persons, who require access to PHI to carry out their duties, in the workforce, including interns and trainees, will be listed according to job classification with the

minimal necessary PHI required for successful job performance to serve the Individuals, and

ii) For each such person or class of persons, the category, or categories of PHI to which access is needed and any conditions appropriate to such access.

iii) Safeguards will be developed and documented to restrict workforce access to the minimum necessary, especially as detailed in Standard 5050 Facility Security and Access Control.

iv) The Privacy Officer shall ensure documentation of the results of this analysis in Appendix E – Minimum Necessary – Workforce, Disclosures and Requests. This report will be available for public inspection.

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

1030 Confidentiality Safeguards (Oral & Written)

STANDARD
JCBDD shall utilize appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.530(c) – Administrative, Technical, and Physical Safeguards
34 CFR 99.31(a)(1)(ii) Safeguards
ORC § 5126.044 Ohio law on confidentiality
OAC § 5180-10 (F) Confidentiality (effective 7/1/2014), for EI/Pre-School/School Age for EI/Pre-School/School Age

PROCEDURES

1) **General Procedures**
   a) Visitors shall be required to sign in and wear a visitor badge while on the premises of a JCBDD facility or be escorted by FCBDD staff.
   b) Employees shall be familiar with any additional visitor control procedures for their building and enforce them when appropriate.
2) **Oral Privacy**
   a) Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings and using appropriate volume when speaking to prevent others from overhearing conversations.
   b) Employees should refrain from holding conversations in common areas where Individuals receiving services or visitors can overhear PHI.
   c) Discussions concerning Individuals should be done in a private area and discussions must be limited to "need to know" information for purposes of providing the best services.
   d) Overheard conversations are not to be shared or repeated.
   e) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.
3) **Safeguards for Written PHI**
   a) **Control of any Original Paper Records**
      i) Case and School records shall be kept locked and secured. Employees requiring access to these records shall have a key and/or combination for the storage room or cabinet.
      ii) Paper files shall be put away promptly when not being used.
      iii) Original paper records shall not be removed from the building without the authorization of the Superintendent, Privacy Officer, or designee.
      iv) Individual records shall be retained per Policy 8.02 Records Retention Schedule.
   b) **Other use and storage of paper records**
      i) Employees shall minimize the use of hardcopy PHI.
      ii) Personal appointment books with names of Individuals being served should be safeguarded while away from the office. It is best to avoid putting last names in appointment books if possible.
      iii) Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer.
   c) **Faxing Procedure**
      i) When faxing a document with PHI, use a cover sheet which indicates that information is confidential, protected under state and federal laws, and not to be re-disclosed.
      ii) Care shall be taken to address and transmit fax to the proper recipient.
      iii) Faxed documents should not be left at a common fax machine.
   d) **Printing and Copying PHI**
      i) Printers and copiers used for printing of PHI shall be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
      ii) PHI printed to a shared printer should be promptly removed.
      iii) The Security Officer shall monitor all printer and photocopier acquisitions. Any equipment which includes internal storage devices and retains images of photocopies made shall be managed by the IT department who shall ensure destruction of any PHI upon decommissioning of the device.

e) **Transportation/outside use of documents with PHI**
    i) Caseworkers and other employees who remove documents from the facility are responsible for safeguarding these documents.
    ii) When leaving documents unattended in a personal vehicle, the vehicle shall be locked. Preferably, the documents and/or their container shall not be visible.
    iii) If any documents with PHI are lost or stolen, the incident shall be immediately reported to a supervisor and the HIPAA Privacy Officer.
f) **Visibility of records and other PHI**. All employees using records for Individuals and other paperwork with PHI shall arrange these items so that PHI is not readily visible to unauthorized persons, especially in high traffic areas such as reception area.
g) **Shredding**. Unneeded paper documents containing PHI shall be destroyed by shredding
h) **Destruction of PHI in non-paper formats**. Any written PHI in non-paper formats, such as imprints on carbon films used in fax machines, shall be destroyed appropriately.
i) **Clean Desk.** All employees should clean their desks of PHI whenever leaving their work area for a time, especially at end-of-day.
j) **Confidentiality with Cleaning Personnel**. Cleaning personnel with access to the facility shall be placed under a confidentiality agreement.

4) **Compliance Audits/Facility Review**. Annually or on another periodic basis, the HIPAA Privacy Officer or designee may audit staff compliance with these guidelines. Any required corrective action shall be taken.
5) **Enforcement**. All supervisors are responsible for enforcing this standard. Employees who violate this standard will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

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

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

AUDIENCE
All Staff

AUTHORITY
45 CFR § 164.510(b)
45 CFR § 164.510(b) Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object-Involvement in the Individual's Care and Notification Purposes

PROCEDURES
1) **If the Individual is present**
   a) **Permitted disclosure to family or friend present**. If a family member, or friend of the Individual is present while services are being rendered, an employee serving the Individual may disclose PHI after one of the following:
      i) verbally seeking permission for the disclosure, and the Individual agrees; or
      ii) giving the Individual the opportunity to object to the disclosure, and the Individual does not express an objection; or
      iii) the staff member reasonably infers from the circumstances, based on the exercise of professional judgment, that the Individual does not object to the disclosure.
2) **If the Individual is not present**
   a) **Communications about the Individual's care**
      i) During a phone call or other discussion with a family member or one involved with the care of the Individual being served by JCBDD, where the Individual is not present, the employee may use their professional judgment to determine if the disclosure is in the best interests of the Individual and, if so, may disclose only the PHI that is directly relevant to the person's involvement with the Individual's care.
   b) **Notifications**
      i) An employee may disclose PHI to notify a family member, a personal representative of the Individual, or another person responsible for the care of the Individual of the Individual's location or general condition.

1050 Authorizations

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

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.508 – Uses and Disclosures for which an Authorization is Required
ORC § 3701.243 – Disclosing of HIV Test Results or Diagnosis
ORC § 5126.044 – Ohio Statute on Confidentiality of Records
OAC § 5123-4-01(O) – Administration and Operation of County Boards of Developmental Disabilities-Records
OAC 5123-3 Licensed Residential Facilities
OAC 5160-1-32 Medicaid: Safeguarding and Releasing of Information
OAC § 3301-51-04(E) and (M) – Confidentiality for EI/School Age: Records of Disclosures, Consent; see also:
34 CFR 99.30 – FERPA Requirements for Prior Consents to Disclose Information
34 CFR 99.32 – FERPA Recordkeeping Requirements Concerning Requests and Disclosures
34 CFR 303.414 Consent Prior to Disclosure or Use (IDEA Part C, Early Intervention)
34 CFR 300.622 Consent (IDEA Part B, School Age)
42 CFR Part 2 – Confidentiality of Records from Federally-funded Drug and Alcohol Abuse Treatment Centers
42 CFR Part 483, Subpart I – Conditions of Participation for Intermediate Care Facilities for Individuals with Intellectual Disabilities

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

PROCEDURES
1) **Valid Authorization**. Unless otherwise authorized by JCBDD standard and/or state or federal law, release of an Individual's records requires specific authorization by the Individual being served or his/her legal representative. A standard authorization form is included as an Appendix. For authorizations received on other forms, the following elements must be included to be valid:
   a) Full Name of the Individual.
   b) A specific description of the information to be released. For example, a range of dates, or category of record.
   c) The purpose or need for the disclosure.
   d) The name of the person or agency disclosing the information.
   e) Names of the person(s), or agency to whom the disclosure is to be made.
   f) The date, event, or condition upon which the authorization expires.
   g) Statement of the Individual's right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke.
   h) Statement that JCBDD may not condition treatment on whether the Individual signs the authorization.
   i) A statement informing the Individual of the potential that information disclosed could be redisclosed if the recipient is not subject to federal or state confidentiality restrictions.
   j) Signature and date of the Individual, guardian or personal representative.
   k) If the authorization is signed by a guardian or personal representative, a description of that person's relationship to the Individual and authority to sign the authorization.
   l) Written in plain language.
2) **Invalid Authorization.** A PHI authorization is considered invalid if the authorization has the following defects:

a) Authorization is incomplete.
b) Authorization is not dated, or time has elapsed.
c) Authorization does not contain required elements as explained above.
d) JCBDD is aware the authorization has been revoked.
e) JCBDD is aware the information is false.
f) The authorization to release PHI is combined with other documents.

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

1060 Verification

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

AUDIENCE
All Staff

AUTHORITY
34 CFR 99.31(c) Under What Conditions Prior Consent is Not Required to Disclose Information-Verification
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.514(h) Other Requirements Relating to Uses and Disclosures of Protected Health Information-Verification

PROCEDURES

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

2) **REQUESTS FROM AN INDIVIDUAL RECEIVING SERVICES, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE**
   a) A properly completed, valid Authorization per the specifications in Standard 1050 Authorizations is sufficient verification of the identity and authority of the person requesting information.
   b) For requests for information other than formal record releases, staff must first verify both the identity and the authority of the person prior to releasing PHI:
      i) If the person is known to the staff person, this is sufficient verification of identity.
      ii) Identity can be verified by questioning the person regarding their knowledge of information in the record of the Individual being served, such as birth date, social security number, etc., which only an authorized person would typically know.
      iii) For requests from someone other than the Individual or the parent of a minor, the person's authority to obtain information must also be verified. For example, a healthcare Power of Attorney and/or statement from the Individual that the requestor is a HIPAA Personal Representative would demonstrate proper authority. See also Standard 1040 Speaking with Family and Friends of an Individual Receiving Services for situations where it may be permissible to give information to a family member.

1070 Minors, Personal Representatives and Deceased Individuals

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

AUTHORITY
ORC 5126.044 Confidentiality
ORC 3319.321(4) Confidentiality and Parental Rights of Access to Student Records
ORC 3109.051(H) Parenting Time – Companionship or Visitation Rights
ORC 1337.13 Authority of Attorney In Fact Under a Durable Power of Attorney for Health Care
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.502(g)(1) Uses and Disclosures of Protected Health Information -Personal Representatives
45 CFR § 164.502(g)(2) Uses and Disclosures of Protected Health Information -Adults and Emancipated Minors
45 CFR § 164.502(g)(3) Uses and Disclosures of Protected Health Information -Unemancipated Minors
45 CFR § 164.502(f) Uses and Disclosures of Protected Health Information -Deceased Individuals
45 CFR § 164.510(b)(5) Uses and Disclosures Requiring and Individual to Agree or Object –Uses and Disclosures When the Individual is Deceased

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

PROCEDURES
1) **Rights of legally Consenting Minors**. Individuals being served, who are minors, and who are legally allowed to consent to treatment under Ohio Law may exercise all rights regarding access to, requests for amendment to, and release of their PHI pursuant to a written authorization.
2) **Rights of an Individual's Personal Representative**. JCBDD recognizes an Individual's personal representative as a person authorized to exercise rights of access and/or inspection of PHI, rights to request amendment of PHI, and the right to sign the JCBDD Authorization Form which permits release of PHI.
3) **Recognized Personal Representative**. JCBDD recognizes the following persons to be personal representatives:
   a) The parent of a child younger than 18 years old
   b) The non-custodial parent of a child younger than 18 years old (ORC 3319.321 and ORC 3109.051(H), unless the custodial parent presents JCBDD a court order restricting the non-custodial parent's access. In the event that JCBDD is presented with such a court order, JCBDD shall adhere to the terms of that order.
   c) A person who is recognized through durable power of attorney to have authority to act on the behalf of the Individual (ORC § 1337.13)
   d) The legal guardian of the Individual
   e) Any other person authorized by law except in Abuse, Neglect, and/or Endangerment situations, or where JCBDD has received a court order or other documentation limiting privileges of a non-custodial parent as provided below.
      i) Abuse, Neglect, and/or Endangerment Situations. Notwithstanding a state law of any requirement of this paragraph to the contrary, JCBDD may elect not to recognize a person as a personal representative of an Individual. In order for JCBDD to choose not to recognize a person as a personal representative, JCBDD must decide that it is not in the best interest of the Individual to treat the person as the Individual's personal representative and must believe that one of the following conditions exist:
         (1) The Individual has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative.
         (2) Treating such person as the personal representative could endanger the Individual.

4) **Receipt of a court order limiting the privileges of a non-custodial parent**. If JCBDD receives from the custodial parent a court order limiting the privileges of the non-custodial parent to act in the capacity of the child's personal representative, JCBDD shall adhere to the restrictions in the court order.
5) **Deceased Individuals**
   a) **Disclosure of PHI After Death**. PHI generated during the life of an Individual is protected from disclosure after death unless disclosure is for treatment or payment, quality assurance or other auditing or program review functions. JCBDD and its employees cannot release PHI regarding a deceased Individual unless a valid personal representative has been established and has requested the PHI through the proper authorization process.
   b) **Disclosure of PHI to Administer Estate**. Upon request, PHI shall be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate (ORC § 5126.044).
   c) **Disclosure to Guardian or next-of-kin:** Upon request, the board may release records regarding an Individual served to the guardian at time of death pursuant to ORC § 5126.044. Absent a guardian, records may be released to the next of kin in order of priority, pursuant to ORC § 5126.044:
      i) The Individual's Spouse (if married)
      ii) The Individual's children
      iii) The Individual's parents
      iv) The Individual's brothers or sisters
      v) The Individual's uncles or aunts;
      vi) The Individual's closest relative by blood or adoption
      vii) The Individual's closest relative by marriage

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

1080 Reporting Security Incidents and Violations

STANDARD
Security Incidents, including any suspected or potential security incidents, must be reported immediately. Additionally, any violations of these privacy and security standards must be reported.

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

PROCEDURES
SECURITY INCIDENT REPORTING
1) Any employee who learns of a security incident or potential security incident must report it immediately by contacting the IT administrator and their immediate supervisor. Examples of common security incidents are:
   a) Compromised accounts: Stolen or cracked passwords, or if you believe your accounts have been compromised in any way.
   b) Malware and viruses: Ransomware infections, or if you think you may have accidentally installed malware.
   c) Lost or stolen devices: Computers, laptops, or mobile devices.
   d) Data breaches: Unauthorized access or distribution of confidential information, or a data breach compromising a large amount of personal data.
   e) Unauthorized access: Any unauthorized access to systems, software, or data, or unauthorized use of computing resources.
   f) Suspicious activity: Any unusual or suspicious activity, such as phishing attempts or if you notice changes you didn't make to your systems.
   g) System intrusion: Any hacking, cracking, or tampering with computer systems.
   h) Denial-of-service attacks: Attacks that disrupt the availability of services.
   i) Phishing: If you think you may have fallen for a phishing scam or shared sensitive information to an unintended recipient.
   j) Illegal acts: Using computing facilities to commit illegal acts.
2) The security incident response team will respond per the procedures specified in Standard 5040 Security Incident Response.

VIOLATION REPORTING
3) **Violations**. Any employee observing a violation of any of the *Privacy and Security Standards* is to report the violation. The HIPAA Privacy Officer shall educate employees regarding the reporting procedure.

1090 Disclosures that do not Require an Authorization

STANDARD
JCBDD employees may use and disclose PHI, without an Individual's authorization, when permitted and/or required by state or federal statute. Staff will carefully follow specific requirements for these unusual and infrequent disclosures.

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.512 Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required
34 CFR 99.31 Conditions Prior Authorization is Not Required
34 CFR 99.36 Conditions for Disclosures of Information in Health and Safety Emergency
OAC § 3301-51-04 Confidentiality (in Education of Students with Special Needs, effective 7/1/2014)
OAC § 3301-51-04 (E) Record of Access
OAC § 3301-51-04 (Q) Disciplinary Information
ORC § 2151.421(A) Reporting Child Abuse or Neglect
ORC § 2305.51 Mental Health Professional or Organization Not Liable for Violent Behavior by Client or Patient-Disclosures to prevent harm to 3rd parties
ORC § 2317.02(B) Uniform Fiduciary Access to Digital Assets Act-Applicability/Privilege for Physicians, School Guidance Counselors, Licensed Social Workers and Licensed Counselors
ORC § 4732.19 Psychologist-Client Privilege
ORC § 5123.19 Operation of Residential Facilities
ORC § 5123.60 Ohio Protection and Advocacy System
ORC § 5123.61Reporting Abuse, Neglect, and other Major Unusual Incidents-
ORC § 5123.61(C)(1) Duty to Report
ORC § 5126.044 Confidentiality
ORC § 5126.055 Services Provided by Board that has Medicaid Local Administrative Authority
ORC § 5126.31 Reviewing Reports of Abuse Neglect
OAC § 5123-17-02(B) Addressing Major Unusual Incidents and Unusual Incidents to Ensure Health, Welfare, and Continuous Quality Improvement - Scope
Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena
ORC § 4113.52 Reporting Violations of Law by Employer or Fellow Employee
34 CFR Part 99 Subpart D Family Educational Rights and Privacy-May an Educational Agency Disclose Personally Identifiable Information from Education Records
20 U.S.C. 7917 No Child Left Behind Act – Transfer of Disciplinary Records

LEGAL NOTES
- ORC § 5126.044 does not authorize any of the excepted disclosures detailed in HIPAA and FERPA. Other Ohio regulations reference disclosures otherwise allowed by federal and state law. HIPAA preempts contrary state law, except where state law offers greater privacy protections, greater rights of access to an Individual's records, or is less coercive. Consult your county prosecutor for review and approval of this standard.
- HIPAA and FERPA/IDEA maintain overlapping but different lists of disclosures permitted without authorization or parental consent. We use the term "Education Records" below to refer to FERPA/IDEA permitted disclosures, and "PHI" regarding HIPAA permitted disclosures.

PROCEDURES
JCBDD employees will follow the indicated procedures for the various special circumstances detailed below:
1) **Recordkeeping**. For all of the disclosures authorized below, the employee handling the disclosure will maintain a record of the disclosure in the adult or school record [45 CFR 164.528, OAC 3301-51-04(E)]. Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.
2) **When required by law**
   a) To officials at another school that an Individual served by the Agency intends to enroll in, or is already enrolled in, for the purposes of Individual's enrollment or transfer. Any such disclosures must include records of any disciplinary actions, particularly the circumstances that resulted in the disciplinary action and relevant information to the safety of the child and others. A description of the disciplinary action taken

must be included if the disciplinary action was taken because the child possessed a weapon on premises, knowingly possessed controlled substances on premises, or inflicted serious bodily to another on premises. [OAC 3301-51-04(Q) Disciplinary Information]

b) The JCBDD may use or disclose PHI or Education Records to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

c) For compliance with mandatory disclosures related to sex offenders

3) **For public health purposes** PHI may be used or disclosed to:

a) A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions.

b) A public health or other government authority authorized by law to receive reports of child abuse or neglect.

c) A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance.

d) A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.

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

a) **Reports of child abuse**

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

ii) The JCBDD may disclose PHI related to the report of abuse to the extent required by applicable law. Such reports shall be made to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

b) **Reports of abuse and neglect other than reports of child abuse or neglect.**

i) The JCBDD may disclose PHI about an Individual believed to be a victim of abuse, neglect, or domestic violence to a governmental authority authorized to receive such reports if:

(1) the Individual agrees; or

(2) the JCBDD believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm.

If the Individual lacks the capacity to agree, disclosure may be made if not intended for use against the Individual and delaying disclosure would materially hinder law enforcement activity.

ii) The JCBDD staff member making the disclosure must promptly inform the Individual whose PHI has been released unless:

(1) doing so would place the Individual at risk of serious harm; or

(2) the JCBDD would be informing a personal representative, and the JCBDD reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the Individual as determined by the JCBDD, in the exercise of professional judgment.

5) **For health or education oversight activities such as investigations, audits, and inspections**

a) PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.

b) Specifically excluded from this category are investigations of an Individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

c) PHI may be used and disclosed to receive and review reports of incidents, and to conduct investigations as authorized by ORC 5126.055(A)(6), 5126.31, 5126.311, 5126.34 and 5126.313.

d) Education Records may be disclosed to the Comptroller General of the US, Attorney General of the US, Secretary of Education and/or State of Ohio Education authorities subject to the requirements of 34 CFR 99.35 or to state officials involved with juvenile justice in accordance with 34 CFR 99.38.

6) **To accrediting organizations**

a) Information in Education Records may be disclosed to accrediting organizations without parental consent. For any disclosure of PHI, a HIPAA Business Associate Agreement should be in place with the accrediting organization.

7) **For judicial and administrative proceedings**
NOTE: These policies do not detail all situations such as grand juries and other infrequent legal proceedings. Consult with legal counsel prior to disclosure for any unusual situations!
HIPAA-specific provisions: The following provisions apply for records of adult (over 18) services:
   a) The JCBDD must always comply with a **court order** but only in accordance with the express terms of the order.
   b) For a **subpoena, discovery request** or **other lawful process**: the JCBDD may comply with such legal requests only if:
      i) The JCBDD receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the Individual who is the subject of the requested PHI has been given notice of the request; or
      ii) The JCBDD receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.

   The JCBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements of HIPAA, FERPA, IDEA and/or OAC 3301-51-04.
8) **For law enforcement purposes**
   a) **Conditions Allowing for Disclosure of PHI to Law Enforcement**. PHI may be disclosed for the following law enforcement purposes and under the specified conditions:
      i) Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; or commission of a felony, subject to any exceptions set forth in applicable law.
      ii) Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.
      iii) The JCBDD may disclose to a law enforcement official protected health information that the JCBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the JCBDD.
   b) **Reporting Commission and Nature of Crime.** HIPAA and Ohio Regulations for School-Age differ in their specifications.
      i) **HIPAA specifications for reporting of crimes:** PHI may be disclosed to law enforcement personnel to report the commission and nature of a crime; The location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime. When responding to requests about the location of a suspect, fugitive, material witness, or missing person, the following PHI may be released:
         (1) Name and address
         (2) Date and place of birth
         (3) Social security number
         (4) ABO blood type and RH factor
         (5) Type of injury
         (6) Date and time of treatment
         (7) Date and time of death, if applicable,
         (8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos
      ii) FERPA / IDEA Part B / OAC 3301-51-04 specifications for reporting of crimes: DD boards may report crimes committed by school-age individuals served. See FERPA99.8(c)(1) and OAC 3301-51-04(R).
   c) **Compliance/Enforcement of privacy regulations**: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.
9) **To coroners, medical examiners, and funeral directors**
   a) PHI may be disclosed to coroners, medical examiners, and funeral directors, as necessary for carrying out their duties.
10) **Organ, eye, or tissue donation**
   a) PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.
11) **To reduce or prevent a serious threat to public health and safety and/or safety of person(s)**
   a) The JCBDD may disclose PHI or Education Records as follows, to the extent permitted by applicable law and ethical standards:

i) **Good Faith.** PHI may be used or disclosed if the entity believes in good faith:
   (1) that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat; or
   (2) the disclosure is to law enforcement authorities to identify or apprehend an Individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.

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

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

12) **Specialized government functions**

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

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

c) **Correctional Institution or Law Enforcement Official.** The JCBDD may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other Individual protected health information about such inmate or Individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:
   i) The provision of health care to such Individuals;
   ii) The health and safety of such Individual or other inmates;
   iii) The health and safety of the officers or employees of or others at the correctional institution;
   iv) The health and safety of such persons and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
   v) Law enforcement on the premises of the correctional institution; and
   vi) The administration and maintenance of the safety, security, and good order of the correctional institution.

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

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

13) **In connection with "whistleblowing"**. In connection with "whistleblowing", or reporting of a violation of law or ethics, an employee of JCBDD may disclose PHI to his/her attorney, and to other parties specified in Ohio Revised Code § 4113.52, while following the procedures outlined in that statute. See also Policy 1.15 Whistleblower & Reporting.

14) **For workers' compensation or other similar programs if applicable**.

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

1100 Acceptable Use of IT Assets

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

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(b) Workstation Use
45 CFR § 164.310(c) Workstation Security
45 CFR § 164.308(a)(5) Log in Monitoring
NIST CSF PR.PS-05

PROCEDURES

1) **WORKSTATION USE**
   a) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the Individuals served: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related.
   b) **Personal Use of Computer Workstation, Including Internet Use**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use. "Limited use" is not easily defined so employees should contact their supervisors for clarification. In general, "limited use" means:
      i) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
      ii) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.
      iii) Workstations must never be used for any activity that would be embarrassing to the Agency if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
         (1) downloading or viewing pornographic, racist, profane, or otherwise objectionable material
         (2) conducting conversations of a sexual nature of relating to an illicit affair
         (3) relating to any illegal activity
         (4) political activity
         (5) operating a business
         If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.
      iv) Personal use of social media, such as Facebook, Twitter, LinkedIn and others is detailed separately.
      v) Employees are prohibited from checking social media and their personal email except during their own time.
      vi) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the Agency.
   c) **E-Mail Use**. Employees with Agency e-mail accounts should check e-mail daily. Agency E-mail accounts are to be used for Agency purposes only. E-mail should be written in a professional manner and should be courteous and respectful. Other policies when using e-mail:
      i) Use of unencrypted email to transmit any PHI is prohibited except in the limited case specified in the HIPAA regulations and outlined in Standard 2000 Individual's Right of Access to Records, when an individual or guardian requests that an electronic copy of their record be sent via email.
      ii) Email sent from one employee to another employee (i.e. the email is transmitted entirely within the agency's email system) is encrypted and may be used to transmit PHI.
      iii) Employees must consult with the HIPAA Security Officer regarding any other agency-approved tools to send encrypted email.

iv) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in [*INSERT REFERENCE TO PUBLIC RECORDS POLICY].
v) For personal matters, employees must use a personal account such as Gmail or Yahoo mail, on a personally owned device:
(1) In the event that any Agency e-mail is received on a personal account, the employee must forward the email to the employee's Agency account so that it is entered into the public record.
(2) In the event that a personal email is received on an Agency account, redirect the discussion to a personal email account.

d) **Data Storage on Network Only**. All data must be stored on the network, not on a workstation hard drive. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate shared or end-user private folder on an agency server. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions. DATA STORED ON WORKSTATION HARD DRIVES IS NOT BACKED UP AND MIGHT BE DELETED WITHOUT NOTICE.

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

f) **Phishing and other suspicious emails**. Any employee who receives a suspected phishing email and/or other suspicious email must report it using the agency-specified procedure.

g) **Security incident reporting.** Any employee who opens a potentially malicious attachment or link, suspects a hacking incident, experiences loss or theft of a mobile device, notices any unusual computer behavior, or commits/observes a violation of any computer security policy or standard must report the incident to the HIPAA Security Officer and/or his/her designee or help desk immediately.

h) **All Usage is Logged**. THE AGENCY MONITORS ALL USAGE OF AGENCY WORKSTATIONS BY LOGGING ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY, INCLUDING ANY PERSONAL USE OF AGENCY COMPUTERS. All logs of employee activity are property of the Agency and may subject to public disclosure.

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

j) **Agency-approved apps and cloud services only.** Employees must use only agency-approved applications (apps) on workstations, smartphones/tablets and/or cloud services for any function involving PHI or other confidential information. The use of any non-authorized software, apps or cloud services with PHI is expressly prohibited.

k) **Agency-approved hardware only**. Only Agency-approved and Agency-installed hardware may be utilized. No smart speakers (e.g., Alexa), video cameras, smart TVs, video cameras, other Internet-of-Things (IotT) devices, wireless networking equipment, smartphones, or other hardware or software may be installed or used without permission of the systems department.

l) **Electronic signatures**. Employees using software that includes Agency-approved electronic signature capabilities shall follow all procedures specified in Standard 5170 Electronic Signatures.

2) **WORKSTATION SECURITY**

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

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

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

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

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

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

3) **USER IDs and PASSWORDS**
   a) Each employee is assigned a unique User ID(s) for agency systems. Employees must only use their User ID to access Agency systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential and not shared with anyone else. If an employee reveals a password, or if becomes known to someone else, that employee must change the password.
   b) Password length – passwords must be a minimum of 6 (six) characters for handheld devices and 12 (twelve) for cloud systems and network-connected devices.
   c) Password complexity. Passwords must include upper-case and lower-case letters, and digits. Passwords may also include special characters. Longer "passphrases" of 20+ characters are recommended (a passphrase is a sequence of 3 or more words).
   d) Not guessable. The password must not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.
   e) Mandatory periodic password changes shall not be required. Mandatory changes shall be required for all users if there is evidence or suspicion of compromise.
   f) When changing passwords, previously used passwords must not be recycled.
   g) Different passwords must be used for each account.
   h) When specifying answers to vendor security questions (for use with password reset requests) it is best to select questions whose answers cannot be easily discovered.
   i) In general, passwords should be memorized and not written. Any written reminder should not be maintained near the workstation.
   j) Passwords should be changed only if there is evidence or suspicion of compromise.
   k) Two-factor authorization and/or Single Sign-On technology should be used, if available.
   l) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

1150 Acceptable Use & Governance of Artificial Intelligence (AI) Tools

STANDARD
Each staff member is responsible for understanding and following this standard regarding the appropriate use of AI tools when performing their job duties.

SCOPE AND PURPOSE
This standard establishes guidelines for the responsible use of Artificial Intelligence (AI) tools by staff. For the purposes of this standard, "AI tools" include computer programs or features that can generate content, provide recommendations, or analyze information in a way that appears similar to human thinking. Examples include tools that summarize text, generate emails or reports, answer questions, or assist with scheduling or documentation. (See definitions below.)

This standard is intended to guide staff to use AI tools while addressing **security** (protecting systems and data), **privacy** (permissible uses and disclosures of information) and **quality** of agency work. AI use is subject to the agency's: (1) HIPAA Security and State law cybersecurity requirements; (2) permitted uses/disclosures under HIPAA/FERPA/IDEA or other law; and (3) records management, retention, and public records requirements.

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR §§ 164.308, 164.310, 164.312
FERPA (20 U.S.C. § 1232g; 34 CFR Part 99)
IDEA (20 U.S.C. § 1400 et seq.)
Ohio Revised Code § 9.64 Political Subdivision Cybersecurity

DEFINITIONS
Generative AI – Systems that create new content (e.g., text, images, audio, or code) based on training data and prompts (ChatGPT, Microsoft Copilot).
Predictive AI – Models that forecast outcomes or trends using historical data (e.g., risk scoring, demand forecasting) (FICO Analytics, Amazon Forecast).
Conversational AI – Chatbots or virtual assistants that interact with users through natural language (e.g., ChatGPT, Copilot, Alexa).
Agentic AI – Artificial intelligence systems capable of operating with a degree of autonomy to pursue goals, make decisions, or take actions without direct human prompting. These systems can plan, reason, and interact with digital or physical environments, often combining generative, predictive, and reinforcement-learning capabilities (e.g. Salesforce AgentForce).
Machine Learning (ML) – Algorithms that learn from data and improve performance over time without explicit programming.
Deep Learning – A subset of ML using neural networks to process complex data such as images, speech, and natural language.
Natural Language Processing (NLP) – AI that understands, interprets, or generates human language.

ROLES & RESPONSIBILITIES
1) **All Staff:** Follow approved tool list, keep human-in-the-loop, and protect data per this standard.
2) **HIPAA Privacy Officer:** Performs Privacy risk assessments, interprets permitted uses/disclosures, minimum necessary, de-identification, redisclosure, and recordkeeping, negotiates HIPAA Business Associate Agreements.
3) **HIPAA Security Officer / IT:** Performs security risk assessments, vendor due diligence, BAA/contract gating, app-consent controls, and monitoring.
4) **Superintendent or Designee:** Approves adoption of AI tools and publishes the Approved AI Tools Register.

PROCEDURES

1) **USE OF AI TOOLS FOR JOB DUTIES ONLY**
   a) **Only Approved AI Tools May be used.** Staff may use only AI tools listed on the agency's Approved AI Tool Register.
   b) Use Only for Approved Purposes. Staff may use AI tools only when necessary to complete work-related responsibilities. This includes drafting content, assisting with decision making, summarizing documentation, performing administrative tasks, and other functions.
   c) **Human Oversight Required.** Any content generated with the assistance of AI must be reviewed and approved by the staff member before use or distribution. The individual staff person using AI is responsible for the accuracy and quality of any AI-assisted output.
   d) **No Automated Eligibility/Service Decisions.** AI outputs must not be used as the sole basis for decisions about services, placement, benefits, or discipline.
   e) **Material Contribution Disclosure.** If AI materially contributes to content (beyond spelling/grammar), follow section 4 below.
   f) **Retention & Public Records.** Staff must be aware that AI-generated content becomes part of official records, is subject to agency retention schedules and may be discoverable under public records laws.
2) **PROTECTION OF CONFIDENTIAL INFORMATION**
   a) **No Entry of PHI, PII, or Confidential Data** into any AI tool unless it is on the agency's Approved AI Tool Register and approved for use with PHI, PII and/or Confidential data.
3) **LIMITATIONS ON USE**
   a) **Personal Use Prohibited.** Staff may not use AI tools for any personal purposes using agency devices, systems, or accounts. All use of AI must directly support the employee's job duties and reflect the agency's mission and values.
   b) **Prohibited Uses.** AI tools must not be used to:
      i) Generate false or misleading information.
      ii) Simulate employee identity (e.g., deepfakes, fake emails).
      iii) Bypass agency security protections.
      iv) Produce content inappropriate by agency standards.
      v) Provide legal, clinical, or eligibility determinations; staff must apply professional judgement and applicable procedures.
4) **DISCLOSURE AND TRANSPARENCY**
   a) **Disclosure of AI Use.** If AI materially contributes to external deliverables (e.g. ISPs, reports, parent/guardian communications, inter-agency correspondence) without significant human alteration or to documentation that becomes part of an official record, note that "AI assistance" was used and name the tool class (e.g. "an approved AI drafting tool"). Disclosure is **not required** for superficial edits (spelling, formatting) that do not affect meaning. Staff must fact-check and take responsibility for all content.
5) **REVIEW AND APPROVAL OF AI TOOLS**
   a) An **Approved AI Tools Register** shall be created and maintained. The register, at a minimum, shall contain:
      i) Application + vendor name
      ii) Approved data types (e.g. public only, ePHI/PII)
      iii) Approval status alongside any exceptions (e.g. no parent/guardian communications)
      iv) Approved business use cases
      v) Any required configuration options (e.g. Chat History OFF, Automated Notes OFF)
      vi) Availability – whether all or limited staff are authorized to use.
   b) New AI Tool Approval Process:
      i) Staff shall submit AI tool requests to the Superintendent for review.
      ii) The HIPAA Security Officer will perform a security risk assessment prior to approval.
      iii) The HIPAA Privacy Officer will perform a privacy risk assessment prior to approval.
      iv) If any use of PHI is involved, a HIPAA Business Associate Agreement will be created
      v) The Superintendent will issue any final approval.
6) SPECIAL SITUATIONS AND SECURITY CONTROLS
   a) App-Consent Governance. End Users must not be permitted to connect AI-related apps to agency tools (such as Microsoft 365). Only IT admins may grant app consents to enable AI-related apps.
   b) Record Retention: Ensure that the tool's record retention configuration aligns with agency policy
   c) Agentic AI (Action-Taking) Controls:

i) No autonomous changes to production records/systems (e.g. Brittco, Intellinetics) are permitted without an approved change or workflow step and a human approval checkpoint.
ii) Systems must maintain complete logs of actions for at least one (1) year.
iii) The agency should test in non-production before enabling in production.
iv) Staff remain accountable for actions triggered by agentic AI they configure or use.

7) **TRAINING AND COMPETENCY**
   a) **Staff Training.** Staff are expected to complete training on responsible and secure use of AI tools prior to utilization. Training will include risks of AI use such as bias, hallucination (false output), and data leakage/exposure.
8) **MONITORING AND ENFORCEMENT**
   a) **AI Use is Monitored.** AI use on agency systems may be monitored and logged. Periodic access reviews are performed for AI integrations.
   b) **Feedback.** Staff should report concerns to leadership about any AI usage.
   c) **Violations.** Improper use of AI tools may result in disciplinary action, including termination. If PHI, PII, or confidential data is exposed through misuse of AI, additional legal or regulatory consequences may apply.
   d) **AI Exposure Incident Handling.** Suspected exposure or over-permissioned app consents are handled via incident response and, when applicable, the Breach Notification Rule.
9) **STANDARD REVIEW**
   a) This standard shall be reviewed at least annually and updated as necessary to reflect evolving technology, agency needs, and regulatory requirements.

REFERENCE

Ohio Administrative Policy IT-17, *Use of Artificial Intelligence in State of Ohio Solutions*, issued by the Ohio Department of Administrative Services (2023)

1110 Social Media Use

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

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164

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

PROCEDURES
1) **Agency-Sponsored Social Media Use**.
   a) The Superintendent and/or designee may approve the establishment of one or more agency-sponsored social media pages or accounts.
   b) Any personnel responsible for social media management must be appropriately trained on this standard
   c) The agency should include a social media privacy policy in an appropriate location on each social media platform
   d) Prior to placing an image or other personally identifiable information on the agency website, social media, print publication, or for any other marketing purpose, the following shall occur:
      i) For individuals served, a properly completed HIPAA authorization must be obtained and retained (see sample form in appendix), and
      ii) For individuals served, or any other persons, and a media release shall be completed and retained (see sample form in appendix).
   e) If an Individual served discloses PHI on an agency-sponsored social media page, the agency may delete or respond to the disclosure.
      i) The Privacy Officer or designee shall review the agency social media account regularly to ensure no improper disclosures have been made by the staff or Individuals served.
      ii) Individuals served are permitted to disclose their PHI on social media, and the agency, at its discretion, may allow it to remain.
      iii) Deleting comments made by Individuals served is permitted, if the comment is deleted **entirely**, at the discretion of the Privacy Officer or designee. If and when an Individual served discloses PHI, the Privacy Officer or designee may remove the information at their discretion, for example, if the comment discloses information judged inappropriate or excessive.
      iv) The agency must never **edit** the disclosure of an Individual served because doing so makes the agency a co-author of the PHI.
   f) For posts from Individuals served, the agency may respond in a general way which in no way acknowledges that the inquirer is an Individual served by the agency. If the post requires a non-general reply, the conversation should be taken offline. The agency should use one of the following three general replies to be used for positive and negative comments and inquiries from Individuals served:
      i) A "like" or favorite
      ii) JCBDD is proud to have been serving the community since 1967 and serves individuals with developmental disabilities. We take privacy seriously. Because federal privacy laws govern protected health information, it is not the policy of JCBDD to substantively respond to negative reviews on the internet. We welcome all individuals served, and their families, to address any concerns or requests for information about services provided with us directly as we strive to continue to provide individualized and excellent service in our community. Please give us a call at 740-264-7176.
      iii) JCBDD is proud to have been serving the community since 1967 and takes its service to individuals – and their privacy – seriously. Because federal privacy laws govern the protected health information of individuals served by this agency, it is not the policy of JCBDD to substantively respond to reviews on the internet, but we always appreciate kind words and recommendations.

2) **Personal use of Social Media by Employees**.
   a) **Employee Use During Work Hours**. During work hours, employees should focus on work-related activities. Employees should not engage in social media during work hours and personal social media use with agency equipment is prohibited.
   b) **Employee Use Outside of Work Hours**. Any statement or image on social media has the potential to become a public communication, so employees of JCBDD must follow the following guidelines:
      i) **Sharing of work-related activities.** Employees should limit the sharing of any JCBDD related information that they would deem acceptable to be made public, for example, on the front page of a major newspaper.
         (1) Examples of information that are appropriate to share on social media include:
            (a) The employee's excitement and satisfaction with the work and mission of JCBDD.
               (i) Details of an upcoming public event sponsored by the Board, such as a local "Special Olympics" day.
               (ii) The name of a friend who is a co-worker at the Board.
         (2) Information that is NOT appropriate to post include:
            (a) The name or image of an Individual receiving services from the agency, unless in compliance with a HIPAA-compliant release of information form and media release form.
            (b) Information about the Agency or its employees that are knowingly untruthful, in violation of law or in violation of an Agency Policy, Standard or Procedure. Employees are directed to seek the express consent of the superintendent for all other Agency information published.
            (c) Comments or displays about coworkers, supervisors, individuals & families, or the agency that are vulgar, obscene, threatening, intimidating, harassing, or a violation of the agency's workplace policies against discrimination, harassment, or hostility on account of age, race, religion, sex, gender, gender identity, ethnicity, nationality, disability, military/veteran status, or other protected class, status or characteristics.
            (d) Unprofessional communication which, if left unaddressed, could potentially result in a civil or criminal cause of action against the agency. Unprofessional communication also includes that which the agency could demonstrate has a substantial risk of negatively affecting the agency's reputation, mission, or operations, such as slander, defamation, or other legal cause of action.
         (3) Employees are not prohibited from making any communication that is protected and regulated by the National Labor Relations Board. Employees are further encouraged but not required to limit communications on social media to those that would portray them in a professional manner.
      ii) **Friending/Connecting/Linking.** Employees are discouraged from "friending", "linking", "following", or otherwise connecting, on any social media platform, to any an Individual served by JCBDD, nor a parent or guardian. JCBDD expects employees to maintain an acceptable professional boundary.
      iii) **Messaging.**
         (1) Employees must not use social media for JCBDD communications, especially if they involve PHI. This is prohibited since the organization does not have a Business Associate agreement with any social media platform.
         (2) Employees who receive unsolicited communications via social media from or about an individual served, or about an individual seeking services, must not respond using social media. Any necessary response must be done in person, via phone, or secure email. If possible, the unsolicited message should be deleted from the social media platform. Any such incident should be reported to the Privacy Officer for investigation.
3) **Social Media and Workplace Harassment.** Harassing communications about coworkers on social media can constitute workplace harassment, even if done outside of the office and/or outside work hours. If you feel that you are the target of workplace harassment, report according to the anti-harassment policy.

1120 Portable Computing Devices

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

AUDIENCE
All Staff

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

PROCEDURES
1) **EMPLOYEE-OWNED MOBILE DEVICES**
   a) **Agreement**. Employees must follow the organization's procedures for enrollment of their mobile device, including signing the Employee-Owned Mobile Device Agreement.
   b) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.
   c) **Personal Use of Phone/Data Backup**. The employee agrees to accept responsibility to back up personal applications and data.
   d) **Text Messaging**. Any text messaging performed from an employee-owned device must be done in accordance with the requirements of this standard. Text messaging using a JCBDD-approved text messaging app is permitted and is the preferred method for any text messaging. The use of standard text messaging with individuals served and/or their parents is prohibited. Medical, behavioral, diagnosis and similar PHI must not be transmitted with standard text messaging. If unsolicited PHI is received via text by a staff member, any response should be via an approved method such as phone call, secure email, or JCBDD-approved text messaging app.
   e) **Audit**. Random audits to ensure compliance with this standard will be conducted by the Information Technologies Department. Employees must surrender the device for audit. Employees failing to comply with this standard may lose access to the JCBDD network resources through a mobile device.
   f) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Standard 1080 Reporting Violations and Security Incidents.
   g) **Permission Granted for Remote Lock/Wipe**. Employee grants the IT Department permission to perform a remote lock, remote wipe and/or geo-location of a device. Employee understands and accepts that the IT Department may perform a remote lock or remote wipe if employee's supervisor makes a written request to the Human Resources Department.
   h) **Use While Driving**. Any use of personally owned mobile devices while driving must be done in accordance with the laws of the jurisdiction in which you are physically present.
   i) **Use of Device by Other People.** Employees using personal devices under this standard are responsible for controlling and/or managing the access and/or use of their device by other people including family members and friends. Employees will be held accountable for any actions performed by others who the employee permits to use the device.
   j) **Replacing a Device**. Prior to replacing/upgrading a device, employees must first remove all of the organization's data prior to returning/selling/disposing of their current device. [Enter any organization-specific procedure here.]
   k) **Sanctions for Violations**. Employees who violate any of the requirements of this standard will be subject to disciplinary action.

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

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

2) **AGENCY-PROVIDED MOBILE DEVICES**

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

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

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

d) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Standard 1080 Reporting Violations and Security Incidents.

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

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

g) **Use of Device by Other People Not Permitted.** Employees using agency-owned mobile devices under this standard must not allow anyone to use agency-owned mobile devices if not permitted to use these devices under this standard. [Modify this standard to conform with agency procedures.]

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

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

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

1130 Employee Work at Home

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

AUDIENCE
All Staff
HIPAA Security Officer and Technical Staff

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

PROCEDURES
1) **Eligibility to Work at Home.** Agency management will evaluate, on an individual basis, the eligibility of employees to work at home.
2) **Privacy and Security Approval.** The HIPAA Security Officer shall review and approve workspace arrangements by employees and independent contractors.
3) **Baseline Work from Home Security Standards**. Unless an exception is granted, employees/independent contractors working from home must follow the Baseline Security Standards below:
    a) The home is equipped with physical security *appropriate for the neighborhood*, including, for example, deadbolt locks, home security system for high crime neighborhoods, and/or video monitoring.
    b) Exterior doors are kept locked when all occupants are away
    c) A private, quiet workspace is available in the home.
    d) Access to the work area by other household members is restricted.
    e) Other household members are prohibited from using agency-owned computing devices
    f) The home network is appropriately secured:
        i) Vendor-supported Routers. The home office uses a router supported by its manufacturer.
        ii) Router Configuration. The router must not use default administrator credentials, must use a strong password, remote management is disabled, and WPA2 encryption is enabled.
        iii) Router firmware must be patched on a timely basis after a vendor-security update is published.
    g) The office is equipped with a shredder for destruction of any confidential paper documents.
    h) A clean-desk practice is followed so that any confidential materials are put away when not in use.
    i) The agency reserves the right to require additional safeguards based on individual review.
4) **Risk Assessment / Exceptions to the Baseline Standards**. The HIPAA Security Officer may perform an individual review for an employee/independent contractor's work-from-home environment. This risk assessment shall consider:
    a) A review/risk assessment is conducted prior to authorizing exceptions to the Baseline Standards:
        i) The threat from outsiders / intruders in the neighborhood
        ii) The threat of access by family and visitors to the remote working equipment
        iii) The threat posed by other computing devices/individuals on the home network
        iv) The physical layout of the home
        v) Other appropriate factors
    b) Based on this risk assessment, the HIPAA Security Officer may approve exceptions to the Baseline Standards.

INDIVIDUAL RIGHTS

2000 Individual's Right to Access Records

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.524(e) Individual's Right to Access PHI
45 CFR § 164.524(b) Time Limits on Response to Access
45 CFR § 164.524(c) Form of Access
34 CFR 99.4 Rights of Parents
34 CFR 300.613(c) IDEA Rights of Parents
OAC § 3301-51-04 Confidentiality, for Education of Students with Special Needs
OAC 3301-51-04(D) Access Rights
OAC 3301-51-04(E) Record of Access
OAC 3301-51-04(F) Records on More than One Child
OAC 3301-51-04(G) List of Types and Locations of Information
OAC 3301-51-04(H) Fees
ORC § 1347.08(A)(2) Individual's Right to Access Records
OAC § 5123-4-01(O) Administration and Operation of County Boards of Developmental Disabilities-Records of Individuals Served

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

PROCEDURES
1) **Parent Information Rights.** Per Ohio law, the following information shall be documented in Appendix E and available to parents:
   a) **Types & Locations of Education Records.** A list of the types and locations of education records collected, maintained, or used by JCBDD must be provided to the parent/guardian of an Individual served upon request, unless rights of the parent/guardian have transferred to the Individual served. [OAC 3301-51-04(G)]
   b) **Names and Positions of Employees with Access to Personally Identifiable Information (PII).** The agency shall maintain a current listing of the names and positions of employees who may have access to PII of children (individuals served who are under age 18). [OAC 3301-51-04(N)]
2) **Who May Access Records**
   a) An Individual served by the Agency above the age of 18, the parent/guardian of a child, the guardian of an adult not able to act on their own behalf, or any "personal representative" of an Individual served may access the records. See Standard 1070 Minors, Personal Representatives and Deceased Individuals.
   b) **3rd Party Review.** An Individual or parent may include any 3rd party of their choosing, including an attorney, to review the records.
   c) **Presumption of Parental Right to Access Records.** JCBDD may presume that either parent of a minor may have access unless presented with documentation that the parent does not have authority under applicable state law governing such matters as guardianship, separation, or divorce.
3) **Procedure, form and method of access**
   a) **Requests for Access.** Requests for access to records shall be directed to the Privacy Officer or his/her

designee.

b) **Verification Procedure.** The Privacy Officer shall follow the Verification Procedure to verify the identity of the requestor. For any grant of access to someone other than the parent, the authority of the requestor to access the information shall also be verified. This might include documentation of guardianship or documentation that the person was appointed a "Personal Representative" under HIPAA.

c) **Redaction of Confidential Information**. Prior to release, Agency staff shall redact any confidential information, regarding other Individuals served. [OAC 3301-51-04(F)]

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

i) **By inspection**. JCBDD shall provide a private room for the Individual to review the records under the supervision of a JCBDD staff member who will ensure that the record is not altered.

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

iii) **Electronic format**. JCBDD shall provide an electronic copy of the information requested if this is feasible; if not, the Security Officer or his/her designee shall negotiate an electronic format and transmission method acceptable to both parties and fulfill the request.

1) If the Individual requests the information via email and only unsecured email is available, the Individual shall be notified that this method is subject to electronic eavesdropping. If the Individual is willing to accept the risks, the info shall be sent via email.

2) The Agency shall honor requests for commonly used media, such as USB Flash drives.

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

f) **Notification to Family Prior to Destruction.** Prior to destruction of data, reasonable efforts shall be made by HCBDD to notify parents/guardians/individuals that they have the right to be provided with a copy of any data which have been obtained or used for the purpose of making individual programming decisions. Reasonable efforts shall be defined as verbal and/or written notice of this right. In the absence of knowing or being able to contact parents, guardians, or other relatives, notice will be placed in the newspaper of general circulation in the county, and failing a response within 30 days, the records will be destroyed.

4) **Other services/rights of Individuals, parents, and guardians**

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

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

c) **Transfer of Rights at Age of Majority**. Rights of parents under these standards and under FERPA and IDEA transfer to the Individual served once that Individual reaches age 18 years. Once a child reaches age 17 years, the child must be informed of this transfer, and the IEP must include a statement that the child has been informed regarding the transfer of rights.

5) **Time for response to request for access**

a) Access shall be granted without unnecessary delay. In particular, requests should be honored prior to any scheduled IEP meeting, hearing, or administrative procedure. Requests in all typical cases shall be honored within 10 business days. In atypical cases, an extension may be required. The Requestor shall be notified in such a case.

6) **Fees for copying/electronic media**

a) JCBDD may charge a fee for reasonable costs of photocopies, postage or electronic media used to provide records.

2010 Individual's Right to Request Amendment of Records

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.526(f) Individual's Right to Request Amendment
OAC § 5123-4-01(O) Administration and Operation of County Boards of Developmental Disabilities-Records of Individuals Served
OAC § 3301-51-04(I), (J), (K), & (L) – Confidentiality - Advising Parent of Right to Hearing, Hearing Opportunity, Hearing Result & Hearing Procedures
ORC § 1347.09 Disputing of Records
34 CFR § 99.20 FERPA – Requesting Amendment of Records
34 CFR § 99.21 FERPA – Rights to a Record Hearing
34 CFR § 99.22 FERPA – Requirements for a Records Hearing

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

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

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

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

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

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

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

2) **RECORDS HEARINGS**

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

a) **Hearing Procedures**

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

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

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

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

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

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

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

b) **Results of Hearing**

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

ii) If, as a result of the hearing, JCBDD decides that the information is not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the Individual, it must inform the Individual of their right to place in the record a statement commenting on the information or setting forth any reasons for disagreeing with the decision of JCBDD.

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

2020 Individual's Right to Receive an Accounting of Disclosures

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

AUDIENCE
HIPAA Privacy Officer
Division Directors

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.528 Accounting of Disclosures of Protected Health Information
45 CFR § 164.528(d) Individual's Right to an Accounting of Disclosures of PHI
34 CFR 99.32 FERPA - Recordkeeping Requirements Concerning Requests and Disclosures

PROCEDURES
1) **Proper Records.** The Privacy Officer shall be responsible for ensuring that proper records are kept to allow for proper and complete responses to any requests for accountings of disclosures. See also procedures listed in 1090 Disclosures that do not Require an Authorization and 1050 Authorizations which specify recordkeeping regarding disclosures..
2) **Individual's Right to Request Accounting of Disclosures of PHI.** Generally, an Individual has the right to request an accounting of disclosures of their PHI by JCBDD and its business associates during a time period of up to six years prior to the date of the Individual's request. Most disclosures are **not** required to be included in the accounting. The types of disclosures which are **not** required to be accounted for are:
   a) For the purposes of treatment, payment and health care operations (45 CFR § 164.502);
   b) To the Individual receiving services, or to a parent, guardian or personal representative, of the Individual's own PHI (45 CFR § 164.502);
   c) Incidental disclosures, as detailed in (45 CFR § 164.502);
   d) Pursuant to an authorization (45 CFR § 164.508);
   e) To persons involved in the Individual's care or other notification purposes (45 CFR § 164.510);
   f) For national security and intelligence purposes, as detailed in (45 CFR § 164.512(k)(2);
   g) Disclosures to prisons and other law enforcement agencies regarding an Individual who is in custody, as detailed in 45 CFR § 164.512(k)(5).

3) **Employee Documentation of Disclosures.** Any employee who makes a disclosure other than listed above shall document the disclosure in the Individual File, with all information described in step 6B below. More specifically, the following types of disclosures must be documented:
   a) To public health authorities
   b) Birth and death reporting
   c) To law enforcement regarding crime on premises
   d) To law enforcement in emergencies where crime is suspected
   e) For cadaveric organ, eye, tissue donation purposes
   f) For judicial and administrative proceedings
   g) For research with an Institutional Review Board (IRB) waiver
   h) To military command authorities
   i) For Workers Comp purposes
   j) To correctional institutions except as detailed in 2G above
   k) About decedents to medical examiners, funeral directors, coroners
   l) For public health activities
   m) About victims of abuse
   n) Regarding child abuse or neglect
   o) To the FDA
   p) To a person who may have been exposed to a communicable disease

q) To health oversight agencies for audits, civil or criminal investigations, inspections, licensure or disciplinary actions
r) In response to a court order
s) In response to a subpoena or discovery request
t) As required by law for wound or injury reporting
u) For identification & locating suspect or fugitive
v) Unlawful and unauthorized disclosures we have knowledge of

4) **Requests to Suspend Individual's Right to Disclosure.** Health oversight agencies and law enforcement officials may request a suspension of an Individual's rights to disclosure. If such a request is received, follow procedures in 45 CFR § 164.528.
5) **Compliance with Request for Accounting Within 45 Days.** The HIPAA Privacy Officer shall comply with an Individual's request for an accounting within 45 days of the request. The JCBDD does not charge a fee for accountings.
6) **The written accounting must meet the following requirements**:
   a) All disclosures of the Individual's PHI during the 6 years prior to the request (or such shorter period as is specified in the request) as stated above.
   b) As to each disclosure, the accounting must include:
      i) The date of the disclosure.
      ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person.
      iii) A brief description of the PHI disclosed.
      iv) A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure.
      v) If during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period, and the date of the last such disclosure during the accounting period.
      vi) If the accounting request includes school records, consult legal counsel regarding the need to obtain records of redisclosures by state or local school officials (see 34 CFR 99.32).
   c) JCBDD will retain documentation (in written or electronic format) for a period of 6 years:
      i) All information required to be included in an accounting of disclosures of PHI.
      ii) All written accountings provided to Individual.

2030 Individual's Right to Request Additional Restrictions

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

AUDIENCE
Privacy Officer, Supervisors

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.522(a) Rights to Request Privacy Protection for Protected Health Information

PROCEDURES
1) **Refer the Request to JCBDD Privacy Officer or Designee:** All requests for additional restrictions on the use or disclosure of PHI will be referred to the HIPAA Privacy Officer, or his/her designee. Upon receiving a request, the Privacy Officer shall consider the following factors, in the decision to grant or deny the request:
   a) Whether the restriction might cause the organization to violate applicable federal or state law;
   b) Whether the restriction might cause the organization to violate professional standards, including medical ethical standards;
   c) Whether JCBDD' systems and organization make it very difficult or impossible to accommodate the restriction;
   d) Whether the restriction might unreasonably impede the organization's ability to serve the Individual;
   e) Whether the restriction appears to be in the best interests of the Individual.
2) **Decision Whether JCBDD will agree**: The JCBDD is not obligated to agree to any requests for restriction, except in the unlikely event that the request is not to bill the Medicaid program or other 3rd party payer and that the Individual receiving services agrees to pay for the service themselves.
3) **Notify the Individual:** JCBDD will notify the Individual of its final decision (whether approving or denying the request) in writing. The notice will be maintained in the Individual's record.
   a) Granting the Request: If JCBDD agrees to the restriction, the notice to the Individual will clearly state what restriction JCBDD is agreeing to in language the Individual will understand. This notice will state that the restriction will not apply if the information is needed for emergency treatment.
   b) Denying the Request: If the request is denied, the notice will clearly state why the request cannot be complied with, in language the Individual will understand.
4) **Take Appropriate Action to Implement Restrictions:** If JCBDD agrees to the requested restriction, the Privacy Officer/designee will be responsible for taking appropriate action to implement the restriction.
5) **Modifying or Terminating a Restriction:** An Individual may request a restriction to be eliminated at any time. If JCBDD desires a modification, consult legal counsel regarding appropriate procedures.
6) **Documentation:** The Privacy Officer is responsible for maintaining the following documents, to assure that additional privacy protections are handled properly, and assure they are maintained for six years from the date of their creation:
   a) Copies of Individual requests for restrictions.
   b) Copies of any notice informing the Individual about JCBDD' decision to grant or deny a restriction.
   c) Copies of any written Individual request to terminate a restriction, or alternatively, copies of any documentation in the Individual's record that the Individual made such request orally.

2040 Individual's Right to Request Confidential Communications

STANDARD
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 JCBDD administrative systems.

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.502(h) Confidential Communications
45 CFR § 164.522(b) Confidential Communications Requirements

AUDIENCE
Privacy Officer

PROCEDURES
1) **Individual's Right to Request Confidential Communications**. Individuals, or their personal representative, may make a request for confidential communications in writing to the Privacy Officer.
2) **Receiving a Request.** When the Privacy Officer receives a request, the Privacy Officer may not ask the reason for the request. The Privacy Officer shall contact the Individual making the request to obtain an alternate means of contacting them (e.g. cell phone, PO Box, etc.). The Individual will be informed at that time of steps JCBDD will take to implement the request.
3) **Implementing the Request.** If existing systems are capable of administering the request, the Privacy Officer shall take necessary steps to implement the request, such as adjusted phone numbers or addresses in computer files or mailing lists.
4) **Documenting the Request.** The Privacy Officer shall document the request, and disposition, in the Individual's Record.
5) **Recommending Necessary Improvements in Computer Systems or Administrative Procedures.** When needed, the Privacy Officer will make recommendations to the Superintendent of improvements necessary in computer systems or administrative procedures in order to implement reasonable requests for confidential communications.

2050 Individual's Right to Notice of Privacy Practices

STANDARD

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

AUTHORITY

HIPAA Privacy and Security Rules, 45 CFR § 164
- 45 CFR § 164.520 Notice of Privacy Practices for Protected Health Information
- 45 CFR § 164.502(i) Uses and Disclosures Consistent with Notice

OAC 3301-51-04(C) Confidentiality for EI/Pre-School/School Age; See also:
- 34 CFR 99.7 Notice (FERPA)
- 34 CFR 300.612 Notice (IDEA Part B)
- 34 CFR 303.404 Notice (IDEA Part C)

ORC § 1347.08(A)(3) Rights of Persons Who are Subject of Personal Information
OAC 5123-4-01(O) Administration and Operation of County Boards of Developmental Disabilities – Records

LEGAL NOTES

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

AUDIENCE

Privacy Officer

PROCEDURES

1) **Drafting of Notice**. The Privacy Officer shall draft a Notice which is compliant with the requirements of the HIPAA, FERPA and IDEA regulations as well as OAC 3301-51-04(C). This shall include translations as necessary based on the language needs of the Individuals served. Further, the Notice shall be consistent with the Agency's privacy practices as detailed in these policies. Notice is detailed in the Notice of Privacy Practices.
2) **Updating Notice.** The Privacy Officer shall update the Notice as necessary based on changes in the Agency's privacy policies and/or the legal requirements as necessary. Upon update, the website and Notices posted at each facility (see below) shall be updated. Additionally, an updated copy will be provided to all Individuals receiving services and/or parents.
3) **Distribution of Notice.** The Privacy Officer shall ensure that Agency workflows, are maintained to ensure appropriate distribution of Notice. The following standard shall apply:
    a) All adults at intake will be given a copy of the Notice of Privacy Practices. At the time that the Notice is provided, the Individual or guardian shall sign an acknowledgement of his or her receipt of this Notice as part of the intake/transition of rights paperwork. This acknowledgement will be retained as part of the permanent record, for compliance with HIPAA requirements.
    b) For children (under age 18) a copy of the Notice shall be provided annually to the parent or guardian.
    c) For children (under age 18), the Agency shall coordinate with the appropriate education authority to ensure that the notice, "A Guide to Parent Rights in Special Education" (formerly "Whose IDEA Is This?"), is distributed annually.
    d) An additional copy of the Notice shall further be provided upon request by an Individual or parent.
4) **Posting of Notice.** The Privacy Officer shall ensure that the Notice is posted:
    a) **Website.** On the Agency's website.
    b) **At Each Facility.** At each facility, in a place where Individuals served can be reasonably expected to see the Notice, such as the reception areas of all Agency facilities.
    c) Copies of the Notice will be maintained for 6 years, as detailed in Policy 802 – Records Retention Schedule.

REFERENCE

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

PERSONNEL SECURITY

3000 Onboarding and Offboarding – IT and Facility Access

STANDARD
Documented onboarding and offboarding procedures will be used for granting and removing access to IT assets and agency facilities.

AUDIENCE
Human Resources
HIPAA Privacy Officer
HIPAA Security Officer

REFERENCES
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR 164.308(a)(3)(ii)(B) –Workforce Clearance Procedure
45 CFR 164.308(a)(3)(ii)(C) – Termination Procedures
NIST CSF GV.RR-04, PR.AA-01

PROCEDURES
1) **Onboarding Procedures**.
   a) Employee and independent contractor background checks will be performed per agency policy
   b) Employees will complete general orientation and any job-specific training.
   c) Employees will be enrolled in Security Awareness Training in accordance with the Standard 3020 Staff Training.
   d) Access to company IT Assets will be handled as detailed in Standard 3010 Access Control.
   e) Access to facilities shall be granted based on agency policy.
2) **Offboarding Procedures**. Upon termination of an employee and/or independent contractor, the termination procedure will include the following steps, to be completed on the day of termination:
   a) Any keys or access tokens for company facilities will be returned. Facility access control systems will be promptly updated to disallow access.
   b) Any company-owned computing equipment or other property will be returned
   c) If the individual used any personally-owned (BYOD) computing equipment for company business, any data related to the company will be securely deleted
   d) Email accounts and voicemail accounts assigned to the individual will be re-directed to another employee and the password will be changed. Personal files will be archived or transferred to another employee.
   e) All IT Asset accounts used by the individual will be disabled and/or the password will be changed.
   f) For any shared accounts that the individual had access to, the passwords will be changed.
   g) For involuntary terminations, appropriate preparation, planning, and security precautions will be taken, especially for IT personnel, to protect the agency from any retaliation.

   Records of these termination steps will be maintained in the employee's personnel file and/or independent contractor file.

3010 Access Control

STANDARD
Access Control will be strictly managed. Access will be granted only upon approval from an authorized individual, role-based access controls will implemented based on minimum necessary analysis.

AUDIENCE
Superintendent, Department Heads, System Owners
HIPAA Privacy Officer
HIPAA Security Officer

REFERENCE
HIPAA Privacy and Security Rules, 45 CFR § 164
164.308(a)(3) & (a)(4) Workforce Security and Information Access Management
164.308(a)(5) Password Management
164.312(a) Access Control, Unique User identification, Emergency Access Procedure, and Automatic Logoff
NIST CSF PR.AA-05, GV.RR-04

PROCEDURES
1) Only department heads and System Owners have authority to grant access to agency information systems, and to grant exceptions/additions to standard access privileges.
2) Role-based access controls shall be created using the minimum necessary analysis created per Standard 1020 Minimum Necessary .
3) Access credentials must be delivered to end-users securely.
4) Periodic audits, at least annually, shall be made to IT asset access control lists, including a review of the standard role permission profiles for Role-based access controls.
5) For any third-party system access:
   a) HIPAA Business Associate Agreements shall be obtained when applicable,
   b) Appropriate end-user agreements shall be established when applicable, and
   c) System Owners are responsible for disabling access when the business need for access is concluded
6) For employee job changes, access privileges no longer needed shall be de-authorized and removed.
7) In the event of an emergency such as natural disaster, the System Owner and/or HIPAA Security Officer, or designee, may grant employee access to systems outside of normal guidelines to ensure continuity of the agency's mission.

3020 Staff Training

STANDARD
Appropriate staff training will be provided regarding privacy and security compliance and IT security.

AUDIENCE
Human Resources
HIPAA Security Officer
HIPAA Privacy Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.530(b) Training and Training Implementation Standards
45 CFR § 164.530(i) Policies and Procedures
45 CFR § 164.520 Notice of Privacy Practices for Protected Health Information
45 CFR § 164.308(a)(5) Security Awareness and Training
ORC § 5123.64(A) Training in Rights
OAC § 5123-5-02(D) Service and Support Administration Certification Standards – Annual Training Requirements
OAC § 5180-10-05(D) Early Intervention Program-Developmental Specialist Certification-Annual Training Requirements, renumbered 1/2/2025
OAC § 5123-5-07 Investigative Agent Certification Standards
NIST CSF GV.RR-04, PR.AT-01, PR.AT-02

PROCEDURES
1) **Training New Staff on *Privacy and Security Standards*.** The HIPAA Privacy Officer, HIPAA Security Officer, and Human Resources department shall collaborate to ensure that all new staff receive training on JCBDD *Privacy and Security Standards* promptly after hiring and whenever policies are substantially revised.
2) **Security Awareness Training**. The agency shall ensure implementation of an appropriate, ongoing security awareness training program for all employees and contractors. NIST SP 800-50 Rev. 1, published September 2024 shall be used to design the program. The following elements shall be considered for program design:
   a) Training Goals
   b) Target Audience and audience sub-groups, for example, financial staff, top management, help desk staff
   c) Deployment methods
   d) Evaluation and Measurement
   e) Frequency.

   The training program may be developed in-house, or a commercially available program may be used.
3) **Role-based Training.** Additional IT security training may be provided to the following groups:
   a) **Privileged User Training**. IT administrators and others with privileged access shall receive appropriate training.
   b) **Executive Training**. Senior executives shall receive training on their roles and responsibilities as they relate to the organization's Security Program. This includes but is not limited to budgetary and supervisory responsibilities for the security management process, the incident response process, and business continuity process.
   c) **Cybersecurity Personnel**. Individuals involved with IT Security and Compliance, Business Continuity, Data Recovery, and/or Incident Response shall receive appropriate training.
   d) **Software Developers**. Software developers shall receive appropriate training in secure coding.
4) **Documentation**. Training records shall be maintained in each employee's personnel file for at least 6 years.

3030 Investigation and Response to Privacy/Security Violations

STANDARD
Reports of potential violations of these *Privacy and Security Standards* shall be investigated and addressed.

AUTHORITY
HIPAA Privacy Rules, 45 CFR § 164
45 CFR § 164.530(e)(1) – Sanctions
NIST CSF GV.RR-04

PROCEDURES
1) **Investigation.** The HIPAA Privacy Officer and/or the Security Officer, in conjunction with human resource and other appropriate management personnel, shall investigate any reported privacy violations and/or security incident. The investigation should include:
   a) **Who –** agency personnel involved, names of any individuals served, any known recipients of PHI
   b) What – description of incident. Include narrative of incident, any mitigation, locations, etc.
   c) When – date/time of incident and any chronology
   d) Where - where the incident occurred
   e) Why – provide any motivations / details of the incident. For example, was this an accident?
2) **Procedure for Security Incident.** For security incidents which are potential data breaches, the Privacy and/or Security Officer will follow procedures detailed in Standard 4030 Breach Reporting **Procedure for Privacy Violation.** For Privacy Violations, the Privacy Officer will follow procedures in Standard 4040 Mitigation.
3) **Filing of Written Report by Privacy and/or Security Officer.** A written incident report will be written by the Privacy and/or Security Officer. It will be filed in:
   a) the Privacy Officer's Privacy Violations file; and
   b) the employee's personnel file.
4) **Employee Discipline**, if appropriate, will be taken and documented in accordance with the following standard:
   - Policy 6.01 Discipline & Policy 6.02 Guidelines for Discipline
5) **Post-Incident Review**. A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in standards/procedures, additional training, or other appropriate action.

COMPLIANCE AND THIRD-PARTY MANAGEMENT

4000 Regulatory Compliance

STANDARD
The agency will ensure appropriate regulatory compliance for privacy and security regulations including HIPAA, FERPA/IDEA, other federal laws and state laws relating to privacy and security.

AUTHORITY
HIPAA Privacy Rules, 45 CFR § 164
45 CFR § 164.530(e)(1) – Sanctions
45 CFR § 164.530(j) – Documentation requirement
45 CFR § 164.520(e) – Notices of Privacy Practices
45 CFR § 164.524(e) – Access of individuals to protected health information
45 CFR § 164.526(f) – Amendment to protected information
45 CFR § 164.508(b)(6) – Uses and disclosures for which an authorization is required
45 CFR § 164.522(a)(3) – Rights to request privacy protection for protected health information
45 CFR § 164.528(d) – Accounting of disclosures of protected health information – Implementation specification
ORC §9.64 Cybersecurity for Political Subdivisions
ORC § 5126.044 DD Board Confidentiality
OAC 3301-51-04(N) Confidentiality Safeguards
NIST CSF GV.OC-03, GV-RR-02,

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

PROCEDURES
1) **Regulatory Compliance**. The agency shall identify applicable compliance obligations and develop appropriate compliance programs. This shall include HIPAA, FERPA/IDEA, ORC § 9.64 and other state security and privacy laws, and other applicable laws and regulations relating to privacy and security.
2) **Privacy Officer.** The Superintendent shall designate a person to the Privacy Officer role, to be responsible for development, implementation, enforcement, and update of HIPAA Privacy program. This individual shall be accountable for ensuring the confidentiality of any personally identifiable information [per OAC 3301-51-04(N)].
3) **Security Officer**. The Superintendent shall designate a person to the Security Officer role, to be responsible for the development, implementation, enforcement, and update of the HIPAA Security program.
4) **Job Descriptions**. Job Descriptions for the Privacy and Security Officers are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer.
5) **Other Appointments.** The Superintendent may also designate other persons to assist/support the Privacy and Security Officers, e.g., a HIPAA committee, Disaster Recovery Team (DRT), Incident Response Team (IRT) and any other support roles.
6) **Periodic Review and Update of Compliance Policies.** The HIPAA Privacy Officer and Security Officer shall periodically review all privacy and security policies and update them as necessary based on new circumstances, changes in federal regulations and any changes in Ohio state laws and regulations governing DD Boards.
7) **Policy/Standard Audit Trail.** An audit trail of standard changes will be maintained for 6 years.
8) **Documenting Records Covered by HIPAA and FERPA**. The records covered by HIPAA and FERPA shall be documented following the procedures for the "Designated Record Set" of the HIPAA regulations.
9) **HIPAA Mandated records**. HIPAA Mandated records include the following:
    a) HIPAA Required designations, including, Hybrid entity designation if applicable, description of records in Designated Record Set, the names of staff responsible for duties of Privacy Officer, receiving HIPAA complaints, providing access to Individual records, receiving requests for amendment of Individual records, answering questions about HIPAA policies and procedures. See Appendix F.

b) Notice of Privacy Practices, as described in Standard 2050 Individual's Right to Notice of Privacy Practices, and signed acknowledgements that Individuals served have received a copy of the notice.
c) Restrictions on use or disclosure of PHI agreed to by JCBDD as described in the Standard 2030 Individual's Right to Request Additional Restrictions.
d) Records of disclosures, as required by the Standard 2020 Individual's Right to Receive an Accounting of Disclosures.
e) Any signed authorization as described in Standard 1050 Authorizations.
f) All privacy-related complaints received, and their disposition, if any, as described in Standard 4060 Privacy Complaints.
g) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Standard 1080 Reporting Violations and Security Incidents.
h) Incident Reports and other documentation specified by Standard 4030 Breach Reporting and Standard 5040 Security Incident Response.
i) Records detailed in Standard 5000 Security Program, including the formal Security Risk Analysis, records that this was reviewed by all decision makers, and risk management actions taken.
j) Training records maintained in accordance with Standard 3020 Staff Training.

10) See also Policy 802 Records Retention Schedule for retention periods and destruction procedures.

4010 Data Governance

STANDARD

Data governance principles are established to define responsibilities for data-related matters. Responsibilities are shared between the HIPAA Security Officer, HIPAA Privacy Officer and System Owners as defined in this standard.

AUDIENCE

HIPAA Privacy Officer, HIPAA Security Officer, System Owners

AUTHORITY

HIPAA Privacy and Security Rules, 45 CFR Part 164
- 164.308(a)(3) Workforce Security
- 164.308(a)(4) Information Access Management
- 164.308(a)(5) Password Management
- 164.312(a)(2)(ii) Emergency Access Procedure
- 164.312(a)(2)(iii) Automatic Logoff

NIST CSF GV.RR-02

DATA GOVERNANCE RESPONSIBILITIES

1) **Responsibilities**. Responsibility for the confidentiality, accuracy and integrity, availability, and compliance are shared among different individuals and departments at JCBDD. Responsibilities are either:
   A) Primary (P). Primary responsibility is the day-to-day, ongoing duty to perform the task, or
   B) Secondary (S). Secondary responsibility is the obligation to provide guidance and/or assistance when requested.
2) **System Owners.** Each department head or designee assigns the application System Owners. These designations are documented in Appendix C. System Owners have primary responsibility for access control, system configuration, end-user training, first-level support, internal audit, and ensuring individual and parent rights for access to their information and/or requests for amendment of records.
3) **HIPAA Security Officer.** The HIPAA Security Officer maintains primary responsibility for data backup and recovery, data integrity and second-level support and issue resolution.
4) **Privacy Officer**. The Privacy Officer maintains secondary responsibility for privacy, confidentiality, compliance, and the rights of access and data correction processes for Individuals served and their parents/guardians.
5) **Responsibility Chart**. The following responsibility chart defines the roles of the various parties in data governance:

	RESPONSIBILITIES		
Task	**System Owner**	**HIPAA Security Officer**	**HIPAA Privacy Officer**
Access Control – Defining, Implementing and Maintaining Access Rights	P	S	S
Access Control – Onboarding and separation process of users	P		
Access Control – Annual audit of authorized users	P	S	S
Secure configuration of applications: automatic logoff, enabling audit controls, configuring password policy	P	S	
End-user Training and First-level user support	P		
Second-level user support		P	
Internal audit, per HIPAA requirements	P	S	S
Data Backup, Data Integrity, and Data Recovery		P	
Individual and Parent Rights regarding information access and/or requests for amendment	P		S
Data Retention	P		

4020 Third Party Management

STANDARD
JCBDD will obtain satisfactory assurance that third-parties will safeguard PHI by using a third-party privacy and security management program including vendor risk assessment, vendor security assurance, and appropriate contracting.

AUTHORITY
45 CFR 160.103 General Administrative Requirements – Definitions
HIPAA Privacy and Security Rules, 45 CFR Part 164
45 CFR § 164.502(e) Disclosures to Business Associates Standards
45 CFR § 164.504(e) Business Associate Contracts Standards
34 CFR 99.31(a)(1)(i)(B) Conditions that Prior Consent is Not Required
ORC § 5126.044 – Confidentiality
NIST CSF GV.OC-02, GV.RM-05, GV.SC (01 to 10)

PROCEDURES
1) **Business Associate Contract or Memorandum of Understanding.** JCBDD will have a written Business Associate Contract with every Business Associate. For a COG or other government agencies, a Memorandum of Understanding will be executed. See Appendix A Identifying Business Associates.
2) **Contracting Terms**. Whenever possible, the agency shall negotiate contract terms to protect the agency including indemnification of the agency by the third-party for costs relating to data breaches, specific protocols for timely notification of security incidents, and the requirement for cyber-liability insurance commensurate with the potential exposures. The contract form shall conform with requirements of HIPAA, FERPA/IDEA, and other regulatory obligations. See Appendix B - Sample HIPAA Business Associate Agreement.
3) **Vendor Security Assurance**. Due diligence will be exercised by the HIPAA Privacy and/or Security Officer to validate Business Associate compliance with the terms of the agreement. This may include a vendor security management program consisting of one or more of the following elements:
    a) Risk assessment of vendors based on the nature of the service, resulting in different levels of safeguards based on the risk posed by the vendor relationship.
    b) The requirement that high-risk vendors achieve third-party certifications such as SSAE22 SOC 2, ISO 27001, or other certification.
    c) Security evaluations which may include security questionnaires, audit of security artifacts supplied by the vendor, and/or on-site inspections. Vendor cybersecurity risk shall be included in the agency's ongoing risk assessment and risk management processes.
    d) Security responsibilities for independent contractors working at the company's facilities or accessing the company's systems shall be clearly articulated and agreed.
    e) The agency shall ensure appropriate vendor risk management upon contractor termination.
4) **Shared-Responsibility Security Model**. For vendor contracts which specify obligations of the agency under a shared-responsibility security model, the HIPAA Security Officer shall ensure the agency's compliance with any agency obligations.
5) **Material Breach or Violation of Business Associate Contract.** In the event JCBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, JCBDD will take steps to cure the breach or end the violation. If JCBDD is unable to cure the breach or end the violation, JCBDD will terminate the Business Associate Contract.

4030 Breach Reporting

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

AUDIENCE
HIPAA Security Officer, HIPAA Privacy Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164, Subpart D Notification in the Case of Breach of Unsecured Protected Health Information
45 CFR § 164.400, Applicability
45 CFR § 164.402, Definitions
45 CFR § 164.404, Notifications to Individuals
45 CFR § 164.406, Notification to the Media
45 CFR § 164.408, Notification to the Secretary
45 CFR § 164.410, Notification by a Business Associate
45 CFR § 164.412, Law Enforcement Delay
45 CFR § 164.414 Administrative Requirements and Burden of Proof
NIST CSF GV.SC-08, RC.CO-03, RC.CO-04

PROCEDURES
1) After investigation of privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer shall jointly determine if the incident meets the definition of a breach. Legal counsel and other outside expert advice may be obtained. The following procedure shall be used:
   a) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   b) Does one of the statutory exceptions listed in the breach definition in Standard 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   c) Unless the incident is clearly a breach, the Team shall conduct a risk assessment using Appendix G – HIPAA Security Incident Risk Assessment Template. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.
   d) **Documentation.** Record a summary of the incident in the HIPAA Incident Log, noting the date, individuals impacted, risk assessment status, and whether the incident meets the definition of a reportable breach. The log entry should include a reference to the corresponding risk assessment document. Retain the completed risk assessment and investigation notes for 6 years from completion, in accordance with HIPAA documentation requirements.
   e) **Decision**. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred, and this process may stop. Otherwise, a breach has occurred, and the Team should proceed with the steps that follow in the remainder of this standard.
2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   a) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the Agency may use telephone, email or other means to immediately notify Individuals of the breach.

ii) Prepare formal written notification for approval by Superintendent. The notification shall be written in plain language and include the following:
   (1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
   (2) A description of the types of unsecured protected health information that were involved in the breach;
   (3) Any steps that Individuals should take to protect themselves from potential harm resulting from the breach;
   (4) A brief description of what the Agency is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and
   (5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site or postal address.

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

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

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

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

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

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

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

4040 Mitigation

STANDARD

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

AUDIENCE

Privacy Officer

AUTHORITY

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

PROCEDURES

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

4050 Non-intimidation and Non-etaliation

STANDARD

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

AUDIENCE

Privacy Officer

AUTHORITY

45 CFR § 164.530(g) – Refraining from intimidating or retaliatory acts
45 CFR § 164.530(h) – Waiver of rights

PROCEDURES

1) **JCBDD will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:**
   a) **Individuals Receiving Services**. Any Individual for the exercise by the Individual of any right under, or for participation by the Individual in any process established by the HIPAA regulations;
   b) **Individuals Receiving Services and others**. Any Individual receiving services, or other person for:
      i) Filing of a complaint with the Secretary of HHS regarding a HIPAA issue;
      ii) Testifying, assisting or participating in an investigation, compliance review, proceedings or hearing under Part C of Title XI; or
      iii) Opposing any act or practice made unlawful by the HIPAA regulations, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information.
2) **Retaliatory action is defined as doing any of the following**:
   a) Removing or suspending the employee from employment;
   b) Withholding from the employee salary increases or employee benefits to which the employee is otherwise entitled;
   c) Denying the employee a promotion that would have otherwise been received;
   d) Transferring or reassigning the employee;
   e) Reducing the employee in pay or position.
3) **Non-retaliation statement**. A person who in good faith brings a complaint will not be subject to retaliation. Retaliation against any person who falls within this definition, either Individual served or staff member of JCBDD, is strictly prohibited.
4) **Prohibition against Waiver of Rights**. No office, program, facility or employee of the JCBDD shall require Individuals to waive any of their rights under HIPAA as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits. The Agency may require parents of children under age 18 receiving services reimbursed by Medicaid to sign an authorization granting the Agency permission to bill Medicaid.
5) **Employee Disclosures of PHI for Whistleblowing**. Employees are permitted to disclose PHI when necessary for whistleblowing. JCBDD will also follow Policy 1.15 Whistleblower and Reporting as appropriate.

4060 Privacy Complaints

STANDARD
Any Individual or employee to may complain about the JCBDD's *Privacy and Security Standards* and/or the JCBDD's compliance with those policies. The JCBDD shall take action and document all such complaints.

AUDIENCE
All Staff

AUTHORITY
45 CFR § 164.530(d) HIPAA Complaint Procedures
ORC § 5123.64(A) requires establishment of a Complaint Procedure
ORC § 5126.06 Resolution of Complaints
OAC § 5123-4-04 Administrative resolution of complaints involving the programs, services, policies, or administrative practices of a county board or the entities acting under contract with a county board

PROCEDURES
1) **The HIPAA Privacy Officer shall manage this complaint process**, and shall be designated in the Notice of Privacy practices as the person to receive complaints.
2) The JCBDD will extend the provisions of Policy 1.15 Whistleblower and Reporting, to all persons who file confidentiality or privacy related complaint.
3) **Employee to File Written Complaint with Privacy Officer.** An employee or Individual should file their complaint in writing to the Privacy Officer. Employees may review Policy 1.15 Whistleblower and Reporting which provides for alternate officials to receive the written complaint.
4) **Review and Investigation of Complaint.** Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Superintendent) shall review and investigate the complaint.
5) **Corrective Action.** If warranted, the Privacy Officer shall take corrective action, which may include:
   a) Change of standard and/or procedure.
   b) Intervention with an employee who is not following procedures including additional training and/or sanctions.
   c) Other action as appropriate.
6) **Communicating Results of Investigation and Corrective Action.** The Privacy Officer shall communicate the results of the investigation and any corrective action taken to the person filing the complaint.
7) **Documentation of Complaints.** The JCBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Standard 4000 Regulatory Compliance.

COMPUTER SECURITY

5000 Security Program

STANDARD
JCBDD will operate a comprehensive IT security program under the direction of its HIPAA Security Officer.

AUDIENCE
Executive Management
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(2) Assigned Security Responsibility Standard
Ohio Rev. Code § 9.64 Political Subdivision Cybersecurity

PROCEDURES
1) **Security Program**. The agency Board of Trustees has directed the executive leadership to implement a cybersecurity program consistent with the NIST cybersecurity framework: :
   a) Controls shall be selected consistent with the size and scale of the organization based on risk assessment
   b) Cybersecurity roles and responsibilities must be identified and assigned
   c) Senior leadership shall fully support this program and fund it with appropriate budgetary allocations.

   The Superintendent shall define the program in these *Privacy and Security Standards* and update them on a regular basis.
2) **The HIPAA Security Officer will be responsible for the security management process**. This will include:
   a) **Computer Security Risk Analysis**. A risk analysis will be conducted and updated periodically. The Risk Analysis is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI and other important agency information maintained on systems owned or used by JCBDD. The Computer Security Risk Analysis will be handled as follows:
      i) JCBDD will use an established and reputable risk analysis methodology, either NIST SP 800-30 Revision 1 or the FAIR Methodology.
      ii) The risk assessment shall include risks in the cybersecurity supply chain
      iii) The results of this analysis shall be documented and maintained for 6 years
      iv) The risk analysis shall be updated on an regular basis, or more frequently if appropriate based on technical and environmental variables, major software updates, infrastructure, or other technological changes.
      v) The risk analysis shall be reviewed by the Security Officer, Privacy Officer, Superintendent, and any other person(s) involved in risk management decision making or implementation. JCBDD will maintain written documentation that these persons reviewed this risk analysis and will maintain that documentation for 6 years.
   b) **Risk Management**. JCBDD shall manage the risks identified in the risk analysis:
      i) JCBDD's Superintendent, in conjunction with the Board of Trustees, shall articulate its risk tolerance.
      ii) The HIPAA Security Officer shall lead the risk management process in consultation with senior leadership. Based on the agency's risk tolerance, identified risks must be reduced, transferred (through contract or insurance) or accepted.
      The HIPAA Security Officer shall appropriately manage any projects identified to reduce risk.
      iii) These decisions shall be formally documented in a risk register. This documentation shall be maintained for 6 years.
      iv) The risk management outcomes, strategy, and performance shall be evaluated annually for the purposes of continuous improvement.
   c) **Annual Report to the Board of Trustees**. The Superintendent and/or HIPAA Security Officer shall make an annual report to the Board of Trustees regarding the cybersecurity program.

REFERENCES

NIST SP 800-30 Guide for Conducting Risk Assessments
NIST CyberSecurity Framework Project
Center for Internet Security (CIS) Top 18 Controls
The Fair Institute and FAIR Method
NIST CSF GV.OC-1, GV.OC-2, GV.RM-01, GV.RM-02, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.RR-01, GV.RR-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-01, GV-SC-03, GV.SC-09, ID.RA-04, ID.RA-05, ID.RA-06

5010 IT Asset Management and Data Flow Mapping

STANDARD
The organization shall maintain an accurate IT asset inventory

AUDIENCE
HIPAA Security Officer

REFERENCE
45 CFR § 164 HIPAA Privacy and Security Rules
45 CFR 164.308(a)(1) Administrative Safeguards -Security Management Process
NIST CSF ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID-AM-07

PROCEDURES
1) **Accountability**. The HIPAA Security Officer should ensure that accurate inventories and data flow maps are maintained per this standard.
2) **IT Asset Inventories**. Inventories will be maintained, using appropriate systems and procedures, for the following:
    a) IT Processing Assets
        i) Cloud environments
        ii) Physical, virtual, and/or cloud servers or desktops
        iii) Mobile devices, including, laptops, smartphones, tablets
        iv) Physical storage devices, including NAS, external disk drives, USB flash drives, external disk drives, and any other storage device
        v) Network gear, including firewalls, switches, access points, and any other gear
        vi) IOT devices
        vii) Any other physical or virtual device
    b) Software Assets
        i) Operating Systems
        ii) Application Software
    c) Third-Party Services / Cloud Applications
    d) Databases, Fileshares, Folders, and/or Datafiles containing PHI, PII or other sensitive data
3) **IT Asset Lifecycle Management**. The agency uses a lifecycle management program for its IT Assets:
    a) IT Assets – hardware, operating systems, and other software shall be upgraded prior to end of life. Only hardware and software which is supported by the vendor or author shall be used.
    b) Employee workstations should be replaced at least every 5 years
4) **IT Asset Movement**. Appropriate operating procedures shall be used for IT asset movement and decommissioning as detailed in Standard 5100 Device and Media Management.
5) **Data Flow Mapping**. Data flows of data may be mapped for any systems which process HIPAA-regulated information and/or other sensitive information.
6) **Business Continuity / Disaster Recovery**. IT asset inventories shall be protected as part of the organization's Disaster Recovery and/or Business Continuity plans.

5020 Data Backup

STANDARD

The HIPAA Security Officer will ensure that a robust data backup regimen is continually operational. The HIPAA Security Officer shall personally ensure that the procedures below are consistently maintained.

AUDIENCE

HIPAA Security Officer

AUTHORITY

HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(7) Administrative Safeguards- Contingency Plan
NIST CSF ID.AM-05, PR.DS-11, GV.OC-05,

NOTE

"**Protected from Malicious Deletion**" means that one or more safeguards are in place to prevent deletion of the backup as part of a ransomware attack. Various technologies and strategies exist, including

a) Isolation of backup, for example, by omitting a backup server from the domain or using a cloud backup service
b) Rigorous access control and authentication, for example restricting access to the backup facility, omitting access credentials from password managers, and/or enabling MFA for the backup facility
c) Backing up to removable media (e.g. magnetic tape) which is physically detached
d) Saving the backup to unmodifiable media (e.g. Write-once, read-many (WORM))
e) Cloud vendor anti-ransomware features which retain backups after deletion and permit recovery via an authenticated phone call
f) Mandating dual authorization for configuration changes

PROCEDURES

1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality.
2) **Multiple Backup Generations**. Backups should include as many generations as is practical to store and no fewer than daily snapshots for 30 days. Backup frequency shall be determined based on risk assessment and Recovery Point Objective specified in the Disaster Recovery Plan.
3) **Backup Software**. An appropriate backup facility/system shall be used. Configuration and/or scripting shall be reviewed and adjusted whenever infrastructure changes are made to ensure that appropriate data backup is maintained.
4) **Multiple Backup Copies**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include at least 2 backup copies: one on-site and one off-site. At least one backup must be protected from malicious deletion.
5) **Backup Documentation**. A written description of the backup regimen should be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
6) **Responsibility**. The HIPAA Security Officer shall designate the employee with primary responsibility to perform daily monitoring of backup, with an alternate person if the primary employee is not working. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7) **Backup Log**. A daily electronic log of backup must be maintained.
8) **Backup Media Security**. Backup media shall be maintained in a secure location.
9) **Testing and Plan Revision.** On at least a yearly basis, a trial restore should be performed to verify the proper function of the backup process.

5030 Disaster Recovery and Business Continuity Plans

STANDARD
JCBDD personnel shall develop contingency plans, to include a Disaster Recovery (DR) Plan and Business Continuity (BC) Plan to prepare for system failures, and for procedures for maintaining critical JCBDD operations in the event of system failures.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR 164.308(a)(7) Administrative Safeguards - Contingency Plan
NIST PR.IR-04, RC.RP-01, RC.RP-02, RC.RP-03, RC.RP-06, RC.CO-03

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

vii) The criteria for declaring end of incident response is defined

5) **Business Continuity (BC) Planning Process**.
   a) **Preparation Steps**. For each prioritized business process, the necessary preparation steps necessary to permit functioning in the absence of systems shall be identified. Preparation steps may include:
      i) Creation and updating of alternate, up-to-date, copies of key information,
      ii) Maintenance and update of manual systems, for example, paper forms, and/or
      iii) Periodic drills to ensure adequacy of preparation.
   b) **Business Continuity (BC) Plan**. A formal, written Business Continuity Plan shall be created which will include the following sections:
      i) Purpose and Scope of Plan,
      ii) Plan Overview including procedures for plan updating and plan testing,
      iii) Plan activation protocol and decision-making procedures during Business Continuity, and
      iv) Playbooks for functioning for each system/department prioritized for inclusion in the BC Plan.
6) **Plan Testing**. The agency shall periodically test the DR Plan and the BC Plan. All tests and their results shall be documented.
7) **Plan Update**. The DR Plan and BC Plans shall be updated periodically based on changes to the organization, technology platforms, and systems, and to incorporate improvements based on plan testing.

5040 Security Incident Response

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

AUDIENCE
All Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(6) Administrative Safeguards-Security Incident Procedures
NIST CSF GV.SC-08, ID.IM-02, ID.IM-04, RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.CO-02, RS.MI-01, RC.RP-01, RC.CO-03

PROCEDURES
1) **Creation of Response Team, Contingency Planning and Drills**
   a) **Incident Response Team.** The HIPAA Security Officer is responsible for managing security incident response and reporting. The agency may appoint an Incident Response Team (IRT). The mandate of any IRT is to coordinate the Agency's response to security incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services by the Agency and the media.
   b) **Response Plans/Protocols.** Incident response planning may include creation of plans and protocols including:
      i) Triage of incidents, which includes a validation process
      ii) Protocols for different categories of incidents
      iii) Decision making process during security incidents
      iv) Identification of specialist firms including an incident response/forensic consultant, public relations consultant, and/or legal counsel
      v) Communications procedures for internal stakeholders, legal counsel, ISACs/threat intelligence organizations, and others
      vi) Notifications to insurers, law enforcement, and external stakeholders, including all notifications required by ORC § 9.64.
      vii) Protocols for recordkeeping during an incident which specify that records should be complete, specify all actions taken, time of action, person, tools used, and be immutable, e.g. written in a bound notebook
      viii) Mitigation plans
      ix) The criteria for shifting from incident response to data recovery should be defined
      x) Playbooks for each scenario identified. Playbooks should include
         (1) Containment steps
         (2) Eradication steps
   c) **Security Incident Response Tests.** The Incident Response Team may conduct security incident tests, such as table-top exercises, to communicate and train staff on the agency's incident response plans and to develop skills, improve the plans, and improve performance in the event of a serious security incident.
2) **Security Incident Reporting and Response Procedure**
   a) **Reporting Security Incidents.** Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
   b) **Response Procedure.** The HIPAA Security Officer and/or Incident Response Team will respond high priority incidents.in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Standard 4030 Breach Reporting and Standard 1080 Reporting Violations and Security Incidents, Standard 4040 Mitigation will be followed as appropriate. The Superintendent of the Agency will be notified and any contingency plans will be activated.
   c) **Documenting Security Incidents.** In conjunction with the HIPAA Security Officer, a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include:
      i) Date and time of report
      ii) Date and time of incident

iii) Description of circumstances
iv) Corrective action taken
v) Mitigating action taken

Documentation will be kept for 6 years.

3) **Post-Incident Analysis.** The HIPAA Security Officer and/or Incident Response Team will conduct a post-incident analysis to identify the root cause, to evaluate the organization's safeguards, and the effectiveness of response. The analysis should recommend appropriate corrective action to address the root cause and to improve the incident response process..

5050 Facility Security and Access Control

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

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(a)(1) Physical Safeguards-Facility Access Controls
NIST CSF GV.RR-04, PR.AA-06, DE.CM-02

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

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

REFERENCES
NIST SP 800-66 Rev. 2

5060 Vulnerability Management and Evaluations

STANDARD
The agency should manage vulnerabilities of its network, use appropriate threat intelligence, conduct annual evaluations of its security program, and take appropriate corrective action.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(8) Administrative Safeguards-Evaluation
ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-06, ID.RA-08, ID.IM-01, ID.IM-02, ID.IM-03

PROCEDURES
1) **Vulnerability Management**. The organization should execute an appropriate vulnerability management program for its network which may include
   a) Periodic and/or continuous network scanning, including external and internal authenticated scans. Periodic evaluation of any cloud security posture should be conducted.
   b) Remediation. Vulnerabilities shall be reviewed and responses chosen, prioritized, planned, tracked, and communicated.
   c) Operating procedures should be developed with metrics and standards for timeliness of remediation based on priority.
2) **Threat intelligence**. Appropriate threat intelligence shall be used. This may include
   a) Monitoring of alerts from vendors in the technology stack used by the company,
   b) Participation in the MS-ISAC,
   c) Monitoring alerts from U.S. government agencies including CISA and HHS OCR, and/or
   d) Dark web scanning.

   Threat intelligence shall be communicated to the appropriate team and/or individual for action
3) **Periodic Evaluations.** On at least an annual basis, an evaluation of the technical infrastructure and/or the organization's compliance with computer security regulations/standards will be conducted. From year to year, type of evaluation(s) may vary and will be selected by the HIPAA Security Officer. Appropriate evaluations may include
   a) Penetration tests
   b) Social Engineering exercises/tests
   c) IT Asset audits to identify missing assets
   d) Audits of policies, procedures, and standards for compliance with the following standards/regulations
      i) HIPAA
      ii) CARF
      iii) FERPA/IDEA
      iv) NIST CSF
      v) State laws
   e) Audits of compliance with policies, procedures, including verification that the processes, procedures and documentation specified in the policies exist, and that the responsible personnel understand the policies

   Evaluations may be done more frequently, if determined by the Security Officer.
4) **Corrective Action.** The HIPAA Security Officer shall take appropriate corrective action based on results of evaluations and security tests.

5070 Audit Control and Activity Review

STANDARD

Appropriate network security monitoring shall be conducted for all systems and environments identified by the HIPAA Security Officer. Monitoring may be conducted in-house and/or outsourced to third-party Managed Security Service Providers. Best practices shall be followed in specifying the audit logs to be monitored. Appropriate protocols shall be in place to support incident response and forensic analysis.

AUDIENCE

HIPAA Security Officer

AUTHORITY

HIPAA Privacy and Security Rules, 45 CFR § 164, 45 CFR 164.312(b) Technical Safeguards-Audit Controls
45 CFR 164.308(a)(1)(ii)(D) Administrative Safeguards -Information System Activity Review
45 CFR 164.308(a)(5)(ii)(C) Administrative Safeguards -Log-in Monitoring
NIST CSF PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-09, DE.AE-03, DE.AE-07, RS.AN-07

PROCEDURES

1) **Applicable Systems and Environments**. The HIPAA Security Officer should identify systems and environments for which a network security monitoring program shall be implemented. This identification shall be based on the nature and quantity of ePHI and/or other important information, contractual requirements, and best practices.
2) **Network Monitoring/Response Capability**. The HIPAA Security Officer should implement an appropriate managed detection / managed response capability. Specific features of the monitoring capability should be selected based on risk assessment, and may include:
    a) Scanning for activity in the MITRE ATT&CK Chain
    b) Monitoring is integrated with cyber threat intelligence
    c) Use of a Security Operations Center (24x7)
    d) Comprehensive collection and analysis of logs with correlation
    e) Pre-defined playbooks with automated containment responses
3) **Assets to Monitor**: The specific activity to monitor shall be based on risk assessment, and may include:
    a) Logs and alerts from third-party IT assets:
        i) Cloud environments
        ii) Firewalls
        iii) Peer-to-Peer activity
        iv) Server operating system security events
        v) DBMSs
        vi) Identity and Access Management facilities
        vii) Web, file, and application servers
        viii) Other system software applications
        ix) End-User workstations

        The audit logs for the above IT assets shall be configured based on best-practice guidelines from authoritative sources.
    b) Human sources, such as end-user ticketing, help desk systems, and help desk phone calls
4) **Synchronization.** IT assets shall be synchronized to an authoritative time server.
5) **Incident Response**. The network monitoring protocol shall serve as an input to the incident response capability as detailed in Standard 5040 Security Incident Response.
6) **Audit Log Security**. Audit logs shall be appropriately protected and secured to ensure availability for forensic investigations.
7) **Log Retention**. Record retention time frames for audit logs shall be determined by risk assessment and contractual obligations.
8) **Audits of PHI Access**. The agency should design an audit strategy to identify probable or anticipated access violations by employees. Specialized auditing software may be used to audit activity logs.

5080 Malicious Software Protection

STANDARD
All Agency IT assets shall be protected using a multi-layered anti-malware strategy.

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5) Administrative Safeguards-Security Awareness and Training
NIST CSF PR.PS-05, DE-CM-09

PROCEDURES
1) Centrally managed endpoint protection software shall be used on all servers and workstations.
2) Anti-malware capabilities shall be used to protect email systems.
3) An appropriately configured, commercial-grade firewall shall be used to protect internal networks (per Standard 5150 Technical Safeguards). Any firewalls should be configured to use a DNS filtering service to limit connections to malicious sites, phishing attacks, and botnets.
4) Zero-trust principles may be employed using tools to implement Secure Access Service Edge (SASE), Cloud Access Security Brokers (CASB) and related technologies when appropriate based on risk assessment.

5090 Change Management

STANDARD
The organization shall maintain a change management process to ensure the proper operations of applications, to prevent security failures, and to ensure high reliability of the agency's IT facilities.

AUDIENCE
HIPAA Security Officer

REFERENCE
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR 164.308(a)(1)(ii)(B) Administrative Safeguards - Risk Management
NIST CSF ID.RA-07

PROCEDURES
1) **Change Management Process**. A formal change management process should be used, to include business justification for the change, assessment of potential impacts (including a security risk assessment), QA checklists, a formal approval process, communication of change details to all relevant persons and formal documentation/audit trail of changes.
2) **Change Pathways**. Different pathways may be established defining the process for different categories of changes. Different categories could include trivial/routine changes, more significant changes (e.g. ITIL "normal" changes), and emergency changes.
3) **Separation of duties**. Formal workflows will incorporate the principle of separation of duties in the change process so that the initiation of a change request is separated from its authorization.
4) **Test and Production Environment**. Separate test and production environments shall be maintained:
    a) The test environment should be configured exactly the same (or as close as possible) as the production environment, and
    b) Test data shall not contain PII or PHI.
5) **Testing Protocols**. Testing protocols are maintained for various types of changes to allow for efficient and comprehensive testing.
6) **End-user Documentation**. When relevant, the change process includes an update of end-user documentation.
7) **Fallback Procedures**. For any proposed change, fallback procedures are developed in advance, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
8) **Change Management Window**. The organization shall maintain a change management window for changes which impact system users.
9) **Operating Procedures**. Written operating procedures are maintained including approval forms, identification of sign-off responsibilities, change management windows, workflows and documentation.

REFERENCES
ITIL
ISO 27002:2022
5.22 Monitoring, review and change management of supplier services
8.32 Change Management

5100 Device and Media Management

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

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(d)(1) Physical Safeguards-Device and Media Controls

PROCEDURES
1) **Media Disposal Handled by HIPAA Security Officer**. As specified in Standard 1100 Acceptable use of IT Assets, Agency employees are prohibited from storing Protected Health Information of the Agency's on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.
2) **Accountability**. The Agency shall properly account for any physical media which is maintained by the Agency to store electronic PHI. A record of the movement of the media and associated hardware shall be maintained to clearly document the chain of custody.
3) **Technical Guidance**. In accordance with instructions from the Secretary of HHS, technical guidance regarding media disposal should be obtained from *NIST SP 800-88 Guidelines for Media Sanitization Rev. 1*. The Agency requires that at a minimum, data from electronic media should be "cleared", as defined in the referenced NIST documentation.
4) **Media Disposal and Re-use**. Procedures vary based on type of storage media:
    a) **Cloud Environments**. The HIPAA Security Officer shall obtain technical guidance from any cloud vendors regarding appropriate procedures for data sanitization. Protocols specified by vendor shall be followed as part of asset destruction to ensure sanitization of discarded assets is performed. Satisfactory assurances shall be obtained from vendor that the technical guidance is accurate.
    b) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
    c) **Hard Drives and floppy disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
    d) **Other Media**. See NIST SP 800-88 Rev. 1 for disposal/recycling methods for other media.
    e) **Notes**. Photocopiers, printers and other office equipment may include media subject to this provision!
5) **Records.** Records of Media disposal should be maintained in accordance with agency policy. When using third parties to perform media sanitization, a Certificate of Destruction shall be obtained.

5110 Encryption and Key Management

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

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR §164.312 (c), (d) and (e) Technical Safeguards-Integrity, Authentication and Transmission Security
45 CFR §164.312(a)(2)(iv) Technical Safeguards -Encryption and Decryption [of data at rest]
NIST CSF PR.DS-01, PR.DS-02

PROCEDURES
1) **Encryption of Data at Rest**. Data at rest shall be encrypted using appropriate standards:
   a) **Servers and Cloud Environments**. Servers and cloud environments storing PHI at rest shall be encrypted using current standards:
      i) Cyphers shall be compliant with ISO/IEC 19790:2025 - Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules.
   b) **Desktop, Mobile Devices and Portable Media**. When encryption of end-user devices is determined appropriate based on risk analysis, JCBDD shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, the Agency:
      i) should consider solutions that use existing system features (such as operating system features) and infrastructure
      ii) should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments
   c) **Keys and Key Management**.
      i) **Encryption Keys**. The HIPAA Security Officer shall ensure appropriate management for all encryption keys including those for cloud environments, servers, DBMS, backup media, desktop and mobile devices and other data assets.
      ii) **Key Management**. Key management best practices shall be used for key assignment, backup, rotation, and destruction as detailed in NIST SP 800-57 Part 2 and NIST SP 800-57 Part 3.
      iii) **Exceptions**. The HIPAA Security Officer may authorize exceptions to key management best practices, based on risk assessment. Any exceptions shall be documented.
2) **External Data in Motion**. For any data transmitted via the internet, JCBDD systems shall use a securely configured transmission protocol that provides both encryption and message integrity.
   a) Acceptable transmission protocols include:
      i) Web Access: TLS 1.2 (HTTPS)
      ii) File Transfer: FTPS, SFTP, SCP, WebDAV over HTTPS
      iii) Remote Shell: SSH2 terminal
      iv) Remote Desktop: radmin
   b) Secure configuration. Protocols shall be configured appropriately.
      i) Any encryption algorithms used must be compliant with ISO/IEC 19790:2025 Information technology – Security Techniques – Security requirements for cryptographic modules.
      ii) The Secretary of HHS's guidance (which provides a safe harbor) is may be used. The HHS guidance specifies the use of one of these standards:
         (1) NIST 800-77, *Guide to IPsec VPNs*,
         (2) NIST 800-113, *Guide to SSL VPNs*
   c) Exceptions. RDP may be used as a Remote Desktop Protocol only with the explicit approval of the HIPAA Security Officer who shall document the rationale for permitting the exception.
3) **Wireless Networks**. Wireless networks in JCBDD facilities and/or employee home offices will be implemented with the following security options:

a) The beacon shall be enabled
b) The SSID should be changed from the default
c) WPA2 should be enabled
d) WPS should be disabled
e) MAC filtering should be employed to allow access only to workstations owned by JCBDD and authorized to use the network.
f) These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
g) The administrator account shall be changed and protected with a strong password (see Standard 5120 User Account Management).

5120 User Account Management

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

AUDIENCE
HIPAA Security Officer
Technical Staff

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR §164.312(a)(2)(i) Technical Safeguards - Unique User Identification
45 CFR §164.312(d) Technical Safeguards - Person or Entity Authentication.
45 CFR §164.308(a)(5)(ii)(D) Administrative Safeguards - Password Management
NIST SP 800-63B Digital Identity Guidelines – Authentication and Lifecycle Management
NIST CSF PR.AA-01, PR.AA-02, PR.AA-03

PROCEDURES
1) **Identification**.
   a) **General Rule**. Each individual requiring access to an IT asset shall be given their own, unique account ID which serves to identify them to the application, system, or device. The organization may manage user identities centrally using an identity and access management system or may use separate identity management systems.
   b) **Exceptions where Shared Accounts are Allowed**. For IT assets or vendors (e.g., a Domain Name Registrar) which do not support multiple accounts, the HIPAA Security Officer may authorize a shared account. In such cases, passwords may be shared. The HIPAA Security Officer shall document these exceptions including the individuals who have access to passwords.
2) **Password Security –Rules for User Accounts**. Password security procedures will vary based on account type. These requirements apply for all User Accounts, that is, accounts used by human beings.
   a) Password length – passwords must be a minimum of 6 (six) characters for handheld devices 12 (twelve) for network and cloud applications.
   b) Password complexity. Passwords must include upper-case and lower-case letters, and digits. Passwords may also include special characters. Longer "passphrases" of 20+ characters are recommended (a passphrase is a sequence of 3 or more words).
   c) Not guessable. The password must not be related to the person in any way, as in a birth date, spouse name, pet name, or anything which can be easily guessed.
   d) Mandatory periodic password changes shall not be required. Mandatory changes shall be required for all users if there is evidence or suspicion of compromise.
   e) When changing passwords, previously used passwords must not be recycled.
   f) Different passwords must be used for each account.
   g) When specifying answers to vendor security questions (for use with password reset requests) it is best to select questions whose answers cannot be easily discovered.
3) **Multi-Factor Authentication (MFA)**. Multi-factor authentication MUST be enabled for any sensitive systems and/or production environments. It should be enabled for any service or capability which supports MFA. The preferred method for MFA is a hardware token or authenticator app such as Google Authenticator. Text messaging-based MFA is permitted with approval of the HIPAA Security Officer.

FOR THE HIPAA SECURITY OFFICER
1) **Mandatory Password Changes with Evidence of Credential Compromise**. If there is evidence of malicious activity for an IT Asset, for example, if notified of a data breach by a cloud vendor which hosts one of the

organizations applications, the HIPAA Security Officer shall ensure that all users change passwords for the application at risk.

2) **Password Vault / Password Manager**. The Agency may use a password vault and/or password manager for maintaining login credentials. The Password Vault / Password Manager shall be included as a critical system for the DR Plan as detailed in Standard 5030 Disaster Recovery and Business Continuity Plans.
3) **Password length**. Whenever possible for an IT asset, password length must be enforced by the system:
   a) Six (6) characters for handheld devices,
   b) ten (10) for network-connected devices,
   c) sixteen (16) for user accounts with elevated privileges, for example, those with Domain Admin or cloud system administration privileges (see Standard 5130 Privileged Account Management).
4) **Enforcing Password Complexity**. Whenever possible with an IT asset, password complexity must be enforced by the system:
   a) For assets which do not support NIST SP 800-63B, complexity is specified as requiring at least 1 upper case letter, 1 lower case letter, and 1 digit.
   b) NIST SP 800-63B guidelines are preferred for enforcing complexity when an IT asset supports this method. However, the Agency requires that the user supply an initial password which conforms to the length requirements above. (The NIST SP 800-63B guidelines specify a protocol for validating a user-supplied password against a database of prohibited passwords compiled from large breach corpuses, dictionaries and repetitive sequences.)
5) **Password History/Recycling Prohibited**. Whenever supported by systems, they shall maintain a history of the most recent 13 passwords. Assets shall be configured to prohibit password recycling.
6) **Maximum Login Attempts**.
   a) Whenever supported by applications, systems or devices, the asset shall be configured to permit only 5 attempts to enter a correct password, after which the User ID should be locked and/or deactivated.
   b) Both end-users and the HIPAA Security Officer shall be notified of the incident which shall then be investigated.

5130 Privileged Account Management

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

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

AUDIENCE
HIPAA Security Officer
Superintendent
System Administrators

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR §164.308(a)(5)(ii)(D) Administrative Safeguards - Password Management

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

PROCEDURES
1) **Approval of Privileged Accounts**. Privileged Accounts must be strictly controlled:
   a) The creation or modification of User Accounts with Elevated Privileges must be approved by at least two individuals: The HIPAA Security Officer or designee and the Superintendent or designee.
   b) The number of User Accounts with Elevated Privileges must be strictly limited to individuals with an authorized business need.
2) **Normal Privilege Accounts**. All users must be given an account without Elevated Privileges for routine work such as email access and web browsing, which must be used whenever the elevated privileges are not required.
3) **User Accounts with Elevated Privileges – Password Rules**. Requirements for passwords for User Accounts with Elevated Privileges detailed in Standard 5120 User Account Management shall apply, with the following modifications:
   a) The minimum length for a Password of a User Account with Elevated Privileges is 16 (sixteen) characters.
   b) Whenever possible, User Accounts with Elevated Privileges must be defined using role-based account privileges to limit privileges to the specific requirements.
   c) Any User Account with Elevated Privileges used by a 3rd party contractor must have an expiration date.
   d) Default passwords must always be changed.
4) **Privileged System Accounts—Password Rules**. Passwords for Privileged System Accounts, which are not used by humans, shall be optimized for security:
   a) The length shall be based on the maximum length for each platform (e.g., 256 for Windows)
   b) Should be a computer-generated random mix of characters including upper case, lower case, digits, and symbols
   c) Shall not use passphrases and should not be memorized
   d) The computer generation must use an unpredictable seed (e.g., the low order bits of system clock time)
   e) Null passwords are always prohibited
   f) Any 3rd Party application with privileged account must have an expiration date
   g) Whenever possible, Privileged Accounts must be defined using role-based account privileges to limit privileges to the specific requirements for the task.

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

5140 Control of Remote Access

STANDARD
The agency shall ensure effective control of remote access to its information systems.

AUDIENCE
HIPAA Security Officer

REFERENCE
HIPAA Privacy and Security Rules, 45 CFR § 164
164.308(a)(3) & (a)(4) Administrative Safeguards -Workforce Security and Information Access Management
164.312(a) Technical Safeguards - Access Control, Unique User Identification, Emergency Access Procedure, and Automatic Logoff

PROCEDURES
1) **Remote Access Standards**. the agency approves the following connection methods for remote access to its system:
   a) **Protocols**. Acceptable transmission protocols include:
      i) Web Access: TLS 1.2 (HTTPS),
      ii) File Transfer: FTPS, SFTP, SCP, WebDAV over HTTPS,
      iii) Remote Shell: SSH2 terminal, and
      iv) Remote Desktop: radmin.
   b) **Secure configuration**. Protocols shall be configured appropriately:
      i) Any encryption algorithms used must be compliant with ISO/IEC 19790:2025 Information technology – Security Techniques – Security requirements for cryptographic modules.
      ii) The Secretary of HHS's guidance (which provides a safe harbor) is may be used. The HHS guidance specifies the use of one of these standards:
         (1) NIST 800-77 Rev. 1, *Guide to IPsec VPNs*,
         (2) NIST 800-113, *Guide to SSL VPNs*
      iii) SSH2 shall be configured using principles specified at https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2016-01.pdf
2) **Remote Access Tools**. The organization may identify approved tools for use by employees and contractors which conform to the standards above.
3) **Authorization**. Any end user access to the organization's systems by an employee or third-party contractor using a remote connection must be authorized as detailed in Standard 3010 Access Control.
4) **Exceptions**. Any exceptions to the organization's remote access standards must be explicitly authorized by the HIPAA Security Officer. All exceptions shall be documented.

5150 Technical Safeguards

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

AUDIENCE
HIPAA Security Officer

AUTHORITY
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(c) Technical Safeguards - Integrity
45 CFR § 164.312(d) Technical Safeguards – Person or Entity Authentication
45 CFR § 164.312(e) Technical Safeguards – Transmission Security
NIST CSF PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, PR.IR-02, PR.IR-04

PROCEDURES
1) **Agency networks and hosting environments** used by JCBDD shall be secured using the following controls:
   a) **Firewalls.** Appropriate firewall technology shall be employed to protect networks and applications, and may include traditional, next-gen, and web application firewalls. These shall be configured based on best-practice recommendations from authoritative sources.
   b) **Network Segmentation**. The network should be appropriately segmented.
   c) **DNS Filtering** with a secure DNS service (e.g. OpenDNS) shall be employed.
   d) **Software Patching**. Hardware firewalls and network gear, hypervisors, operating systems, DBMSs, other system software and application software shall be patched on a timely basis:
      i) A written protocol specifying software and equipment to be monitored, responsible individuals, prioritization process, patching timelines, change management considerations, and management reporting shall be developed.
      ii) Third-party code. For any custom applications maintained by JCBDD, any third-party code included in the custom applications shall be monitored for security updates. Custom applications shall be updated on a timeline based on risk assessment.
   e) **Hardening**. A written protocol for asset hardening shall be developed and followed. This protocol shall specify baseline security configurations for assets in the technology stack including but not limited to cloud environments, firewalls, operating systems, DBMSs, web servers, load balancers, programming languages, end-user application software, network gear, IOT devices, and other technologies used. Configurations published by authoritative sources such as NIST, the Defense Information Systems Agency, Center for Internet Security, or other authority cited in the National Checklist Program (NCP) shall be employed.
   f) **Virtualization Software and environment**. Virtualization-enabling software, aka "hypervisors", shall be secured as follows:
      i) unneeded capabilities shall be disabled to reduce potential attack vectors
      ii) A strong password (see Standard 5130 Privileged Account Management).
      iii) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's
      iv) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations
      v) Use separate logon credentials for each virtual server
   g) **Resilience.** Networks and computing capabilities should be designed and/or selected for resilience, including:
      i) Fault-tolerant hardware
      ii) Redundant servers and/or high-availability configurations such as mirrored database clusters
      iii) Redundant internet connections with automatic failover when the primary is down
      iv) Partners / third-party service providers who provide high-availability services
2) **E-mail**. The agency will maintain and properly configure both standard email and secure, encrypted email:
   a) **Standard Email**. Standard Email shall be securely configured:
      i) TLS shall be enabled to encrypt all communications between email clients and the server

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

b) **Secure Email**. For transmission of PHI, the agency will maintain the capability for end-to-end encryption:
i) If the agency uses desktop or smartphone email clients, the agency email system should be configured to use TLS encryption between the email client and the email server to ensure that email between employees is encrypted, and/or
ii) Using a reputable vendor who provides end-to-end encryption which allows an employee to force end-to-end encryption when required, and/or
iii) Entering agreements with frequent correspondents to each configure email systems to force TLS encryption both i) between end user and email server and ii) between sender email server and recipient email server.

3) **Workstation Security**. Workstations shall be secured with multiple levels of security:
a) **Anti-malware software**. Anti-malware software shall be enabled as detailed in Standard 5080 Malicious Software Protection.
b) **Patching**. Operating system and end-user application software shall be patched and included in the written protocol detailed in the "Software Patching" section above.
c) **Timeout/Screenlock**. Automatic timeout and/or screenlock shall be enforced on all workstations. The timeout period shall be set based on risk assessment.
d) **Hardening**. The hardening protocol for end-user workstations shall include the following controls:
i) Operating systems, web browsers, and major application software including Adobe and Microsoft Office shall be configured with security settings from an authoritative source, and
ii) USB ports shall be configured to disable externally mountable media for all production profiles. This may be overridden only with the express approval of either the CTO or the HIPAA Security Officer.

4) **Appropriate Audit Controls in JCBDD-Used Software**. Software used by JCBDD should be evaluated for the appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements should be made as appropriate. Appropriate audit controls should be criteria for continued use of and/or procurement of any new operating or application software.

5) **Integrity Checks**. The HIPAA Security Officer shall attend to integrity of electronic data:
a) Periodic DBMS maintenance as recommended by the software vendor shall be performed.
b) Message digest integrity reports shall be reviewed with corrective action taken as necessary.

6) **Software utilizing Electronic Signatures**. The HIPAA Security Officer will review and approve any software that offers electronic signature capability prior to implementation at the Agency. The HIPAA Security Officer shall be responsible for implementation and ongoing monitoring/auditing of the software as specified in Standard 5170 Electronic Signatures.

5160 Technical Controls for Mobile Devices

STANDARD
The agency will appropriately manage all agency-owned and personally-owned mobile devices.

AUDIENCE
HIPAA Security Officer
IT Staff

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

PROCEDURES
1) **Setup Procedures.** The IT department will maintain appropriate procedures for configuring, onboarding and/or enrolling agency-owned and any personally-owned mobile devices.
2) **Mobile Device Management.** The Agency should use an appropriate mobile device management capability. The following features and controls should be considered:
   a) Maintenance of an accurate inventory of devices,
   b) Enforced security configurations including at a minimum the use of a passcode/PIN and to encrypt,
   c) Ability to perform remote wipe/lock,
   d) Ability to perform geo-location,
   e) For personally-owned devices the ability to segregate personal information from the organization's information,
   f) Ability to implement anti-malware, and
   g) Ability to implement other controls identified by risk assessment.

5170 Electronic Signatures

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

AUDIENCE
Employees Using Electronic Signatures; Managers

AUTHORITY
ORC § 1306 Ohio Uniform Electronic Transactions Act
ORC § 304 Electronic Records and Signatures for Counties
ORC § 9.01 Official Records – Preserving and Maintaining
ORC § 117.111 State Audits Shall Review Method, Accuracy and Effectiveness of Electronic Signature Security Procedures

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

PROCEDURES
1) **Security**
   a) **Confidentiality statement**. Anyone authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature/ logon password, that the electronic signature will be legally binding and that passwords will not be shared and will be kept confidential.
   b) **Passwords**. All users will have their own user ID and password. Passwords must conform to complexity guidelines detailed in Standard 1100 Acceptable use of IT Assets.
   c) **Personal Identification Numbers (PIN)/ Secondary Passwords.** PIN numbers and/or secondary passwords may be assigned when possible for use with electronic signatures to allow for another level of security (this is optional and county specific). PIN numbers or secondary passwords are not viewable on any screen.
   d) Vendors, outside agency or providers who have access to using an application requiring an electronic signature based upon the user's ID and password as described in this standard, shall use additional controls to ensure the security and integrity of each user's electronic signature:
      i) Follow loss management procedures to electronically de-authorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information and use suitable, rigorous controls to issue temporary or permanent replacements;
      ii) Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
      iii) Test or use only tested devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.
2) **Creating, Maintaining an Electronic Signature**
   a) Electronic signatures can be used wherever handwritten signatures are used except where stated by a specific law or rule.
   b) All who use a system that uses electronic signatures are required to review their entries.
   c) Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of addendum to the original entry. The addendum should also be signed electronically, and date/time stamped by the computer software.

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

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

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