Carroll County Board of Developmental Disabilities

HIPAA Privacy, Confidentiality & Security Policies & Procedures

Table of Contents

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 CarrollCBDD
4) **Applicable Requirements –** Applicable requirements mean applicable federal and Ohio law and the contracts between the CarrollCCBDD and other persons or entities which conform to federal and Ohio Law.
5) **Authentication –** means the corroboration that a person is the one claimed.
6) **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.
7) **Breach –** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information.
    a) Breach *excludes*:
        i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.
        ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.
        iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
    b) Except for the exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:
        i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
        ii) The unauthorized person who used the PHI or to whom the disclosure was made;
        iii) Whether the PHI was actually acquired or viewed; and
        iv) The extent to which the risk to the PHI has been mitigated.
8) **Business Associate (BA) –** A Business Associate, basically, is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The complete definition is included in Appendix A - Identifying Business Associates.
9) **CarrollCBDD –** Carroll County Board of Developmental Disabilities
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 receives services from the Agency. Note that parents or minors, guardians and other "personal representatives" may exercise any right or privilege available to an Individual served.
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 either perform or refrain from performing 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 of DODD, to Individuals served.
        ii) Activities undertaken by the Agency to provide reimbursement to contracted providers for services provided to Individuals served.
    b) The activities in paragraph (A) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:
        i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
        ii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

iii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
iv) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

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 CCBDD 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 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) **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.
47) **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.
48) **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.
49) **Security or Security measures –** encompass all of the administrative, physical, and technical safeguards in an information system.
50) **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.
51) **Shall** – means the individual or entity is required to either perform or refrain from performing the following action. See also "Must".
52) **Should** – means the individual or entity is recommended to perform the specified task, even though the task may not be required.
53) **Social Engineering –** means "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information, he needs to gain access to the system" or "getting needed information (for example, a password) from a person rather than breaking into a system" . … social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
54) **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.
55) **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
56) **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers. This definition includes the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
57) **TPO –** TPO means treatment, payment or health care operations under HIPAA rules. For the purposes of this policy manual, TPO shall also include "Education" as defined above.
58) **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.

59) **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.
60) **User –** means a person or entity with authorized access.
61) **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.
62) **Workforce Member –** Workforce Member means the same as Employee. See definition above.
63) **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 Confidentiality – General Rules

POLICY
All information in an enrollee's records, including electronic information, is confidential. Further, all conversations involving individually identifiable information is confidential.
CarrollCBDD will strive to conform to 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. CarrollCBDD will not use or disclose individually identifiable information except in accordance with applicable requirements.

PROCEDURES
1) Staff of CarrollCBDD 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 for Agency purposes for serving Individuals. In an exception, explicit parent authorization is required for any Medicaid billing for children.
   b) In accordance with a release or authorization.
   c) As permitted in Policy 1040 Speaking with the Family or Friends of an Individual Receiving Services.
   d) As permitted by in Policy 1090 Disclosures that do Not Require an Authorization.

2) For all of the above, the minimum amount of information should be disclosed.

3) All employees are responsible for safeguarding the information regarding Individuals served by CarrollCBDD, whether oral or written including social media, portable computing devices and employee work at home.

1020 Minimum Necessary Policy

POLICY
The use and disclosure of PHI must be limited to the minimum necessary to satisfy the request or to complete the task, except in situations specifically identified by the HIPAA rules.

PROCEDURES

- When using or disclosing PHI, or when requesting PHI from another entity, employees must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- Disclosures to medical, vocational, residential and other providers, and service coordination with other agencies are "treatment" and not part of Minimum Necessary procedures.

Exceptions. The minimum necessary requirement does NOT apply to:
(1) Disclosures to or requests by a health care provider for treatment
(2) Uses or disclosures made to the Individual served, including but not limited to any requests for their records or requests for an accounting of disclosure
(3) Uses of disclosures made pursuant to an Authorization
(4) When the disclosure is required by law, is to the Secretary of HHS, or for compliance with HIPAA regulations.

Identified Routine Disclosures or Requests

1) **Software & Network Providers** – Information in the computer system is incidentally available during system support activities.
   A) **Superior Technology Group.** Support vendor Superior Technology is under contract to provide support for hosted computer servers. Access is provided at all times.
   B) **Brittco and other Support.** Brittco and other support vendors will be granted access rights on an as needed basis. Access is enabled only when support is needed.
   C) **IT Support.** The Tuscarawas County Board IT Specialists has 24/7 access to the computer network and servers for IT Support purposes.
   D) **Document Imaging Support.** Vendor GBS is provided access, when required, for technical support.
   E) **Family Office Equipment.** PC repair services. PC is dropped off for service/repair.
2) **Prosecutor's Office**. When a warrant or subpoena is presented, any file may be released to the Prosecutor's Office. In addition, if the Agency is seeking legal counsel, file contents to be revealed will comply with the minimum necessary standards.
3) **Auditor's Office –** When authorizing payment of bills, fiscal files may be reviewed by the Auditor's office prior to authorization of payment.
4) **Ohio DODD –** Information will be shared routinely with Ohio DODD including TCM. Specific to MUI case files, the Investigative Agent and internal UI staff will utilize the Ohio DODD's secure website to input required information. As Ohio DODD accreditation comes on-site, any requested information will be provided.
5) **Ohio Department of Education/ Department of Children & Youth -** During accreditation, inspectors come on-site. Any school records requested will be provided. Transportation and Child Count data is uploaded to ODE secured website.
6) **County School Districts –** Individual information will be shared.
7) **Bureau of Disability Determination (OOD) –** Using the Bureau's forms, assessment information will be shared in order to determine Individual's eligibility for benefits. Sent via secure email by SSA.

Procedures for Routine Requests of PHI

1) **Eligibility Inquiry** – Individual insurance eligibility will be verified by using procedures provided by the Ohio Dept of DD.
2) **County School Districts** – Referrals are received from school districts.

1030 Confidentiality Safeguards (Verbal & Written)

POLICY
CarrollCBDD will utilize appropriate physical, technical, and administrative safeguards to safeguard Paper and Verbal PHI.

PROCEDURES

1) **General Procedures**
   a) Employees shall be familiar with Policy 3015 - Facility Security and Access Control and plan regarding staff, Individuals receiving services and all other access to the facility.
   b) All employees of CarrollCBDD will be required to sign a Confidentiality Agreement upon employment.
   c) Visitors will be required to sign-in. Employees will work together as to not permit visitors to freely roam throughout the premises.
2) **Verbal Conversation Privacy**
   Employees should be aware of their surroundings and use appropriate volume when involved in a verbal conversation in person or via a phone so as to not divulge an individual's PHI to bystanders. Discussions concerning Individuals should be done in a private area and abide by the Minimum Necessary Policy.
3) **Safeguards for Written PHI**
   a) **Control of Paper Records**
      i) Adult and Student records will be kept locked and secured.
      ii) Paper files shall be put away when not being used.
      iii) Original paper records shall not be removed from the building without the authorization of the Superintendent.
      i) Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer.
   b) **Printing and Copying PHI**
      i) PHI printed to a shared printer or copied should be promptly removed.
      ii) In the event that a printer/copier includes an internal storage device, which retain images of photocopies made, the storage device of the printer/copier asset shall be managed by the IT department for destruction upon disposal.
   c) **Transportation/outside use of documents with PHI**
      i) Caseworkers and other employees who remove documents from the facility, are responsible for safeguarding these documents. This includes locking a vehicle when leaving documents unattended in the vehicle. The documents should be in their container, not visible.
   d) **Visibility of records and other PHI**. All employees using records for Individuals and other paperwork with PHI should arrange these items so that PHI is not readily visible to visitors.
   e) **Shredding**. Unneeded paper documents containing PHI will be destroyed by shredding.
   f) **Clean Desk Policy.** All employees should clean their desks of PHI whenever leaving their work area for a time, especially at end-of-day.

4) **Compliance Audits/Facility Review**. Periodically, the HIPAA Privacy Officer or designee will conduct a walk-through of the facilities noting and discussing with the appropriate staff the observations of the placement of desks, location of computers, monitors and papers consisting of PHI that would be openly visible to a visitor.

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

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

PROCEDURES
1) **If the Adult Individual is present**
    a) **Permitted disclosure to family or friend present**. If a family member, or friend of the Adult 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 Adult Individual is not present**
    a) **Communications about the Individual's care**
        i) In the event of a phone call or other discussion with a family member or one involved with the care of the Individual being served by CarrollCBDD, where the Individual is not present, the employee may use their professional judgment to determine if the disclosure is in the best interests of the Individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Individual's care.
    b) **Notifications**
        i) An employee may disclose PHI to notify a family member, guardian or the responsible care giver the Individual’s location or general condition.

1050 Authorizations

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

LEGAL NOTES
- FERPA applies for records created for education; HIPAA applies to all other records. The term used in the FERPA regulations is "consent". The HIPAA term "authorization" is used in these policies.

PROCEDURES

Valid Authorization. Unless otherwise authorized by CarrollCBDD policy and/or state or federal law, release of an Individual's records requires specific authorization by the Individual being served or his/her legal representative. A standard authorization form is included as an Appendix.

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

Proper Completion of Authorization Form by Staff.
a) The staff person handling the request will complete the Authorization Form in its entirety including annotating the bottom of the form.
b) The original signed authorization will be saved in the Individual's master record, and a copy must be given to the Individual.
c) Using the Disclosure Log, a record of the release will be maintained.
d) If an Individual's records Include the name of another Individual served by CarrollCBDD (such as an MUI report), the other Individual's name must be redacted prior to the release of the record.

Retention Period for Written or Electronic Copy of Authorization. The CarrollCBDD 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.

Revocation of Authorization. Upon instructions of revocation of authorization, CarrollCBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.

1060 Verification

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

PROCEDURES

1) **REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY**
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, CarrollCBDD 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.

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

1070 Minors, Personal Representatives and Deceased Individuals

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

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**. CarrollCBDD 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 CarrollCBDD Authorization Form which permits release of PHI.
3) **Recognized Personal Representative**. CarrollCBDD 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 CarrollCBDD a court order restricting the non-custodial parent's access.
    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 CarrollCBDD 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, CarrollCBDD may elect not to recognize a person as a personal representative of an Individual. In order for CarrollCBDD to choose not to recognize a person as a personal representative, CarrollCBDD must decide that it is not in the best interest of the Individual to treat the person as the Individual's personal representative and must believe that one of the following conditions exist:
            (1) The Individual has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative.
            (2) Treating such person as the personal representative could endanger the Individual.
        ii) Receipt of a court order limiting privileges of a non-custodial parent. In the event that CarrollCBDD 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, CarrollCBDD shall adhere to the restrictions in the court order.
4) **Deceased Individuals**
    a) **Disclosure of PHI After Death**. PHI generated during the life of an Individual is protected from disclosure after death unless disclosure is for treatment or payment, quality assurance or other auditing or program review functions. CarrollCBDD and its employees cannot release PHI regarding a deceased Individual unless a valid personal representative has been established and has requested the PHI through the proper authorization process.
    b) **Disclosure of PHI to Administer Estate**. Upon request, PHI shall be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate (ORC § 5126.044).
    c) **Disclosure to Guardian or next-of-kin:**. Upon request, the Agency shall release records regarding an Individual served to the guardian at time of death. Absent a guardian, records may be released to the next of kin:
        i) The Individual's Spouse (if married), Children, Parents, siblings, uncles or aunts, closest relative by blood or adoption, 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 Violations and Security Incidents

POLICY
Any employee who becomes aware of a violation of either confidentiality or computer security rules should immediately report the violation. Violations will be investigated and appropriate action will be taken.

PROCEDURES

1) **Employees Duty to Report Violation**. Any employee observing a violation of the Confidentiality and Computer Security policies is to report the violation to their supervisor.
2) **Investigation.** The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer will, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, Individuals receiving services, or others, and/or review of computer or paper audit trails.
3) **Procedure for Data Breach.** For potential data breaches, the Privacy and/or Security Officer will follow any procedures detailed in Policy 3035 Breach Reporting.
4) **Procedure for Privacy Violation.** For Privacy Violations, the Privacy Officer will follow procedures in Policy 3065 Mitigation.
5) A written incident report will be written by the Privacy and/or Security Officer. A copy of the report will be kept in the Privacy/Security Officer's files and the employee's personnel file. A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in policy, additional training, or other appropriate action.

1090 Disclosures that do not Require an Authorization

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

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

1) **Recordkeeping**. For all disclosures authorized below, details of the disclosure will be documented on the Disclosure Log which will be maintained in the adult or school record. Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.
2) **When required by law**
   a) To officials at another school that an Individual served by the 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.
   b) CarrollCBDD may use or disclose PHI or Education Records to the extent that such use or disclosure is required by 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 government authority authorized by law to receive reports of child abuse or neglect.
   c) The Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance.
   d) A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.
   e) To the extent that the CarrollCBDD receives PHI disclosed under this section in its role as LMAA, the CarrollCBDD may use the PHI to carry out its duties.
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 CarrollCBDD 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 CarrollCBDD 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 CarrollCBDD 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 CarrollCBDD 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 CarrollCBDD would be informing a personal representative, and the CarrollCBDD 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 CarrollCBDD, 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) To the extent that the CarrollCBDD receives PHI disclosed under this section in its role as LMAA, the CarrollCBDD may use the PHI to carry out its duties.
d) Education Records may be disclosed to the Comptroller General of the US, Attorney General of the US, Secretary of Education and/or State of Ohio Education authorities subject to the requirements of 34 CFR 99.35 or to state officials involved with juvenile justice in accordance with 34 CF 99.38.

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

7) **For judicial and administrative proceedings**
NOTE: These policies do not detail all situations such as grand juries and other infrequent legal proceedings. Consult with legal counsel prior to disclosure for any unusual situations! Also note that HIPAA and FERPA requirements are similar but different in some situations.
a) The CarrollCBDD 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 CarrollCBDD may comply with such legal requests only if:
i) The CarrollCBDD makes reasonable effort to notify the parent involved and/or receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the Individual who is the subject of the requested PHI has been given notice of the request; or
ii) The CarrollCBDD 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 CarrollCBDD will consult with legal counsel, prior to any response to a subpoena to ensure compliance with applicable requirements of HIPAA or FERPA.

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 CarrollCBDD may disclose to a law enforcement official protected health information that the CarrollCBDD believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the CarrollCBDD.
b) **Reporting Commission and Nature of Crime.** PHI may be disclosed to law enforcement personnel to report the commission and nature of a crime; The location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime. When responding to requests about the location of a suspect, fugitive, material witness, or missing person, the following PHI may be released:
i) Name and address
ii) Date and place of birth
iii) Social security number
iv) ABO blood type and RH factor
v) Type of injury
vi) Date and time of treatment
vii) Date and time of death, if applicable,
viii) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos
c) **Compliance/Enforcement of privacy regulations**: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

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

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

11) **To reduce or prevent a serious threat to public health and safety and/or safety of person(s)**
    a) The CarrollCBDD may disclose PHI or Education Records as follows, to the extent permitted by applicable law and ethical standards:
        i) **Good Faith.** PHI may be used or disclosed if the entity believes in good faith:
            (1) that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat; or
            (2) the disclosure is to law enforcement authorities to identify or apprehend an Individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.
    b) **Disclosure of Individual's Admitted Participation in a Violent Crime**. Disclosures of admitted participation in a violent crime are limited to the Individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.
    c) **Disclosure of Individual's Admitted Participation in a Violent Crime Learned in the Course of Treatment**. Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the Individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.
12) **Specialized government functions**
    a) **National Security and Intelligence**: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, Counterintelligence, and other activities authorized by the National Security Act.
    b) **Protective Services**: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
    c) **Correctional Institution or Law Enforcement Official.** The CarrollCBDD 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 CCBDD 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 "4.20 Protection of Whistleblowers".
14) **For workers' compensation or other similar programs if applicable**.
    a) PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

1100 Acceptable Use of IT Assets

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

PROCEDURES

1) **COMPUTER USE**
   a) **System is for Job Duties**. Computers, including use of internal systems, e-mail and the internet, are for use by employees to conduct and fulfill their job duties and responsibilities.
   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 on their own time – before/after work hours, during lunchtime. On occasion, brief access such as checking the weather is permitted. All CarrollCBDD owned computers must never be used for ANY activity that would be offensive or inappropriate. This includes any activity that would be sexual in nature, racist, profane, illegal activity, or operating a business.

   c) **E-Mail Use**. CarrollCBDD email accounts are to be used for CarrollCBDD purposes only. Using CarrollCBDD email accounts for personal use is strictly prohibited. In turn, personal email addresses must never be used for agency communications. Other policies when using e-mail:
      i) Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and must not be used to send Protected Health Information unless it is appropriately encrypted.
      ii) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in the CarrollCBDD Records Retention Policy.

   d) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to any unauthorized cloud service or removable media, such as flash drives 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.
   e) **All Usage is Logged**. CarrollCBDD reserves the right to monitor all usage of CarrollCBDD computers through the logging and storage of all activity, including all emails, web sites and other activity, including any personal use. All logs of employee activity are property of CarrollCBDD.
   f) **Data Storage on Network Only**. Employees must save all files/folders/documents on their Agency computer in either the "Documents" folder or "Desktop". All data within these two are synced / saved on the CarrollCBDD network server and backed up. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions.
   g) **Agency approved hardware only**. Only Agency owned and installed computers & hardware may be connected to and utilized on the CarrollCBDD network and/or the CarrollCBDD private Wi-Fi. CarrollCBDD owned electronic devices for students may be connected to the CarrollCBDD public Wi-Fi only. Electronic devices utilized by contracted therapists, the School Resource Officer, and guests attending meetings or trainings must only connect to the public Wi-Fi if internet access is needed.

2) **WORKSTATION SECURITY**
   a) 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 IT personnel.
   b) Workstation monitors should not face a direction that makes visual access available to unauthorized users.
   c) Staff should logoff or lock their screen when leaving their workstation area for a period of time.

3) **USER IDs and PASSWORDS**
   a) Each employee that is issued a CarrollCBDD owned electronic device will be assigned a unique User ID and Password. Passwords should be kept secure and confidential, not shared with anyone else. Passwords and will only be changed under the direction of the HIPAA Security Officer.
   b) Two-factor authorization and/or Single Sign-On technology should be used, if available.
   c) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

1110 Social Media Use

POLICY
CarrollCBDD guidelines for using social media sites and applications require that confidentiality and privacy of Individuals being served is maintained.

PROCEDURES
1) **CarrollCBDD-Sponsored Use**.
   a) The Superintendent may approve of the establishment of any CarrollCBDD-sponsored social media accounts.
   b) Prior to placing an image or other personally identifiable information on the CarrollCBDD website or social media, both a properly completed HIPAA authorization and/or a media release shall be completed and retained by the CarrollCBDD.
   c) If an Individual discloses PHI on a CarrollCBDD-sponsored social media page, the CarrollCBDD must not respond to or affirm the posting in any way. This includes, but is not limited to, replying or "liking" the posting because doing so is an affirmation by the CarrollCBDD that an Individual is enrolled with the CarrollCBDD. For example, the CarrollCBDD must not "like" a favorable review posted on the CarrollCBDD social media page.
   d) If an Individual or Individual's guardian asks a question or makes a request, either by way of a private message or visible post, to a CarrollCBDD-sponsored page, the CarrollCBDD must not respond through social media. Instead, call, secure email, or mail the Individual.

2) **Personal Use of Social Media by Employees**.
   Employee Use Outside of Work Hours. Any statement or image on social media has the potential to become a public communication, so employees of CarrollCBDD must follow the following guidelines:
   i) **Sharing of work-related activities**. Employees may share any CarrollCBDD-related information to information that they would deem acceptable to be made public, for example, on the front page of a major newspaper.
   ii) Employees are prohibited from originating a social media post that includes business related to CarrollCBDD, including any information regarding individuals served. Employees must portray themselves in a professional manner on any social media both working and non-working hours.
   iii) **Friending/Connecting/Linking**. In general, employees should not "friend", "link", "follow", or otherwise connect to any Individual, including any parent/guardian of an Individual, being served by CarrollCBDD on any social media. CarrollCBDD expects employees to maintain an acceptable professional boundary with Individuals being served. In the rare instances where any employee does friend/connect/link with an Individual served or a family member of an Individual served, any communications via social media must be of strictly a personal nature and not related to CarrollCBDD business.
   iv) **Messaging**. Employees must not use social media for CarrollCBDD-related communications regarding an individual served. Employees are reminded that all CarrollCBDD-related communications are subject to public records disclosure.

1120 Smartphone Devices

POLICY
Certain staff positions of CarrollCBDD will be issued an agency-owned smartphone. Employees in these staff positions must follow all guidelines in this policy. Further, all employees of CarrollCBDD are strictly prohibited from including PHI or any Individually Identifiable Information in a text correspondence using either a personal cell phone or a CarrollCBDD owned cell phone.

a) Using a CarrollCBDD owned cell phone, standard text messaging with individuals served and/or their parents is discouraged, but not prohibited, for "transient" messages regarding meeting dates and times.
b) All employees of CarrollCBDD are strictly prohibited from including PHI or any Individually Identifiable Information in a text correspondence using either a personal cell phone or a CarrollCBDD owned/issued cell phone.
c) If unsolicited PHI or Individually Identifiable Information is received by an employee of CarrollCBDD via a text message, any response must be made by way of a phone call or CarrollCBDD secure email.
d) Employees using a personal smartphone device to access their CarrollCBDD email account are strictly prohibited from saving/storing any CarrollCBDD data, PHI or any Individually Identifiable Information on that device.
e) Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours.
f) Employees are prohibited from allowing any other person to use the CarrollCBDD owned and issued mobile device.
g) Upon termination of employment or upon administrative leave, employee agrees to return the device to their Supervisor.

1130 Employee Work at Home

POLICY
Employees who work at home, including remote workers, must follow these procedures to ensure data security.

PROCEDURES
1) **Eligibility to Work at Home.** The Superintendent will determine, on an individual basis, the eligibility of employees to work remotely.
2) **No Agency Data on Home Computer/Laptop.** Employees are strictly prohibited to use their personal computers/laptops for work related purposes, therefore are also strictly prohibited from storing CarrollCBDD data on their personal computers/laptops.
3) **Unauthorized Cloud Storage Prohibited.** Employees are prohibited from storing CarrollCBDD data on any unauthorized cloud storage service.
4) **Agency Webmail.** Using a CarrollCBDD issued computer, employees are permitted to access, from home, their CarrollCBDD email through web-based email (webmail)

INDIVIDUAL RIGHTS

1200 Individual's Right to Access Records

POLICY
State laws, HIPAA and FERPA all provide that Individuals served by CCBDD, 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.

PROCEDURES
1) **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.
   b) An Individual or parent may include any 3rd party of their choosing to review the records.
   c) CCBDD may presume that either parent of a minor may have access unless presented with documentation that the parent does not have authority under applicable state law governing such matters as guardianship, separation, or divorce.
2) **Procedure, form and method of access**
   a) Requests for access to records shall be directed to the Privacy Officer or his/her designee.
   b) The Privacy Officer shall follow the Verification Procedure to verify the identity of the requestor. 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) Prior to release, Agency staff shall redact any confidential information (such as names of other Individuals served.)
   d) The CCBDD shall provide the Individual a photocopy of the entire record or portion of the record requested.
3) CCBDD will respond to reasonable requests for explanation and interpretation of the records.
4) Requests shall be honored within 5 business days.

1210 Individual's Right to Request Amendment of Records

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

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) An Individual, parent, guardian, or other person acting as a HIPAA personal representative may request amendment of PHI about the Individual (and exercise rights for hearing and statements of disagreement), which they believe is inaccurate, misleading, or violates the rights of the Individual, and is held by the CCBDD or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
   b) The Privacy Officer of the CCBDD will process such requests within 60 days.
   c) If the CCBDD accepts the requested amendment, in whole or in part, CCBDD must make the appropriate amendment, and inform the Individual and other persons or entities who have had access to the information.
   d) **Denied Request for Amendments**.
      Otherwise, if the CCBDD believes the existing record is correct as is, it may deny the amendment:
      i) **Written Notice.** A written notice of the denied request will be given. The notice of denial will include 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 CCBDD 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 CCBDD's denial.
      iii) **Written Rebuttal.** The CCBDD may prepare a written rebuttal to the Individual's statement of disagreement. Whenever such a rebuttal is prepared, the CCBDD 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.
   e) **Individual's Request for Copy of Changed Record.** At the Individual's request, CCBDD will send a copy of the changed record to any party requested by the Individual (per ORC 1347.09).
   f) **Separate Transmission of Information in EDI Format**. If the disclosure which was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, the CCBDD may separately transmit the information to the recipient of the transaction in a standard EDI format.

2) **RECORDS HEARINGS**
   CCBDD 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) CCBDD 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 CCBDD,

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, CCBDD 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, CCBDD 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 CCBDD.

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

1220 Individual's Right to Receive an Accounting of Disclosures

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

PROCEDURES
1) **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 CCBDD 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).
2) **Employee Documentation of Disclosures.** Any employee who makes a disclosure other than listed above shall document the disclosure in the Individual File, with all information described in step 6B below. More specifically, the following types of disclosures must be documented:
   a) To public health authorities
   b) Birth and death reporting
   c) To law enforcement regarding crime on premises
   d) To law enforcement in emergencies where crime is suspected
   e) For cadaveric organ, eye, tissue donation purposes
   f) For judicial and administrative proceedings
   g) For research with an IRB waiver
   h) To military command authorities
   i) For Workers Comp purposes
   j) To correctional institutions except as detailed in 2G above
   k) About decedents to medical examiners, funeral directors, coroners
   l) For public health activities
   m) About victims of abuse
   n) Regarding child abuse or neglect
   o) To the FDA
   p) To a person who may have been exposed to a communicable disease
   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
3) **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.
4) **Compliance with Request for Accounting will be within 45 Days.**
5) **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) CCBDD 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.

1230 Individual's Right to Request Additional Restrictions

POLICY

CCBDD supports Individual's right to request restrictions on the use or disclosure of protected health information which are more stringent than the restrictions defined in organizational policy. CCBDD 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.

PROCEDURES

1) 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, ethical or medical standards.
   c) Whether CCBDD 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) The CCBDD 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) CCBDD will notify the Individual of its final decision in writing. The notice will be maintained in the Individual's record.
   a) Granting the Request: If CCBDD agrees to the restriction, the notice to the Individual will clearly state what restriction CCBDD 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) If CCBDD agrees to the requested restriction, the Privacy Officer/designee will be responsible for taking appropriate action to implement the restriction.
5) An Individual may request a restriction to be eliminated at any time. If CCBDD 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 CCBDD' 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.

1240 Individual's Right to Request Confidential Communications

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

PROCEDURES
1) Individuals, or their personal representative, may make a request for confidential communications in writing.
2) When receiving such request, CCBDD 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 CCBDD will take to implement the request.
3) If existing systems are capable of administering the request, the Privacy Officer shall take necessary steps to implement the request, such as adjusted phone numbers or addresses in computer files or mailing lists.
4) The Privacy Officer shall document the request, and disposition, in the Individual's Record.

1250 Individual's Right to Notice of Privacy Practices

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

LEGAL NOTES
FERPA and IDEA require an annual Notice. HIPAA requires a one-time Notice, with redistribution upon change. HIPAA requires signed acknowledgement of receipt.

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 policies and procedures, namely are maintained to ensure appropriate distribution of Notice:
    a) All adults at intake will be given a copy of the Notice of Privacy Practices. At the time that the Notice is provided, the Individual or guardian shall sign an acknowledgement of his or her receipt of this Notice as part of the intake/transition of rights paperwork. This acknowledgement will be retained as part of the permanent record, for compliance with HIPAA requirements.
    b) For all other Individuals, the Board 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.
    c) An additional copy of the Notice shall further be provided upon request by an Individual or parent.
4) **Posting of Notice.** The Privacy Officer shall ensure that the Notice is posted:
    a) On the Agency's website.
    b) 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 "Records Retention Policy.pdf".

CONFIDENTIALITY POLICIES FOR SUPERVISORS

1300 Business Associate Contracts

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

PROCEDURES

CCBDD 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.

In the event CarrollCBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, CarrollCBDD will take steps to cure the breach or end the violation. If CarrollCBDD is unable to cure the breach or end the violation, CarrollCBDD will terminate the Business Associate Contract.

1310 Non-intimidation and Non-retaliation

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

1320 Privacy Complaints

POLICY
Individuals or CarrollCBDD employees may submit complaints about the CarrollCBDD's Confidentiality and Privacy policies and procedures and/or the CarrollCBDD's compliance with those policies and procedures. The CarrollCBDD shall take action and document all such complaints.

PROCEDURES
1) The HIPAA Privacy Officer shall manage this complaint process.
2) CarrollCBDD will extend the provisions of Policy "4.20 Protection of Whistleblowers", to all persons who file confidentiality or privacy related complaints.
3) An employee or Individual should file their complaint in writing to the Privacy Officer.
4) Upon receipt of a complaint, the Privacy Officer and Superintendent will review and investigate the complaint.
5) If warranted, the Privacy Officer shall take corrective action as appropriate, which may include:
   a) Change of policy and/or procedure.
   b) Intervention with an employee who is not following procedures including additional training and/or sanctions.
6) The Privacy Officer and/or the appropriate supervisor will communicate the results of the investigation and any corrective action taken to the person filing the complaint.

HIPAA SECURITY POLICIES

POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER

3000 Security Management Process

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

PROCEDURES

1) **The Superintendent will designate a HIPAA Security Officer**. The job responsibilities for this person are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer.

2) **The HIPAA Security Officer will be responsible for security management process**.
   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 protected health information maintained on systems owned or used by CarrollCBDD. The Computer Security Risk Analysis will be handled as follows:
      i) CarrollCBDD will use the risk analysis methodology detailed in NIST SP 800-30 Revision 1.
      ii) The results of this analysis shall be documented and maintained for 6 years
      iii) The risk analysis will be updated when appropriate based on technical and environmental variables, major software updates, infrastructure or other technological changes.
   iv) The risk analysis will be reviewed by the Security Officer, Privacy Officer, Superintendent, and IT service providers involved in risk management decision making or implementation.
   b) Implement and maintain the IT infrastructure, deploy Security Policies and Procedures.
      i) Prepare recommendations for the Superintendent as necessary, including implementation of new and updated policies, acquisition of technical security measures, or physical security measures.
      ii) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
      iii) Train Agency staff regarding compliance.
      iv) Monitor Agency compliance with the information security policies.

   c) The HIPAA Security Officer will maintain an inventory of the hardware, software and networking infrastructure.
      i) Content of Inventory:
         (1) Hardware inventory will document all servers, routers and other networking equipment, desktop computers, laptops, smartphones and other portable computing devices, external disk drives, and USB flash drives. Inventory will include physical location, primary user, manufacturer / model / serial number.
         (2) Software inventory will include hardware installed on, Software manufacturer, program name, version number, license/serial number and date.

3005 Data Backup

POLICY
The HIPAA Security Officer will verify that a data backup regimen is in place and operational.

PROCEDURES

1) CarrollCBDD cloud servers leased by Superior Technology Group are backed up nightly and located in Phoenix Arizona. Periodically, the HIPAA Security Officer will check with the network managed service provider, Superior Technology Group, to ensure that the backup and/or replication of managed CarrollCBDD cloud servers is functioning properly. The HIPAA Security Officer will periodically check also that the NAS device located in the CarrollCBDD Administration building is functioning properly.
2) Brittco Software will supply CarrollCBDD their Information Security Policy & Standards and Business Continuity & Disaster Recovery to provide assurance to the HIPAA Security Officer that CarrollCBDD data on their servers is secure and includes a secure backup.
3) Primary Solutions will supply CarrollCBDD their Data Security Policy to assure the HIPAA Security Officer that CarrollCBDD data on their servers is secure and includes a secure backup.

3012 Security Incident Response and Reporting

POLICY
CarrollCBDD will mitigate harmful effects of security incidents to the extent practicable, and document any such security incidents and their outcomes.

PROCEDURES

1) **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, CarollCBDD IT and the Superintendents management team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Policy 3035 Breach Reporting and Policy 1080 Reporting Violations and Security Incidents, Policy 3065 Mitigation will be followed as appropriate. Any contingency plans will be activated.
   c) **Documenting Security Incidents.** A written report will be filed by the HIPAA Security Officer as soon as practically possible after becoming aware of the incident and kept for 6 years.
   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
2) **Post-Incident Analysis.** The HIPAA Security Officer, CarrollCBDD IT and the Superintendents management team will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response and make changes they believe appropriate.

3015 Facility Security and Access Control

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

PROCEDURES

Facility Security and Access Plan

- All exterior doors will be locked from the outside at all times
- All employees will enter via main entrance
- Building Access control system will be maintained by Executive Secretary (High St.) and School Secretary (School) to restrict access of employees to permitted times
- Servers, Telecommunication Equipment, Routers and Switches will be maintained in locked rooms and/or locked cabinets
- Video surveillance cameras are in place to monitor activity in all buildings
- Nurse rooms will be locked when nurse is away
- File cabinets with confidential information will be locked
- Office doors will be locked when the person is away
- A full-time contract Resource Officer is stationed at the entrance to the school to screen all visitors, issue visitor badges and record their ingress and egress

Maintenance of Physical Security Equipment. The Maintenance Supervisor is responsible for maintaining equipment necessary to secure the facility, including locks, alarm systems, doors, security lighting, etc.

3020 Security Evaluation

POLICY
The HIPAA Security Officer will update policies as necessary in response to environmental or operational changes affecting the security of electronic protected health information.

PROCEDURES
1) Periodically, the HIPAA Security Officer will contract with an outside firm to review any updates to federal HIPAA regulations, other applicable federal and/or state statues, and technological issues and update the organization's security policies as appropriate.
2) Periodically, an evaluation of the technical infrastructure and/or the organizations compliance with computer security regulations will be conducted. Appropriate evaluations may include
    a) Vulnerability scanning and remediation
    b) Penetration tests
    c) Social Engineering exercises/tests
    d) IT Asset audits to identify missing assets
    e) Audits of policies and procedures for compliance with the following standards/regulations
        i) HIPAA
        ii) FERPA/IDEA
        iii) State laws
    f) Audits of compliance with policies and procedures, including verification that the processes, procedures and documentation specified in the policies exist, and that the responsible personnel understand the policies
3) **Documentation of Review.** The results of the review will be documented, and documentation shall be retained for 6 years.

3035 Breach Reporting

POLICY
CarrollCBDD will notify Individuals receiving services and the Secretary of HHS when appropriate regarding breaches of protected health information.

PROCEDURES
1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer along with CarrollCBDD IT will jointly determine if the incident meets the definition of a breach. Legal counsel and other outside expert advice will be obtained, if appropriate, for additional guidance. An investigation should be launched, with attention to preserving evidence.
   a) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   b) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   c) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the PHI involved, including types of identifiers and 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.

      The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1330 HIPAA Assignments and Documentation. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred, and this process may stop. Otherwise, a breach has occurred, and steps should be taken that follow in the remainder of this policy.
2) **Breach Notification**. In the event of a breach, the Team shall:
   a) Notify Individuals affected by the breach within 60 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 will include:
         (1) A brief description of what happened, including date of the breach if known and date of discovery of the breach.
         (2) A description of the types of unsecured PHI that were involved in the breach;
         (3) 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.
3) **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.

3040 Security Awareness Program

POLICY

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

PROCEDURES

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

2) **Annual and Periodic security awareness training for all staff.** Annual security awareness training to reinforce CarrollCBDD Security Policies will be completed by all staff. Advisories regarding current threats and issues with new technologies will be reviewed with appropriate staff on a periodic basis.

3050 Device and Media Disposal and Re-Use

POLICY

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

PROCEDURES

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 portable / removable device such as an external hard drive or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.

Hard drives, external/portable hard drives and USB drives shall be reformatted prior to re-use. If these said storage media are to be disposed, a certificate of destruction must be obtained from the company performing the destruction.

Hard drives in multi-function copier machines is another media of which a certificate of destruction is required upon disposal or replacement.

Records of media disposal including any certificates of destruction will be maintained on file for 6 years.

3060 Technical Safeguards

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

PROCEDURES
1) **Firewalls.** Commercial-grade hardware and/or software firewalls shall be installed to protect against network intrusions and to manage/monitor outbound traffic within the confines of our CarrollCBDD network.
2) **Virus Protection.** All company computers will be protected by anti-virus/malicious software protection.
3) **Secure Configurations.** Workstations and servers will be installed with a standard configuration that meets the following specifications:
   Only vendor-supported versions of software will be used. Additional software may be installed for specific users based on unique requirements.
4) **Operating System and Application Software Patching**. Operating Systems, application software and virtual servers if used, shall be patched regularly on both servers and workstations. Auto-update functionally may be employed and update servers.
5) **Virtualization Software and Environment**. The virtualization-enabling software shall be secured as follows:
   a) A strong password (minimum of 8 characters, 1 upper case, 1 lower case, 1 digit) shall be used for the management console.
   b) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's.
6) **DNS Filtering** may be employed at the discretion of the IT department to reduce access to unsafe websites and to reduce phishing attacks, using OpenDNS or an alternative service.
7) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   a) The SSID should be changed from the default.
   b) WPA/WPA2 should be enabled.
   c) WPS should be disabled.
   These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
8) **E-mail**. For transmission of PHI, secure, encrypted e-mail will be employed.

9) **Encryption of staff computers**. Must utilize encrypted software on hard drives. Bitlocker encryption software is currently used on all staff computers.

10) **Encryption of cloud servers**. CarrollCBDD cloud servers managed by Superior Technology Group are encrypted.

3065 Mitigation

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

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.

3070 Electronic Signatures

POLICY
Electronic signatures may be utilized at CarrollCBDD 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.

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

PROCEDURES
1) **Security**
   a) **Confidentiality statement**. Anyone authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature/ logon password, that the electronic signature will be legally binding and that passwords will not be shared and will be kept confidential.
   b) **Passwords**. All users will have their own user ID and password. Passwords must conform to complexity guidelines detailed in Policy 1100 Acceptable Use of IT Assets.
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.

3075 Employee System Access and Termination Procedures

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

PROCEDURES

1) **AUTHORIZATION TO SYSTEMS**

Granting Access to Information Systems. The authority to grant access to information systems rests with the Superintendent. The Superintendent will direct the HIPAA Security Officer to grant access only to the information systems that are necessary for a particular staff position in order for that staff to fulfill their job duties. The minimum necessary standard will be applied.

The HIPAA Security Officer will work with the IT service provider to utilize the security capabilities of the various network and application software systems at the Agency.

The HIPAA Security Officer will audit the access controls to verify that the above policy has been implemented properly and consistently. Such an audit could include verification that recently terminated employees no longer have access, a review of access for employees with job changes in the previous year, and a random sampling of other employee access authorization. Based on the results of this audit, the HIPAA Security Officer will adjust policies and/or staff training as appropriate.

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

a) **Assigning User ID and Password.** New hires requiring computer access will be assigned a unique network User ID and password, and/or User IDs and passwords for other application systems. Security settings appropriate for the person and their position will be assigned accordingly.
b) **User Data Area.** The HIPAA Security Officer will coordinate with the IT service provider to configure a User Data Area on the Server to provide data storage space for the employee. All data is to be stored on the servers managed by the IT network service provider.
c) **Security Awareness Training.** New employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Policy 3040 Security Awareness Program. and the Policy 1100 Acceptable Use of IT Assets, and they will sign written acknowledgement that they understand and will adhere to all policies. This will be maintained in the employee personnel file.

3) **EMPLOYEE JOB CHANGES**

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

4) **EMPLOYEE TERMINATION**

a) On the last day of employment, employee passwords and User IDs to the network and Application Software will be disabled. Account access to all shared cloud systems will be terminated.

b) For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the Security Officer and/or the Privacy Officer who will coordinate with the IT Network Service Provider so that appropriate precautions will be taken to ensure the integrity and security of confidential Agency information. This could include such measures as:
   i) Physically escorting the person off the premises after notifying him/her of the termination.
   ii) Disabling system access and access to all shared cloud systems as specified above on a timely basis.
   iii) Requiring all staff in the former employee's workgroup to change passwords.
   iv) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the person and perceived threat.