COUNTY BOARD OF HEALTH
POLICY # GC-09013
CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION AND COMPLIANCE WITH HIPAA

Approval:	District Health Director	8/14/2020 Date

Public Health
Prevent. Promote. Protect.

1.0 PURPOSE

The purpose of this policy is to establish workplace rules regarding County Board of Health employees' management of confidential data and compliance with HIPAA.

2.0 AUTHORITY – This policy is published under the authority of CBOH and in compliance with the following:

2.1 45 C.F.R, Part 160: "General Administrative Requirements"

2.2 45 C.F.R, Part 162: "Administrative Requirements"

2.3 45 C.F.R, Part 164: "Security and Privacy"

3.0 SCOPE

This policy shall apply to all employees and functions of the CBOH.

4.0 POLICY

The County Board of Health (CBOH) is committed to protecting the confidentiality of personal health information (PHI) in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all state and federal privacy laws. This policy sets forth the standards and procedures for CBOH employees to follow in protecting personal health information.

It is CBOH policy that an individual's health information should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive it has been verified. Health information shall not be disclosed or made available to unauthorized persons, and precautions shall be taken to ensure that health information is not disclosed to unauthorized persons.

This policy does not list every possible situation in which the CBOH may lawfully disclose

personal health information to third parties. Employees are directed to consult the CBOH Privacy Officer if they believe it may be necessary to disclose an individual's personal health information without that individual's authorization.

5.0 DEFINITIONS

5.1 Administrative Safeguards: 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.

5.2 Breach: The acquisition, access, use, loss, or disclosure of protected health information in circumstances where it might be accessed by unauthorized individuals or entities. If protected health information is acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, then it shall be presumed to be a breach unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

5.3 Business Associate: An outside person or entity that performs or assists the CBOH in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

5.4 CBOH: County Board of Health

5.5 Covered Entity: An entity that is subject to HIPAA because it is a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA.

5.6 Designated Record Set: A group of records that includes (1) the medical records and billing records about patients maintained by or for a covered health care provider; (2) records of the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; (3) records used by or for the covered entity to make decisions about the patient. 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.

5.7 Electronic Media: Electronic storage media including memory storage components in computers and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, hard drive, or digital memory card; or transmission media used to exchange information already in electronic storage media. Examples of transmission media include the internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, such as facsimile messages, telephone conversations, or VOIP (voice over internet), are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

5.8 **Electronic Protected Health Information:** Individually identifiable health information that is transmitted by electronic media or maintained in electronic media.

5.9 **Health Care Operations:** Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

5.9.1 Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

5.9.2 Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

5.9.3 Underwriting and other activities relating to the creation, renewal, or replacement of health insurance or health benefits contract, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;

5.9.4 Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detecting and compliance programs;

5.9.5 Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

5.9.6 Business management and general administrative activities including de-identifying protected health information and creating a limited data set.

5.10 **Health Care Provider:** A provider of services as defined in 42 U.S.C. 1395x(u), a provider of medical or health services as defined in 42 U.S.C. 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

5.11 **Health Information:** Any information, whether oral or recorded in any form or medium, that is created or received by a health car provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and which relates to the past, present or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient.

5.12 **Health Oversight Agency:** An agency or authority of the United States, a territory, a political subdivision of a state or territory, 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, 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.

5.13 **HIPAA Privacy Officer:** An employee who is responsible for the development and implementation of the policies and procedures required to comply with the HIPAA privacy rule.

5.14 **HIPAA Security Officer:** An employee who is responsible for the development and implementation of the policies and procedures required to comply with the HIPAA security rule.

5.15 **Individually Identifiable Health Information:** Health information pertaining to an identifiable named patient, and which is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient, and that identifies the patient, or for which there is a reasonable basis to believe the information can be linked to the patient.

5.16 **Limited Data Set:** Protected health information that removes the following identifiers of the individual or individual's relatives, household members, and employers: name, postal address information (other than town or city, State, and zip code), telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers related to Social Security, medical records, health plans, account, certificates, licenses, motor vehicles and license plates, driver's licenses, device and serial numbers, Internet Protocol (IP addresses, and Universal Resource Locators (URLs).

5.17 **Minor:** An unmarried person under the age of eighteen who has not been emancipated by order of the courts.

5.18 **Patient:** The person who is the subject of the protected health information.

5.19 **Protected Health Information (PHI):** Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Examples of Protected Health Information include, but are not limited to an individual's:

5.19.1 Name;

5.19.2 Address;

5.19.3 All elements of dates (except year) for dates directly related to an individual;

5.19.4 Telephone number;

5.19.5 E-mail address;

5.19.6 Social Security number;

5.19.7 Medical record number;

5.19.8 Health plan beneficiary number;

5.19.9 Account Number;

5.19.10 Internet Protocol (IP) address number; and

5.19.11 Any other unique identifying number, characteristic, or code.

5.20 **Psychotherapy Notes:** 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 patient'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.

5.21 **Public Health Authority:** An agency or authority of the United States, a state, territory, a political subdivision of a state or territory, or an Indian tribe, or a person acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency, that is responsible for public health matters as part of its official mandate.

5.22 **Security Incident:** The attempted or successful unauthorized access, use, disclosure, modification, loss, or destruction of health information, or interference with system operations in an information system that stores health information.

5.23 **Technical Safeguards:** The technology and the policy and procedures for its use that protect electronic protected health information and control its access.

5.24 **Unsecured Protected Health Information:** Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

6.0 RESPONSIBILITIES

6.1 The District Health Director shall designate an employee to serve as the HIPAA Privacy Officer for the Health District, to be responsible for the development of the policies and procedures for the protection of PHI and compliance with HIPAA, administrative safeguards, assistance with training materials, and providing advice as needed.

6.2 The Information Technology Manager shall designate a member of his or her staff to serve as HIPAA Security Officer for the CBOH, to be responsible for the implementation of appropriate technical safeguards as required by HIPAA to ensure the integrity of all electronic PHI that the CBOH creates, maintains, receives, or transmits.

6.3 The HIPAA Privacy Officer is responsible for training of CBOH employees in privacy compliance, for documenting such training for individual employees, and for referring and recommending appropriate sanctions against employees who violate privacy policies and procedures.

6.4 The Security Incident Response Team shall respond to any suspected breach of PHI in accordance with the Personal Health Information Security Incident Response Protocol. The Team shall consist of the HIPAA Privacy Officer and the HIPAA Security Officer. If circumstances warrant, the Team may request the support of additional staff or resources.

6.5 Supervisory personnel are responsible for ensuring compliance with this policy by CBOH employees under their supervision.

7.0 PROCEDURES

PHI should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive the PHI has been verified. In addition, care must be taken to prevent accidental disclosure or access to PHI by unauthorized persons.

Note: These standards apply even if the patient is deceased.

7.1 Face to Face Discussions

Employees must take reasonable steps to protect the privacy of all face-to-face discussions of PHI, whether inside or outside of the office. When possible, employees should use enclosed offices or interview rooms for discussions involving PHI. If enclosed offices or rooms are not available, then employees should take reasonable precautions to ensure that their conversations are not overheard. In all cases, discussions of PHI should be limited to only that PHI which is necessary to conduct the business at hand.

7.2 Telephone Calls

7.2.1 Before discussing PHI over the telephone with a patient, including providing test results or contacting the patient about appointments, employees must confirm the identity of the patient. This may be done by asking the patient to confirm his or her full name, date of birth, and the last four digits of their Social Security number and/or by other unique identifiers for the patient.

7.2.2 Employees must honor any previously agreed upon request by the patient to use alternate means of communication, such as alternate phone numbers, or limiting calls to certain hours.

7.2.3 Telephone calls should be made in private locations where possible. The employee should be aware of the surroundings and make sure that the conversation is not heard by nearby persons. The employee should also ask the patient to confirm that there is no one else on the line.

7.2.4 If the employee gets the patient's voicemail and decides to leave a message, then the message should only include the name and phone number of the person to be called back. Do not leave any other information, such as the name of the program from which the employee is calling or the fact that test results have been received, since that may compromise patient confidentiality if someone else retrieves the message.

7.3 Visual Access to PHI Displayed on Computer Screens

7.3.1 Employees must ensure that PHI displayed on computer screens is adequately shielded from view by unauthorized persons. Polarized screens or other screen overlay devices that shield information on the computer screen should be used when possible.

7.3.2 Computer workstations must be locked when not in use, and PHI must be cleared from the screen when it is not being used.

7.3.3 Computers and other electronic storage devices containing PHI must be stored in a secured location at all times.

7.4 Paper Records and Files

7.4.1 Employees must store files and documents containing PHI in secure filing cabinets, rooms, or storage systems. If lockable storage is not available, staff must take reasonable steps to ensure the safeguarding of documents containing PHI.

7.4.2 Papers containing PHI must be shredded before they are placed in the trash.

7.4.3 Documents containing PHI must be shielded from view by unauthorized persons and should not be left unattended in open areas.

7.5 Outgoing Mail (Including Inter-Office or Intra-Office Mail)

7.5.1 Documents or other medium containing PHI should be mailed in sealed envelopes or other secure container, properly addressed to the recipient, and the outer envelope should be clearly labeled "Confidential".

7.5.2 If PHI is stored on electronic media, then the media should be password protected before mailing.

7.5.3 The information sent should be the minimum necessary for the intended purpose.

7.5.4 All outgoing mail containing PHI should clearly display a return name and address on the outer envelope, so that misdirected mail can be returned to the sender.

7.6 Facsimile Communications

7.6.1 The fax machines should be located in a non-public place and near to the intended recipients for sending and receiving PHI information.

7.6.2 When receiving a fax containing PHI employees should request a call from the sender prior to transmission, so that someone will be standing by to retrieve the document from the machine as soon as it is received.

7.6.3 When sending a fax containing PHI, employees must contact the recipient to schedule transmission, confirm the fax number, and ensure that the fax will be retrieved by an authorized person after it is sent. Outgoing faxes containing PHI must have a cover page labeled "CONFIDENTIAL". After sending the fax, employees must confirm that delivery was made to the intended recipient by either contacting the recipient to confirm receipt or reviewing the fax transmission confirmation.

7.6.4 The information sent should be the minimum necessary for the intended purpose.

7.6.5 In the event that a fax is inadvertently sent to an unintended recipient the recipient must be contacted immediately and asked to destroy the information. Misdirected faxes are considered a security incident and must be reported to the Privacy Officer.

7.7 Emails

7.7.1 Public webmail (i.e., yahoo, gmail and Hotmail) must not be used to transmit any PHI. Transmission of PHI through public webmail would constitute a breach of information. Employees may not send PHI to a home account.

7.7.2 Emails should not contain PHI unless the PHI is in encrypted form. Where feasible, the PHI should be sent in a password-protected attachment instead of in the body of the email, with the password being sent in a separate email or communication which should also notify the recipient that the information has been emailed.

7.7.3 Emails containing PHI must be encrypted and marked "CONFIDENTIAL" in the subject line, and should only be sent to persons who understand the CBOH's privacy policies and applicable privacy laws and regulations, and will not forward the email to unauthorized persons.

7.7.4 The information sent should be the minimum necessary for the intended purpose.

7.7.5 Employees should verify and review the recipient's email address prior to sending the email. In the event an email is inadvertently sent to the unintended recipient, the recipient must be contacted immediately and asked to delete the email and attachment. Misdirected emails are considered a security incident and must be reported to the HIPAA Privacy Officer.

7.8 Text Messages

7.8.1 Text messages must be sent in accordance with the CBOH's Use of Text Messaging Policy.

7.9 THE "MINIMUM NECESSARY" RULE WHEN USING OR DISCLOSING PHI

Even when use of disclosure of PHI is appropriate, employees must ensure that only the minimum PHI necessary to accomplish the intended purpose will be used or disclosed.

7.9.1 Necessary Access and Use:

Access and use should be restricted based on specific roles. Each division, office, and program supervisor must identify the persons or groups of persons who need access to PHI to carry out their job functions, identify the type of PHI to which each person or group needs access, as well as the conditions under which they need access, and make reasonable efforts to limit the access of its staff to only the information appropriate and necessary for their job requirements. Access to PHI should not be granted to any unit or program that does not need access to perform its job functions.

7.9.2 Minimum Necessary Disclosures:

Before disclosing PHI, staff must evaluate the purpose of the disclosure and limit the disclosure to the minimum necessary to satisfy the intent of the disclosure. Staff should identify routine and recurring disclosures and determine what information is reasonably necessary to fulfill the purpose of these requests so that the disclosure can be limited to the minimum necessary. In making this determination, staff should evaluate whether the purpose of the disclosure can be fulfilled with de-identified information or a limited data set. Non-routine and non-recurring requests should be reviewed on an individual basis to ensure only the minimum necessary is disclosed for each of these requests.

7.9.3 Situations in which the minimum necessary requirement does not apply:

7.9.3.1 disclosures to or requests by a health care provider for treatment of the patient;

7.9.3.2 disclosures made to the patient or his/her authorized representative;

7.9.3.3 disclosures made pursuant to a valid authorization;

7.9.3.4 disclosures made to the Secretary of the U.S. Department of Health & Human Services;

7.9.3.5 disclosures required by law; or

7.9.3.6 disclosures required for compliance with HIPAA regulations.

7.10 RESPONDING TO REQUESTS FOR DISCLOSURE OF PHI

7.10.1 Requests for Disclosure Made by the Patient

7.10.1.1 The CBOH shall disclose PHI to a patient when the patient requests access to their own PHI. However, there is one exception: a therapist's psychotherapy notes may not be disclosed to a patient without prior approval from the DPH HIPAA Privacy Officer.

7.10.1.2 The patient's identity shall be verified in accordance with paragraph 7.2.1 before releasing PHI.

7.10.2 Requests for Disclosure Made by the Patient's Authorized Representative

7.10.2.1 The CBOH shall disclose PHI to a third party who is legally authorized to act as a representative of the patient with regard to health matters.

7.10.2.2 The scope of the representative's authority to act for the patient depends on his or her authority to make health care decisions for the patient. If the authority to act for a patient is limited to a particular health care decision, the person should be treated as the patient's representative only with respect to PHI relevant to that decision. Employees are encouraged to consult with the HIPAA Privacy Officer if they have any doubt about the representative's authority.

Common situations involving a patient authorized representative include:

7.10.2.2.1 *Adult or Emancipated Minor:* If a person is authorized to act on behalf of an adult or emancipated minor in making health care decisions, then this person must be treated as a personal representative with respect to PHI related to such representation. Examples include persons acting pursuant to a health care power of attorney or general power of attorney, or a court appointed legal guardian.

7.10.2.2.2 *Deceased Patient:* Privacy rights under HIPAA continue for fifty years after the patient dies. An executor, administrator, or other person authorized by law to act on behalf of the deceased person's estate may be treated as personal representative with respect to the deceased's PHI.

7.10.2.2.3 *Minor Children:* If a parent, guardian, or other person acting in the place of a parent (in loco parentis) is authorized to act on behalf of a minor in making health care decisions, then this person may be

treated as a personal representative with respect to PHI related to such representation. It may be necessary in some cases to require proof of a parent or other person's authority to have access to the child's PHI; for example, a divorced parent without authority to make health care decisions for the child should not have access to the child's PHI. In addition, the CBOH must *not* make disclosures to a parent or guardian if:

7.10.2.2.3.1 the minor consented to care, and the consent of the parent is not required under State or other applicable law (*e.g.,* testing or treatment of venereal disease);

7.10.2.2.3.2 the minor obtained care at the direction of a court or a person appointed by the court; or

7.10.2.2.3.3 the parent or guardian agreed that the minor and the health care provider may have a confidential relationship. This agreement should be documented in medical chart.

7.10.2.2.4 *Married Persons:* Employees are cautioned that a married person should *not* be given access to a spouse's PHI, unless that person presents proof of authorization in accordance with this Paragraph.

7.10.3 The identity *and* authority of a third party seeking the PHI must be verified as specified in Paragraph 7.2.1 prior to disclosure of PHI to the third party. The proof needed to verify authority will vary depending on the nature of the authority. For example, a court-appointed guardian or the executor of a decease person's estate will have an order of appointment from the probate court, and a person acting pursuant to a health care power of attorney will have a written power of attorney. Consult the HIPAA Privacy Officer if you have any concerns about proof of authority.

7.10.4 The CBOH may refuse a request for PHI from a person acting as the patient's personal representative if it appears that the personal representative may have subjected the patient to violence, abuse, or neglect; if treating the person as a personal representative could endanger the patient; or if a licensed healthcare professional determines, in the exercise of professional judgment, that it is not in the best interest of the patient to treat the person as a personal representative.

7.11 Requests for Disclosure Made by Third Parties with a Written Authorization From the Patient

A patient's PHI shall be disclosed to a third party pursuant to a valid written authorization signed by the patient. Patients should be encouraged to use the standard CBOH Authorization for Release of PHI Form, but any authorization form that meets the requirements of Paragraph 7.11.1 should be honored. Upon request, the HIPAA Privacy Office shall review an authorization form to ensure that it is legally sufficient. The CBOH must retain a copy of all signed authorizations.

7.11.1 Criteria for a Valid Authorization

If an employee receives a request for disclosure of PHI from a third party with an Authorization Form signed by the patient attached, the form will be honored only if it contains all of the elements below in plain language:

7.11.1.1 A specific description of the information requested;

7.11.1.2 The name of other specific identification of the person(s), or class or persons, authorized to request the information;

7.11.1.3 The name or other specific identification of the person(s), or class of persons, to whom the CBOH may give the requested information;

7.11.1.4 A description of the purposes for which the information is requested;

7.11.1.5 An expiration date or an expiration event that relates to the patient or the purpose of the request;

7.11.1.6 Signature of the patient and date;

7.11.1.7 A statement adequate to place the patient on notice of his or her right to revoke the authorization in writing, a list of the exceptions to the right to revoke, and a description of how the individual may revoke the authorization;

7.11.1.8 A statement adequate to place the patient on notice of whether or not treatment, payment, enrollment or eligibility for benefits will be conditioned on whether the patient signs the authorization; and

7.11.1.9 A statement adequate to place the patient on notice of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.

7.11.2 Authorization for Disclosure of Psychotherapy Notes

A separate specific authorization form must be obtained for the disclosure of psychotherapy notes that are included within a patient's medical records. The form must specifically request psychotherapy notes in addition to having all the elements listed in Paragraph 7.11.1. Consult with the HIPAA Privacy Officer if

there are any questions regarding the sufficiency of an authorization for the disclosure of psychotherapy notes received from a third party.

7.11.3 Invalid Authorization

An authorization will not be honored by the CBOH if it has any of the following defects: (i) the expiration date or event has passed; (ii) the Authorization Form has not been filled out completely; (iii) the authorization has been revoked; (iv) any information on the authorization is known to be false; (v) an authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes. An invalid authorization should be returned to the person who submitted it, with an explanation of why the authorization cannot be honored. Consult with the HIPAA Privacy Officer if you receive an authorization that may be invalid.

7.11.4 Compound Authorization

An authorization for use or disclosure of PHI must be a separate document, and may not be combined with any other document from the patient to create a compound authorization, except as follows: (i) an authorization for the use or disclosure of PHI for a research study may be combined with the informed consent document that will be used in the research project; (ii) an authorization for the use or disclosure of psychotherapy notes may be combined with authorization for the use or disclosure of psychotherapy notes to other persons (*e.g.,* a single authorization can be used for disclosure to multiple agencies or individuals); (iii) an authorization may be combined with authorization to other persons (*e.g.,* a single authorization can be used for disclosure to multiple agencies or individuals).

7.11.5 Revocation of Authorization

A patient may revoke his or her authorization in writing at any time. If the patient revokes an authorization, the CBOH cannot disclose information after the effective date of the revocation. A revocation should be maintained in the patient's file.

7.12 Requests for Disclosure Made by Third Parties Without Patient Authorization

The CBOH may disclose PHI to third parties without the written authorization of the patient only in certain limited circumstances. *All requests for disclosure without patient authorization must be sent to the HIPAA Privacy Officer for review before any response is made.* The HIPAA Privacy Officer may determine that disclosure of PHI without patient authorization is appropriate in the following situations:

7.12.1 To a healthcare provider covered by HIPAA for the purpose of treatment, payment, or healthcare operations;

7.12.2 Disclosures required by law;

7.12.3 Disclosures for public health activities to (i) Public Health Authorities that are authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including the reporting of disease, injury, vital events, and public health surveillance (*e.g.,* the CDC); (ii) public health or other government authority legally authorized to receive reports of child abuse or neglect; or (iii) a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

7.12.4 Disclosures about victims of abuse, neglect or domestic violence to a government authority authorized by law to receive such information under certain circumstances;

7.12.5 Disclosures for health oversight activities authorized by law (*e.g.,* audits);

7.12.6 Disclosures for court proceedings, including search warrants, court orders, subpoenas, interrogatories, or requests for production of documents.

Note: Any legal paper seeking PHI should be faxed, emailed, or hand-delivered to the HIPAA Privacy Officer immediately upon receipt.

7.12.7 Disclosures for law enforcement purposes to a law enforcement official, if certain conditions are met;

7.12.7.1 Disclosures about decedents to a coroner or medical examiner to identify a deceased person or determine cause of death, and to funeral directors;

7.12.7.2 Disclosures to avert a serious threat to the health or safety of a person or the public;

7.12.7.3 Disclosures for specialized government functions, including national security and intelligence activities;

7.12.7.4 Disclosures to comply with laws relating to workers' compensations;

7.12.7.5 Disclosures to persons involved in the patient's care and for notification of the patient's location, general condition, or death purposes. If the patient is present, he or she must be given the opportunity to agree or object to such disclosures.

Note: Disclosure of PHI is ordinarily *not* permitted in response to an Open Records Act request. Contact the HIPAA Privacy Officer immediately if you receive an Open Records Act request for PHI.

7.13 Verification of Identity Prior to Disclosure of PHI

Prior to making any permitted disclosure of PHI, staff must verify the identity of the person requesting the PHI and the authority of such person or entity to receive such disclosure,

if their identity or authority is not already known. Staff must also obtain any documentation, statements, or representation that are a condition of the disclosure from the person or entity making the request.

7.13.1 Verifying a Patient's Identity

The patient must provide their name, date of birth, address on file, and if available a copy of a government issued picture identification. Whenever practicable, requests should be in writing and signed by the patient. A copy of the request should be kept in the patient's file. While the social security number is not required, if provided by the patient it serves as further identification.

7.13.2 Verifying the Identity and Authority of the Patient's Personal Representative

Staff must verify the identity *and* authority of personal representatives requesting access to a patient's PHI. Staff must (i) verify the name and date of birth of the patient who is the subject of the request; (ii) obtain appropriate documentation supporting the request for access to the PHI, such as guardianship documents, custody orders, power of attorney, or Authorization Form; (iii) verify the requestor's name and obtain a copy of a government issued picture identification; (iv) confirm any limitations regarding the disclosure of information to the personal representative (v) once identity and authority has been confirmed, disclose only the minimum information necessary to fulfill the request.

7.13.3 Verifying the Identity and Authority of a Public Official

Staff may rely on any of the following to verify identity of a public official:

7.13.3.1 If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

7.13.3.2 If the request is in writing, the request is on the appropriate government letterhead; or

7.13.3.3 If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate governmental letterhead that the person is acting under the government's authority or other evidence or documentation, 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.

CBOH may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

7.13.3.3.1 A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or

7.13.3.3.2 If a request is made pursuant to legal process, then a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

7.13.4 Verifying the Identity and Authority of Law Enforcement official

Staff may disclose PHI to a law enforcement official for certain law enforcement purposes. The staff should ask to see the law enforcement official's official identification and the subpoena, summons, request for records, civil or authorized investigative demand, or similar legal process by which the PHI is being requested, and then consult the HIPAA Privacy Officer A copy of this legal process should be kept in the patient's file.

7.14 Other Requirements Relating to the Use and Disclosure of PHI

7.14.1 Disclosure of properly de-identified information is permitted by the HIPAA Privacy Rule. PHI is de-identified by removing certain individual identifiers to make it impossible to identify the health information as belonging to a particular patient. PHI is properly de-identified only if the information cannot be used alone or in combination with other information to identify a patient who is a subject of the information, **and** there is either a statistician determination pursuant to Paragraph 7.14.1.1 **or** removal of identifiers pursuant to Paragraph 7.14.1.2. De-identified data may only be released in accordance with DPH's Data Request and Use Policy or as otherwise approved by the Privacy Officer.

7.14.1.1 De-Identification Through Statistician Determination

Data is "de-identified" if a CBOH employee with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data applies such principles and methods to the Data, and determines that such application results in a very small risk that the de-identified data could be used, alone or in combination with other reasonably available information, to identify an individual whose de-identified PHI will be disclosed. Such a determination must be properly documented.

7.14.1.2 De-Identification Through Removal of Identifiers

Data is "de-identified" through removal of the following identifiers of the individual or the individual's relatives, household members, and employers: name, addresses (except for the State and the first three digits of the zip code, if the current total population of all zip codes

with those three digits is more than 20,000), month and day of all dates directly related to an individual, all ages over 89 and all elements of dates indicative of such ages, telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicle sand license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

7.14.1.3 Re-identification

Staff may assign a code or other means to allow de-identified information to be re-identified, provided that the code or other means is not derived from or related to information about the patient and cannot be translated to identify the patient, and the CBOH does not disclose the code or mechanism for re-identification.

7.14.2 Business Associate Agreements

A business associate is a person or organization that, on behalf of the CBOH, performs or assists in the performance of a function or activity involving the user or disclosure of PHI, or provides services to or for the CBOH which require access to PHI. All CBOH must identify Business Associates, so that the appropriate contractual requirements are in place to govern the Business Associates' use of PHI.

Before the CBOH discloses PHI to a business associate, the associate must sign the CBOH Business Associate Agreement, or a contract to which the CBOH Business Associate Agreement is attached. Any material breach or violation of the Business Associate Agreement must be reported to the HIPAA Privacy Officer. If the Business Associate fails to cure the breach and end the violation, then its access to PHI must be cut off, and its contract with CBOH must be terminated.

7.15 REQUESTS FOR PHI CONTAINING RECORDS OF TREATMENT OR DIAGNOSIS OF MENTAL ILLNESS, HIV/AIDS, ALCOHOL OR DRUG DEPENDENCY, OR TREATMENT OF THE DEVELOPMENTALLY DISABLED

7.15.1 Employees are cautioned to consult with HIPPA Privacy Officer before releasing PHI which contains any reference to diagnosis or treatment of HIV/AIDS, drug or alcohol dependency or abuse, mental illness, or treatment of the developmentally disabled. Such record may be entitled to heightened legal protection in accordance with:

10.1.1 O.C.G.A. § 37-3-166 (records of treatment of mental illness)

10.1.2 O.C.G.A § 37-4-125 (records of treatment of the developmentally disabled)

10.1.3. O.C.G.A. § 37-7-166 (records of treatment for alcohol or drug dependency or abuse)

10.1.4 O.C.G.A. § 24-12-21 (records of testing, diagnosis, treatment of HIV/AIDS).

7.16 DOCUMENT RETENTION

All documents required by this Policy must be retained for six years from the date of creation or the date when it was last in effect, whichever is later, including its policies, standard forms and notices, and procedures in written or electronic form, all communications required to be in writing, and any action, activity or designation required to be documented. Although the HIPAA document retention period is six years, consult the CBOH's Record Retention Policy to ensure compliance with the CBOH's record retention schedule as well.

7.17 TRAINING

The HIPAA Privacy Officer will develop HIPAA training for use by all members of the workforce and will collect and maintain a certificate of completion from each employee who completes the training. Training is required for all current employees and for all new employees within the established time period of becoming employed. The content of the training will include key points of the Policy, and procedures for detecting, guarding against, and reporting malicious software. Periodic security updates will be distributed to the CBOH workforce as changes are made to federal HIPAA regulations or this Policy and as needed.

7.18 PATIENT RIGHTS

7.18.1 Right to Notice of Privacy Practices

A copy of the current CBOH Privacy Notice shall be given to each person receiving healthcare service from the CBOH. Staff must make a copy of the notice available to any person upon request, and for patients receiving treatment no later than the date of first service, or in an emergency treatment situation, as soon as reasonably practicable after the emergency. For patients receiving treatment, employees must make good faith effort to obtain a written acknowledgement of receipt of the notice, and if unsuccessful, document good faith efforts to obtain the acknowledgement and the reasons it was not obtained. The written acknowledgement and documents showing efforts to obtain it must be maintained. The notice should be available at physical service delivery sites and posted in a clear and prominent location. The notice shall be posted on and made available through the CBOH's website.

7.18.2 Right to Request Restriction of Uses and Disclosures of PHI

7.18.2.1 Patients may request that the use and disclosure of their PHI be restricted to treatment, payment or health care operations, disclosures to persons involved in the patient's health care, or disclosures to notify family members or others about the patient's health care, or disclosures to notify family members or others about the patient's general condition, location or death. The CBOH is not required to honor such requests, but if it elects to do so, then the restriction must be documented and retained in the patient's file. Notwithstanding such a restriction, however, CBOH may disclose the patient's PHI if it is needed for the purpose of treating the patient in the event of an emergency.

7.18.2.2 Patients may request that their PHI pertaining to a particular health care item or service *not* be disclosed to the patient's health plan, if that particular health care item or service was paid for without assistance from the patient's health plan. The CBOH must honor such a restriction. The restriction must be documented and retained in the patient's file.

7.18.3 Right to Request That Communications Be Made in a Confidential Manner

CBOH must accommodate reasonable requests by patients to receive communications of PHI by alternate means or at alternate locations or times. Employees must require that the request be in writing where possible. The patient must specify the requested alternate address or other method of contact but need not give a reason for the request. The request must be documented and retained in the patient's file.

7.18.4 Right of Access to PHI

7.18.4.1 A patient has a right of access to inspect and obtain a copy of his or her PHI in a designated record set, for as long as the PHI is maintained in a designated record set. All requests for access must be in writing and must be immediately forwarded to the HIPAA Privacy Officer, so that the CBOH can act on the request within 30 days of receipt. Staff must document the designated record sets that are disclosed to patients and retain such documentation.

7.18.4.2 A Patient's access to his or her PHI may be denied only in the following circumstances: psychotherapy notes may not be disclosed; the PHI was obtained from someone other than a healthcare provider and confidentiality was promised; or a licensed health care professional has determined that disclosure would endanger the life or safety of the patient or any other person. If access to any part of the patient's PHI is denied, then the patient shall be notified and given an opportunity to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

7.18.4.3 The patient may request either paper or electronic copies of his or her PHI, and may be charged a reasonable fee to cover the cost of finding, copying, and providing the PHI.

7.18.5 Right to Request Amendment of PHI

7.18.5.1 A patient has a right to have the CBOH amend PHI or a record about him or her in a designated record set, for as long as the PHI is maintained in a designated record set. All request for amendments must be in writing and specify the reasons for the request, and shall be immediately forwarded to the HIPAA Privacy Officer, so that the CBOH can act on the request within 60 days of receipt. The request must be documented and retained in the patient's file, along with any statement of disagreement.

7.18.5.2 A patient's request for an amendment to his or her PHI may be denied only in the following circumstances: CBOH did not create the PHI and the creator is available to act on the requested amendment; the information to be amended is not part of the designated record set; the PHI is accurate and complete; or the information is not lawfully subject to access by the patient. If any part of the patient's request is denied, then the patient shall be notified of the reasons, and given an opportunity to submit a statement of disagreement and to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

7.18.6 Right to Request an Accounting of Disclosures of PHI

A patient has a right to receive an accounting of disclosures of PHI made by the CBOH in the six years prior to the date on which the accounting is requested. All requests for accounting must be made in writing, and immediately forwarded to the HIPAA Privacy Officer, so that the CBOH can act on the request within 30 days of receipt. The request should include the patient's name and specify the time period for which the accounting is being sought. The accounting must include disclosures of PHI for the time requested, including disclosures to or by Business Associates or for research purposes, date of the disclosure(s), name of the person or entity which received the PHI and, if known, the address, and a brief description of the information disclosed. A copy of the written request for an accounting and the accounting provided to the patient must be retained.

7.19 COMPLAINT PROCEDURES

Complaints about the CBOH's compliance with its privacy policies and procedures and the HIPAA Rule shall be forwarded immediately to the HIPAA Privacy Officer, along with as much information regarding the complaint as possible, including the complainant's name, contact information, date of incident, nature of complaint, to whom the PHI was improperly disclosed, any harmful effects that resulted, steps requested to limit the harm, and any additional comments. The HIPAA Privacy Officer will investigate or oversee the investigation of the complaint, determine the appropriate response, and provide a written

response to the complainant. Corrective action shall be taken as necessary, and appropriate sanctions will be imposed upon any employee who failed to comply with CBOH privacy policies or HIPAA requires. Documentation of complaints and their disposition will be retained by the HIPAA Privacy Officer.

7.20 SANCTIONS AGAINST EMPLOYEES FOR VILOATION OF POLICY

7.20.1 Sanctions

The CBOH shall apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the CBOH or the requirements of the HIPAA regulations. Any violation of these policies or the HIPAA Privacy Rule will be reported to the employee's supervisor, the HIPAA Privacy Officer, and Human Resources. Human Resources will make a recommendation to the employee's supervisor about the appropriate sanction based on the nature of the violation. The type of sanction will vary depending on the severity of the violation, whether it was intentional or unintentional, and whether the employee engaged in a pattern of improper use or disclosure of PHI. Sanctions may include a warning, additional training, reassignment of job functions, suspension, demotion, or other adverse actions up to and including termination of employment. The responsibility for training and managing the employee's job function will be considered. The employee will receive appropriate notice and opportunity to respond. Violations will be reviewed on a case by case basis; therefore, sanctions may vary depending on the nature of violation. However, sanction will be applied with consistency to the extent possible. Sanctions will be documented and retained by the Human Resources.

7.20.2 Disclosures by Whistleblowers

An employee shall not be subject to sanctions for the inappropriate disclosure of PHI if the employee believes in good faith that the CBOH has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the CBOH potentially endangers one or more patients, workers, or the public; and the disclosure is to (i) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the CBOH; or (ii) an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the CBOH; or (iii) an attorney retained by or on behalf of the employee for the purpose of determining the legal options of the employee.

7.20.3 Refraining from Intimidation or Retaliation

The CBOH may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any patient or other person for (i) filing of a complaint with the Secretary of the U.S. Department of Health and Human Services; (ii) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of the U.S. Department of Health and Human Services; or (iii) opposing any act or

practice made unlawful by this subchapter, provided the patient or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule.

7.21 RESPONDING TO SUSPECTED BREACH OF PHI

If any employee becomes aware of a possible acquisition, access, use or disclosure of protected health information that is not permitted under HIPAA regulations and this policy, the employee must report the security incident within 24 hours to the HIPAA Privacy Officer. All such incidents will be investigated by the Security Incident Response Team, and other staff as necessary, in accordance with the Personal Health Information Security Incident Response Protocol GC-09013E.

8.0 REVISION HISTORY

REVISION #	REVISION DATE	REVISION COMMENTS
0	September 1, 2013	Initial Issue
1	June 20, 2017	Annual Review and update formatting
2	June 11, 2020	Periodic review of policy, addition Section 5.8

9.0 RELATED FORMS

CBOH Form GC-09013A	*Business Associate Agreement*
CBOH Form GC-09013B	*Notice of Privacy Practices*
CBOH Form GC-09013C	*Authorization for Release of Protected Health Information*
CBOH Form GC-09013D	*Authorization for Release of Psychotherapy Notes*
CBOH Form GC-09013E	*Personal Health Information Security Incident Response Protocol*
CBOH Form GC-09013F	*Technological Safeguards for the Protection of Personal Health Information*

BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the Georgia Department of Public Health ("DPH") and <Contractor Name> ("Contractor") have entered into the attached Contract, whereby Contractor will provide functions, activities, or services to DPH involving the use of Protected Health Information ("PHI") as defined by Health Insurance Portability and Accountability Act of 1996 ("HIPAA");

WHEREAS, DPH is required by HIPAA to enter into a Business Associate Agreement with entities which provide functions, activities, or services on behalf of DPH involving the use of PHI;

NOW, THEREFORE, in consideration of the mutual promises contained herein, DPH and Contractor agree as follows:

1. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in HIPAA and Title XIII of the American Recovery and Reinvestment Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or "HITECH"), and in the implementing regulations of HIPAA and HITECH, now and as they may be amended in the future. Together HIPAA, HITECH, and their implementing regulations are referred to in this Agreement as the "Privacy Rule and the Security Rule."

2. Subject to the limitations of this Agreement, Contractor may use or disclose PHI only to the extent necessary to meet its responsibilities as set forth in the Contract, provided that such use or disclosure would not violate the Privacy Rule or the Security Rule if done by DPH.

3. Contractor warrants that the individuals described on Attachment D-1 require access to PHI in order to perform services under the Contract. Contractor shall update Attachment D-1 as necessary.

4. Contractor warrants that the individuals described on Attachment D-2 require access to a DPH information system in order to perform services under the Contract. Contractor shall notify the DPH Project Leader no less than 24 hours in advance if any other individuals will need access to the DPH information system

5. Contractor warrants that only individuals designated by title or name on Attachments D-1 and D-2 will request or access PHI from DPH, that they will only do so in the performance of services under the Contract, and that these individuals will only request the minimum necessary amount of information in order to perform those services.

6. The parties agree that Contractor is a "Business Associate" to DPH within the meaning of the Privacy and Security Rule. Contractor shall comply with all obligations of the Privacy Rule and Security Rule that apply to DPH, and shall comply with all Privacy Rule and Security Rule requirements that apply to Business Associates. Contractor further warrants that it maintains and follows written policies and procedures to achieve and maintain compliance with the Privacy and Security Rules that apply to Business Associates, and that it will update such policies and procedures as necessary in order to comply with the and changes to the Privacy and Security Rules. These policies and procedures, and evidence of their implementation, shall be provided to DPH upon request.

7. All communications related to compliance with this Agreement will be forwarded to the following Privacy and Security Contacts:

A. At DPH:

Meredith Grant
HIPAA Privacy Officer, Office of General Counsel
2 Peachtree Street, NW, 15th Floor
Atlanta, Georgia 30303
Meredith.Grant@dph.ga.gov
404-232-1682

Tamika Bass, CISA, CRISC, CBCP
Chief Information Security Officer, Office of Information Technology
2 Peachtree Street, NW, 12th Floor
Atlanta, Georgia 30303
Tamika.Bass@dph.ga.gov
404-463-0802

B. At Contractor: _____

_____

_____

8. Contractor further agrees:

A. Contractor will not request, create, receive, use or disclose PHI other than as permitted or required by this Agreement, the Contract, or law.

B. Contractor will establish, maintain and use appropriate administrative, physical, and technical safeguards to prevent loss, use, or disclosure of the PHI other than as provided for by this Agreement, the Contract, or law.

C. Contractor will implement and use administrative, physical, and technical safeguards that protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of DPH.

D. In addition to the safeguards described above, Contractor shall impose access controls that restrict access to PHI to the individuals listed on D-1 and D-2, as amended from time to time.

E. Contractor will password-protect and encrypt all electronic PHI for transmission and for storage on portable computers and media devices.

F. Contractor will mitigate, to the extent practicable, any harmful effect that result from a loss, use, or disclosure of PHI by Contractor in violation of the requirements of this Agreement, the Contract, or law. Contractor shall bear the costs of mitigation, which shall include the reasonable costs of credit monitoring or credit restoration when the use or disclosure results in exposure of information commonly used in identity theft (including name, date of birth, and Social Security Number.)

G. Contractor will maintain a written Business Associate Agreement with any agent or subcontractor that will create, receive, maintain, or transmit on Contractor's behalf any PHI pertaining to DPH. Such Agreement shall provide that Contractor's agent or subcontractor agrees to the same restrictions and conditions of this Agreement with

respect to PHI that Contractor receives from DPH, and that Contractor's agent or subcontractor assumes the same duties with regard to the PHI that Contractor has assumed under this Agreement. Contractor further agrees that if it becomes aware of a pattern of activity or practice of its agent or subcontractor that constitutes a material breach or violation of its agreement with Contractor, then Contractor shall take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the agreement.

H. Contractor will immediately report to DPH any "Breach" as defined by 45 CFR 164.402, and any known or suspected loss, use, or disclosure of PHI that is not authorized by this Agreement, the Contract, or law.

I. Make an initial report to DPH in writing in such form as DPH may require within three business days after Contractor learns of a suspected unauthorized loss, use, or disclosure of PHI. This report will include the following:

i. The nature of the loss, use, or disclosure, a brief description of what happened, the date it occurred, and the date Contractor discovered the incident;

ii. The specific data points of PHI involved in the loss, use, or disclosure;

iii. The names of all persons with knowledge of the loss, use, or disclosure, and the names or categories of persons who may have obtained access to the PHI as a result;

iv. The corrective or investigative actions taken or to be taken in order to mitigate harmful effects, and to prevent further losses, uses, or disclosures;

v. Recommended protective actions to be taken by individuals whose PHI may have been lost, used, or disclosed; and

vi. Whether Contractor believes that the loss, use, or disclosure constitutes a Breach.

J. Contractor will, upon request by the DPH Privacy Officer or the DPH Information Security Officer, provide a complete report of the Breach to DPH including a root cause analysis and a proposed corrective action plan. Upon request by DPH, Contractor shall implement the corrective action plan and provide proof of implementation.

K. Contractor will report to the DPH Privacy Officer and the DPH Information Security Officer any successful unauthorized access, modification, or destruction of PHI or interference with system operations in Contractor's information systems as soon as practicable but in no event later than three business days of discovery.

L. Contractor will cooperate with DPH and provide assistance necessary for DPH to determine whether a Breach has occurred, and whether notification of the Breach is legally required or otherwise appropriate.

M. If DPH determines that a Breach has occurred as a result of Contractor's loss, use, or disclosure of PHI or failure to comply with obligations set forth in this Agreement or in the Privacy or Security Rule, then Contractor will provide all required notices to affected individuals, the Secretary of the U. S. Department of Health and Human

Services, and the media, at Contractor's expense and in accordance with 45 C.F.R. Part 164 subpart D. Such notices shall be submitted in advance to the DPH Privacy Officer for approval.

N. Contractor will honor requests by DPH or by an individual for access to the individual's own PHI in accordance with 45 CFR 164.524; to make PHI available for amendment, and to incorporate such amendments into a designated record set in accordance with 45 CFR 164.526; to provide an accounting of all disclosures of the individual's PHI in accordance with 45 CFR 164.528; to document any such requests and the Contractor's response; and to notify DPH as soon as practicable of any such requests.

O. Contractor will provide access to the Secretary of the U.S. Department of Health and Human Services to Contractor's books and records and policies, practices, or procedures relating to the use and disclosure of PHI received from DPH, or created or received by Contractor on behalf of DPH.

P. In addition to any indemnification provisions in the Contract, Contractor will indemnify DPH from any loss or liability resulting from any violation of the HIPAA Privacy and Security Rules or Breach that arises from the conduct or omission of Contractor or its employees, agents, or subcontractors. Such liability will include without limitation all actual and direct costs, settlement payments, damages awarded, civil penalties, litigation expenses, and attorneys' fees incurred by DPH.

9. Unless otherwise provided by law, DPH agrees that it will:

A. Notify Contractor of any new limitation in DPH's Notice of Privacy Practices in accordance with the provisions of the Privacy Rule if such limitation will affect Contractor's use or disclosure of PHI.

B. Notify Contractor of any change in, or revocation of, permission by an individual for DPH to use or disclose PHI if such change or revocation will affect Contractor's use or disclosure of PHI.

C. Notify Contractor of any restriction regarding its use or disclosure of PHI that DPH has agreed to in accordance with the Privacy Rule if such restriction will affect Contractor's use or disclosure of PHI.

D. Before agreeing to any changes in or revocation of permission by an individual, or any restriction to use or disclose PHI, DPH will contact Contractor to determine feasibility of compliance. DPH agrees to assume all costs incurred by Contractor in compliance with such special requests.

10. The effective date of this Agreement shall be the same as that of the Contract. Unless otherwise terminated, this Agreement shall continue until all of the PHI provided by DPH to Contractor, or created or received by Contractor on behalf of DPH, is destroyed or returned to DPH.

A. Termination for Cause. Upon violation of a material term of this Agreement by Contractor, DPH may provide an opportunity for Contractor to cure the breach and, if Contractor fails to cure the breach, terminate the contract upon 30 calendar days' notice.

B. Termination for Convenience. In the event that the Contract is terminated for any

reason, then DPH may terminate this Agreement for convenience.

C. Effect of Termination.

i. Upon termination of this Agreement, DPH shall determine whether return or destruction of PHI is feasible. If so, then Contractor shall at the direction of DPH either destroy the PHI or to return it to DPH, keeping no copies. If DPH determines that return or destruction is not feasible, then Contractor shall continue to extend the protections of this Agreement to the PHI for as long as Contractor maintains the PHI, and shall limit the use and disclosure of the PHI to those purposes that make the return or destruction of the PHI infeasible.

ii. The obligations imposed upon Contractor with respect to its care, use, and disclosure of PHI, and its duty to comply with the Privacy and Security Rule with regard to such PHI, shall survive the termination of this Agreement and the termination or completion of the Contract.

11. Nothing in this Agreement is intended to confer any rights, remedies, obligations, or liabilities upon anyone other than DPH and Contractor.

12. This Agreement is intended to supplement, and not to diminish or alter, the terms and conditions of the Contract.

<Contractor Name>

BY: _____
SIGNATURE

_____
TITLE

_____
DATE

ATTACHMENT D-1

Individuals Permitted to Receive, Use, and Disclose DPH PHI

The following individual, as employees or agents of Contractor, need access to DPH Protected Health Information in order for Contractor to perform the services described in the Contract:

- _____ Title: _____
- _____ Title: _____
- _____ Title: _____
- _____ Title: _____
- _____ Title: _____

Approved methods of secure delivery of PHI between Contractor and DPH:

- Secure FTP file transfer (preferred)
- Encrypted email or email sent through "secure tunnel" approved by DPH Information Security Officer
- Email of encrypted document (password must be sent by telephone only)
- Encrypted portable media device and tracked delivery method

Contractor must update this list as needed and provide the updated form to the DPH Project Leader. Use of DPH Protected Health Information by individuals who are not described on this Attachment D-1, as amended from time to time, is a violation of the Agreement.

DPH Project Leader Contact Information:

_____

_____

_____

ATTACHMENT D-2

Part 1:

Please initial beside the correct option. Please select only one option.

_____ Contractor DOES NOT need any user accounts to access DPH Information Systems. Do not complete Part 2 of this form.

_____ Contractor DOES need user accounts to access DPH Information Systems. Please complete Part 2 of this form.

Part 2:

Please complete the table below if you indicated that Contractor DOES need any user accounts to access DPH Information Systems. Please attach additional pages if needed.

List of Individuals Authorized to Access a DPH Information System Containing PHI

The following individuals, as employees or agents of Contractor, need access to DPH Information Systems containing DPH Protected Health Information in order for Contractor to perform the services described in the Contract:

Full Name	Employer	DPH Information System	Type of Access (Read only? Write?)

The DPH Project Leader must submit a completed DPH Network Access Request Form for each individual listed above, and for anyone who might later be added to this list.

Contractor must notify the Project Leader identified in the Contract immediately, but at least within 24 hours, after any individual on this list no longer needs the level of access described. Failure to provide this notification on time is a violation of the Agreement.

Contractor must update this Attachment D-2 as needed and provide the updated form to the DPH Project Leader.

[DPH Form GC-00901A (Rev. 08.24.2018)]

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Georgia Department of Public Health (DPH) to maintain the privacy of your health information, inform you of its legal duties and privacy practices with respect to your health information through this Notice of Privacy Practices, notify you if there is a breach involving your protected health information, agree to restrict disclosure of your health information to your health plan if you pay out-of-pocket in full for health care services, and abide by the terms of this Notice currently in effect. We reserve the right to change the terms of this Notice at any time. The Notice will be posted on the DPH website at www.dph.georgia.gov. Copies of the Notice are available upon request.

The Department of Public Health and the County Boards of Health will follow this Notice.

HOW WE MAY USE AND DISCLOSE YOUR HEALTH INFORMATION

Treatment: We may use or disclose your health information to provide you with treatment or services. County Boards of Health may disclose your health information to doctors, nurses or other healthcare personnel involved in your care. For example, County Boards of Health may share your information with programs involved in your follow-up care, such as the Babies Can't Wait program. Also, the DPH Public Health Laboratory will return lab test results to the person who ordered the tests, and those results may be used for your treatment or follow-up care.

Payment: We may use or disclose your health information to bill and collect payment for the services that you receive. For example, your health insurance company may need to provide your health plan with information about the treatment you received so that it can make payment or reimbursement for services provided to you.

Health Care Operations: We may use and disclose information about you for health care operations. For example, we may review treatment and services to evaluate the performance of our staff in caring for you, and to determine what additional services should be provided.

Appointment Reminders, Follow-Up calls: We may use or disclose medical information about you to remind you of an upcoming appointment or to check on you after you have received treatment.

Individuals Involved in Your Care: If you do not object, we may disclose your health information to a family member, relative, or close friend who is involved in your care or assists in taking care of you. We may also disclose information to someone who helps pay for your care. We may disclose your health information to an organization assisting with disaster relief to help notify your family member, relative, or close friend of your condition, status and location.

Business Associates: We may disclose your information to contractors (business associates) who provide certain services to us. We will require these business associates to appropriately safeguard your information.

Public Health Activities: We may disclose your health information for public health activities which include: preventing or controlling disease, injury or disability; reporting child abuse or neglect; reporting reactions to medications or problems with products or notifying a person of product recalls; and notifying a person who may have been exposed to a disease or may be at risk of contracting or spreading a disease or condition.

Victims of Abuse, Neglect or Domestic Violence: We may disclose your medical information to notify the appropriate government authority if we believe you have been the victim of abuse, neglect or domestic violence. We will only disclose this if you agree, or when required or authorized by law or regulation.

Health Oversight Activities: We may disclose your health information to a health oversight agency that is authorized to conduct audits, investigations, inspections, licensure and other activities necessary to monitor the health care system, government programs and compliance with civil rights laws.

Health Information Exchange: We may disclose your health information to the Georgia Health Information Network, Inc. (GaHIN), the statewide health information exchange network through which we securely share and access medical information in accordance with applicable state and federal laws and regulations. This exchange of information allows us to provide you with access to better treatment and coordination of healthcare services. GaHIN has established Network Operating Policies and Technical Requirements, which members and member affiliates of GaHIN must meet, to ensure the confidentiality and integrity of data.

Judicial and Administrative Proceedings: We may disclose your health information if ordered to do so by a court or administrative tribunal that is handling a lawsuit or other dispute. We may also disclose your health information in response to a subpoena, discovery request, or other lawful process, but only if reasonable efforts have been made to notify you of the request or to protect the health information requested.

Law Enforcement: We may release health information to law enforcement to comply with a court order, warrant, subpoena or similar process in order to identify or locate a suspect, fugitive, material witness or missing person about the victim of a crime in certain circumstances. For example, if we believe a death resulted from criminal conduct, to report a crime occurring on our premises in emergencies, to report a crime, the location or victims of the crime, or the identity, description and location of the person committing the crime.

Research: Under certain circumstances we may use or disclose your health information for research. In most cases, we will ask for your written authorization before doing so. Sometimes, we may use or disclose your health information for research without your written authorization. In those cases, the use or disclose of your health information without your consent will be approved by an Institutional Review Board or Privacy Board.

Coroners, Medical Examiner and Funeral Directors: We may disclose health information to a coroner or medical examiner. This may be necessary, for example, to determine the cause of death. We may also disclose medical information to funeral directors as necessary to carry out their duties.

To Avert a Serious Threat to Health or Safety: We may use or disclose your health information if necessary to prevent or lessen a serious and imminent threat to your safety, another person, or the general public. We will only disclose your information to a person who can prevent or lessen that threat.

National Security and Intelligence Activities and Protective Services for the President: We may disclose your health information to authorized federal officials conducting intelligence and other national security activities. We may also disclose your health information to authorized federal officials for the provisions of protective services to the President, other authorized persons, foreign heads of state or to conduct special investigations.

Military and Veterans: We may disclose the health information of Armed Forces personnel to appropriate military command authorities for the execution of their military mission. We may also disclose health information about foreign military personnel to foreign military authorities.

Inmates: If you are an inmate, we may disclose your health information to the law enforcement official or correctional institution having custody to provide you with health care, and to protect your health or safety or that of other inmates or persons involved in supervising or transporting inmates.

Workers' Compensation: We may release your health information for workers' compensation or similar programs that provide benefits for work-related injuries.

As Required by Law: We will disclose your health information when required to do so by law.

Except in limited circumstances, we must obtain your authorization for 1) any use or disclosure of psychotherapy notes, 2) any use or disclosure of your health information for marketing, and 3) the sale of your health information. If your health information has information relating to mental health, substance abuse treatment, or HIV/ AIDS, we are required by law to obtain your written consent before disclosing such information. Any other use or disclosure not mentioned in this Notice will be made only with your written authorization, and you can revoke that authorization at any time. The revocation must be in writing, but will not apply to disclosures made in reliance on your prior authorization.

YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION

Right to Inspect and Copy: You have the right to inspect and copy your records. You must submit your request in writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street, N.W., 15th Floor, Atlanta, Georgia, 30303, and include your name, date of birth, social security number, and the location where services were received if you received services at a local county health department. We may deny your request and in some circumstances, you may request a review of the denial.

Right to Request an Amendment of PHI: You may request that we amend information that we have about you, for as long as we keep that information. You must submit your request in writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street, N.W., 15th Floor, Atlanta, Georgia, 30303, and include your name, date of birth, social security number, a reason that supports your request, and the location where services were received if you received services at a local county health department. Your request may be denied if 1) the information was not created by us unless the creator of the information is not available to make the requested amendment, 2) the information is not kept by us, 3) the information is not available for your inspection, or 4) the information is accurate and complete.

Right to an Accounting of Disclosures: You have the right to receive an accounting of disclosures of your health information made by us in the six years prior to the date on which the accounting is requested. The accounting will not include any disclosures 1) to you or your personal representative, 2) made pursuant to your written authorization, 3) made for treatment, payment or business operations, 4) made to your friends and family involved in your care or payment for your care, 5) that were incidental to permissible uses or disclosures of your health information, 6) of limited portions of your health information that excludes identifiers, 7) made to federal officials for national security and intelligence activities, and 8) to correctional institutions or law enforcement officers about inmates. To request an accounting of disclosures, submit your request in writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street, N.W., 15th Floor, Atlanta, Georgia, 30303. Please include your name, date of birth, social security number, the period for which the accounting is being requested, and the location where services were received if you received services at a local county health department.

Right to Request Restrictions: You may request that we restrict the way we use and disclose your health information for treatment, payment or health care operations. You may also request that we limit how we disclose your health information to a family member, relative or close friend involved in your care or payment for your care. We are not required to agree to your request, but if we do, we will comply with your request unless you need emergency treatment and the information is needed to provide the emergency treatment. We may terminate our agreement to a restriction once we notify you of the termination. To request a restriction on the use or disclosure of your health information, please send your request in writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street N.W., 15th Floor, Atlanta, Georgia 30303. Please include your name, social security number, and date of birth, what information you want to limit, to whom you want the limitation to apply, and the location where services were received if you received services at a local county health department.

Right to Request Confidential Communications: You may make reasonable requests to receive communications of your health information by alternate means or at alternate locations. For example, you may ask to be contacted only by mail, and not by phone. To request confidential communications, please send your request in writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street N.W., 15th Floor, Atlanta, Georgia 30303. Please include your name, social security number, date of birth, how you would like to be contacted, and the local county health department where you received services.

Right to Receive a Paper Copy of this Notice: You have a right to receive a paper copy of this Notice, which you may request at any time. You may obtain a paper copy by writing to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street N.W., 15th Floor, Atlanta, Georgia 30303.

COMPLAINTS

If you believe that your privacy rights have been violated, you may send a written complaint to the Privacy Officer, Office of the General Counsel, Georgia Department of Public Health, 2 Peachtree Street N.W., 15th Floor, Atlanta, Georgia 30303. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services. There will be no retaliation for filing a complaint.

FOR FURTHER INFORMATION

For further information you may contact the DPH Privacy Officer, Office of the General Counsel at (404) 657-2700.

THIS NOTICE IS EFFECTIVE 27 MARCH 2017.

Georgia Department of Public Health

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

NAME OF INDIVIDUAL/PATIENT	
DATE OF BIRTH	
ADDRESS	**CITY/STATE/ ZIP**

1. I hereby voluntarily authorize _____ to disclose the medical information indicated below to _____.
2. The purpose for this disclosure is for _____.
3. The information to be disclosed is:

   ___ Entire Medical Record
   ___ Only medical information from the period _____ to _____.
   ___ Other (specify) _____

   If you would like any of the following sensitive information disclosed, please indicate with a check mark below:
   ___ Alcohol/ Drug Abuse Treatment
   ___ HIV/ AIDS- related Treatment
   ___ Mental Health (other than psychotherapy notes*)

4. This authorization shall become effective immediately and shall remain in effect until _____ (date) or for one year from the date of signature if no date is entered.

I understand that I may revoke this authorization in writing at any time prior to the release of information from DPH, and that revocation will not affect any action taken in reliance on this authorization before the written revocation was received.

I understand that my eligibility for benefits, treatment or payment is not conditioned upon my provision of this authorization.

I understand that information disclosed by this authorization may be subject to re-disclosure by the recipient and no longer protected by the Health Insurance Portability and Accountability Act.

_____ Print Patient's Name

_____ Patient's Signature

_____ Print Authorized Representative's Name (if applicable)

_____ Authorized Representative's Signature (if applicable)

_____ Date

**Psychotherapy notes* means notes recorded 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. 45 C.F.R. 164.501.

Georgia Department of Public Health

AUTHORIZATION FOR RELEASE OF PSYCHOTHERAPY NOTES

NAME OF PATIENT	
DATE OF BIRTH	
ADDRESS	CITY/STATE/ ZIP

1. I hereby voluntarily authorize _____ to disclose any psychotherapy notes that may be in my medical files to _____.

2. The purpose for this disclosure is for _____.

3. This authorization shall become effective immediately and shall remain in effect until _____ (date) or for one year from the date of signature if no date is entered.

I understand that I may revoke this authorization in writing at any time prior to the release of information from DPH, and that revocation will not affect any action taken in reliance on this authorization before the written revocation was received.

I understand that my eligibility for benefits, treatment or payment is not conditioned upon my provision of this authorization.

I understand that information disclosed by this authorization may be subject to re-disclosure by the recipient and no longer protected by the Health Insurance Portability and Accountability Act.

_____ Print Patient's Name

_____ Patient's Signature

_____ Print Authorized Representative's Name (if applicable)

_____ Authorized Representative's Signature (if applicable)

_____ Date

Psychotherapy notes means notes recorded 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. 45 C.F.R. 164.501.

Georgia Department of Public Health

Form GC-09013E

GEORGIA DEPARTMENT OF PUBLIC HEALTH
PERSONAL HEALTH INFORMATION SECURITY
INCIDENT RESPONSE PROTOCOL

This protocol sets out the procedures for responding to an actual or suspected personal health information security incident, and the responsibilities of persons tasked to respond to such incidents.

A **Security Incident** is an actual, suspected, or attempted loss or disclosure of individually identifiable personal health information within the custody or control of a DPH or County Board of Health employee. A Security Incident can take place in many different ways: the loss of a disk or laptop computer containing PHI, a malfunction or unauthorized attempt to enter into an information system on which PHI is stored, disclosure of PHI by email or telephone to the wrong person, an unauthorized modification or destruction of data, leaving papers with PHI in plain sight in a common area, etc.

A Security Incident shall be declared to be a **Breach** if protected health information was acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

The **Security Incident Response Team** consists of the DPH Privacy Officer and the DPH Information Security Officer. Depending on the circumstances of the incident, they may request the support of the Director of Communications or the Inspector General. If the Security Incident involves PHI within the custody of a county or District office, then the District Privacy Officer and District MIS Director will be on the Response Team.

Step One: Investigation.

Any event that might possibly be a Security Incident shall be reported immediately to the Privacy Officer or Information Security Officer. The Security Incident Response Team shall immediately investigate the event, including personal interviews of any person who might have knowledge of the facts, and shall include the Director of Communications and Inspector General if necessary.

At the conclusion of the investigation, the Response Team shall decide whether there has been a Breach. The incident shall not be considered a Breach in the following circumstances:

- The acquisition, access, or use of the PHI was by a DPH employee or business associate in good faith and within the scope of their authority, and there was no further use or disclosure in violation of HIPAA;

- An inadvertent disclosure of PHI was made by a DPH employee or business associate authorized to access PHI to another DPH employee or business associate authorized to access PHI, and there was no further use or disclosure in violation of HIPAA;

- The PHI was disclosed to an unauthorized recipient, but there is a good faith belief that the recipient would not reasonably have been able to retain the PHI; or

- A risk assessment of the following factors by the Security Incident Response Team shows that there is a low probability that the PHI was compromised:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.

Step Two: Response.

Regardless of whether or not the Security Incident is deemed to be a Breach, the Security Incident Response Team shall develop and implement a plan to accomplish the following:

- Ensure that the conditions that made the incident possible are corrected so as to prevent future incidents. This may include recommendations for further training of employees, or changes to office technology, training, policy, or procedures.

- Identify individuals whose PHI was or may have been disclosed, and the persons or entities to whom PHI was or may have been disclosed.

- Mitigate any possible harm that may have resulted from the incident.

- Recommendations to the Office of Human Resources or District Health Director for disciplinary actions against persons responsible for the incident, if warranted.

Step Three: Notifications.

If the Security Incident Response Team determines that there has been a Breach, then the Privacy Officer will advise on how to provide notice of Breach as required by law.

1. **To Affected Individuals**: Notice of a Breach shall be given to each affected individual. The Privacy Officer will prepare the notice in accordance with 45 CFR 164.404(c), and the program will be responsible to ensure that the notices are sent. The notice shall be written in plain language and contain the following:

    - The date of breach, the date it was discovered, and a brief description of what happened;
    - A description of the types of PHI that were involved (*e.g.,* full name, Social Security number, date of birth, home address, account numbers, diagnoses, disability codes, etc.);
    - Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
    - A description of what DPH is doing to investigate the breach, mitigate harm to

individuals, and protect against further breaches; and
- Contact information for individuals to ask questions or learn additional information, such as an email address, website, or mailing address.

The notice shall be sent by first-class mail to each individual's last known address; by email, if the individual has agreed to electronic notice; or to the next of kin or personal representative, if deceased. The Privacy Officer may approve another form of notice in accordance with 45 CFR 164.406 if the contact information for an individual or group of individuals is insufficient or out-of-date.

2. **To Others:** If there are more than 500 affected individuals, then the Privacy Officer shall prepare a notice of the Breach for the Director of Communications to distribute to prominent media outlets serving Georgia no later than sixty days from discovery of the Breach. In addition, the Privacy Officer will provide notice to the Secretary of the U. S. Department of Health and Human Services as required by 45 CFR 164.408 contemporaneously with the notice to individuals, but no later than sixty days after discovery of the breach.

Step Four: Documentation.

At the conclusion of every investigation, the Privacy Officer shall ensure that a file is prepared and maintained to document the facts of the incident, the basis for the determination that there was or was not a Breach, the response, and proof that all notices required by law were made.

Public Health
Prevent. Promote. Protect.

COUNTY BOARD OF HEALTH
SAFEGUARDS FOR THE PROTECTION OF
ELECTRONIC PERSONAL HEALTH INFORMATION

The CBOH must ensure the confidentiality, integrity and availability of all electronic PHI that it creates, receives, maintains or transmits, must protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA regulations.

The CBOH may use any security measures that allow it to reasonably and appropriately implement the standards and specifications required by HIPAA. In deciding which security measures to use, the CBOH shall take into account its size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; the cost of security measures; and the probability and criticality of potential risks to electronic PHI.

Administrative Safeguards

1. **Security Management.** The CBOH shall prevent, detect, contain, and correct security violations, and shall do the following:

    a. **Risk Analysis.** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the Department;
    b. **Risk Management.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the requirements contained in the introductory paragraphs above;
    c. **Periodic Review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. **HIPAA Security Officer.** The Information Technology Director shall serve as the HIPAA Security Officer responsible for the development and implementation of the information security policies and procedures required by this Form to ensure compliance with HIPAA security regulations.

3. **Workforce Security.** The HIPAA Security Officer must implement policies and procedures to ensure that employees only have such access to electronic PHI as is appropriate for their duties, and to prevent other employees from obtaining access to electronic PHI, including the following:

    a. **Authorization and Supervision.** Implement procedures for the authorization and supervision of employees who work with electronic PHI, or in locations where it might be accessed;
    b. **Workforce Clearance.** Implement procedures to determine that the access of an employee to electronic PHI is appropriate;

c. **Termination of access.** Implement procedures for terminating access to electronic PHI when the employment of an employee ends.

4. **Information Access Management**. The HIPAA Security Officer must implement policies and procedures for authorizing access to electronic PHI that are consistent with HIPAA requirements, including the following:

   a. **Access Authorization.** Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, program, process or other means;
   b. **Access Establishment and Modification.** Implement policies and procedures that, based upon the CBOH's access authorization policies, establish, document, review and modify a user's right of access to a workstation, program or process.
   c. **Security Reminders.** Provide periodic security updates as needed;
   d. **Malicious Software.** Implement procedures for guarding against, detecting, and reporting malicious software;
   e. **Log-in Monitoring.** Implement procedures for monitoring log-in attempts and reporting discrepancies;
   f. **Password Management.** Implement procedures for creating, changing, and safeguarding passwords.

5. **Contingency Plan**. The HIPAA Security Officer must establish and implement as necessary, policies and procedures for responding to an emergency or other occurrence that damages a system containing electronic PHI, including the following:

   a. **Data Backup Plan.** Establish and implement procedures for a data back-up plan, to create and maintain retrievable exact copies of electronic PHI;
   b. **Disaster Recovery Plan.** Establish and implement procedures as needed, for a disaster recovery plan to restore any loss of data;
   c. **Emergency Mode Operation Plan.** Establish and implement procedures as needed, for an emergency mode operation plan, to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
   d. **Testing and Revision.** Implement procedures for periodic testing and revision of contingency plans.
   e. **Application and Data Criticality Analysis.** Assess the relative criticality of specific applications and data in support of other contingency plan components.

6. **Evaluation**. The HIPAA Security Officer must perform a periodic technical evaluation to ensure that CBOH security policies and procedures meet the requirements of this Policy.

Physical Safeguards

1. **Facility Access Controls.** The HIPAA Security Officer must implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, but ensure that authorized access is allowed, including the following:

   a. **Contingency Operations:** Establish and implement procedures as necessary that allow facility access to support the restoration of lost data under the disaster recovery and emergency mode operations plans in the event of an emergency;

b. **Facility Security Plan:** Implement policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering, and theft;
c. **Access Control and Validation:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and to control access to software programs for testing and revision;
d. **Maintenance Records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility related to security (*e.g.*, walls, hardware, doors, and locks).

2. **Workstation Use**. The HIPAA Security Officer must implement policies and procedures that specify the proper functions to be performed, the way in which these functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI.

3. **Workstation Security**. The HIPAA Security Officer must implement physical safeguards for all workstations that access electronic PHI, to restrict access by unauthorized users.

4. **Device and Media Controls**. The HIPAA Security Officer must implement policies and procedures for the receipt and removal of hardware and electronic media containing electronic PHI into and out of a facility, as well as the movement of these items within a facility, including the following:

   a. **Disposal.** Implement policies and procedures to address the final disposition of electronic PHI, and the hardware or electronic media that stores it;
   b. **Re-Use of Media.** Implement procedures for removal of electronic PHI from electronic media prior to the media being made available for re-use.
   c. **Accountability.** Maintain a record of the movements of hardware and electronic media and anyone person responsible for such movements;
   d. **Data Back-up and Storage.** Create a retrievable, exact copy of electronic PHI, when needed, before moving equipment.

Technical Safeguards

1. **Access Control**. The HIPAA Security Officer must implement technical policies and procedures for information systems that maintain electronic PHI, which allow access only by those persons or software programs that have access rights, including the following:

   a. **Unique User ID.** Assign a unique name or number for tracking and identifying user identity;
   b. **Emergency Access Procedure.** Establish and implement procedures as needed to obtain necessary electronic PHI during an emergency.
   c. **Automatic Log-off.** Implement procedures to terminate an electronic session after a certain period of inactivity;
   d. **Encryption.** Implement a mechanism to encrypt and decrypt electronic PHI.

2. **Audit Controls**. The HIPAA Security Officer must implement hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

3. **Integrity**. The HIPAA Security Officer must implement policies and procedures to protect electronic PHI from improper alteration or destruction, and to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

4. **Person or Entity Authentication**. The HIPAA Security Officer must implement procedures to verify that a person or entity seeking to access electronic PHI is the one claimed.

5. **Transmission Security**. The HIPAA Security Officer must implement technical security measures to guard against unauthorized access to electronic PHI being transmitted over an electronic communications network, including the following:

    a. **Integrity Controls.** Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified during transmission;
    b. **Encryption.** Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

Documentation

The HIPAA Security Officer must maintain the policies and procedures implemented to comply with this section in written format. A copy must be provided to the HIPAA Privacy Officer. The documentation must be reviewed periodically and updated as needed due to environmental or operational changes affecting the security of electronic PHI. Procedures followed in the event of a security incident and the outcome must also be documented. The documentation must be kept for six years from the date of its creation or the date when it was last in effect, whichever is later.