CITY AND COUNTY OF BROOMFIELD
One DesCombes Drive • Broomfield, CO 80020 • 303.469.3301 • www.broomfield.org

City and County of Broomfield

HIPAA Compliance Plan

Policies & Procedures

June 28, 2022 Revision Date

TABLE OF CONTENTS

Section 1: Overview and Definitions

ADMINISTRATIVE POLICY

CITY AND COUNTY OF BROOMFIELD

DESIGNATION AS A HYBRID ENTITY UNDER HIPAA

Policy Statement: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and all regulations promulgated thereunder (hereinafter collectively referred to as "HIPAA") comprise United States legislation that provides data privacy and security provisions for safeguarding certain protected health information (PHI) and electronic protected health information (ePHI). HIPAA applies to covered entities, which include (1) health plans; (2) health care clearinghouses; and (3) health care providers that transmit health information in electronic form in connection with a transaction covered by HIPAA, as well as business associates whose services involve the use of PHI obtained from a covered entity.

Although the City and County of Broomfield (City of Broomfield) as a whole does not primarily engage in these functions, the performance by some departments within the City of Broomfield of certain functions causes the City of Broomfield to be included within the definition of a covered entity under HIPAA. Entities such as the City of Broomfield that have both covered components and non-covered components may choose to be designated as a hybrid entity.

The purpose of this policy is to designate the City of Broomfield as a hybrid entity under HIPAA and to define how the City of Broomfield will identify departments as health care components pursuant to HIPAA regulations. In this case, while the City of Broomfield remains responsible for oversight, compliance and enforcement obligations, certain other requirements of HIPAA will only apply to the health care components of the City of Broomfield.

Health Care Component Designation: The City of Broomfield HIPAA Privacy Program will, in consultation with the appropriate administrators and other qualified personnel, identify those departments, programs or other functions that comprise health care components which are required to comply with the standards of the HIPAA Privacy and Security Rules. The HIPAA Privacy Program will, not less than annually, review the activities of the City of Broomfield's departments, programs and other functions to assess whether any modifications to the designated health care components should be made. Such determination will be

based on whether the unit meets the definition outlined below. The results of the review will be documented in written format and maintained for a period of six (6) years.

The following criteria will be utilized in determining whether a department constitutes a health care component that is required to comply with HIPAA regulations:

- A department that would meet the definition of a covered entity if it were a separate legal entity.
- A department that performs covered functions or transactions under HIPAA.
- A department that performs activities that would make it a business associate if it were a separate legal entity.

As applicable to the City of Broomfield's hybrid designation, a business associate is: (a) a department which another covered entity or an organized health care arrangement (OHCA) (as defined in 45 CFR § 160.103), performs or assists in the performance of a function or service that involves the use or disclosure of individually identifiable health information, or any other function regulated by the subchapter; or (b) a department which provides legal, actuarial, accounting, consulting, data aggregation, management, accreditation, administrative, or financial services to or for the City, covered entity or OHCA from another business associate.

The departments listed in Section 6 have been designated as health care components and are therefore required to comply with applicable HIPAA regulations. This Appendix may be amended from time to time to reflect which agencies, departments, subdivisions or other units meet the applicable criteria for a health care component designation.

General Safeguard Requirements: In general, the City of Broomfield's health care components are the only units within the entity that have the right to use, maintain, access or transmit PHI or ePHI. Health care components within the City of Broomfield may not impermissibly use or disclose PHI or ePHI to non-covered components unless allowed under HIPAA. Further, health care components must protect ePHI with respect to another health care component in the same HIPAA compliant manner and as if the components were separate and distinct legal entities.

A member of the City of Broomfield's workforce that performs duties for both a health care component and a non-health care component shall not use or disclose PHI created or received in the course of the member's duties for the health care component while performing duties for the non-health care component if such disclosure would be prohibited by HIPAA or the City of Broomfield's HIPAA policies and procedures.

Technical Safeguard Requirements: The City of Broomfield shall implement procedures and technical safeguards to limit access to PHI by members of its workforce that perform duties for the non-covered components. These procedures and safeguards shall include, but not be limited to, access control and validation procedures to limit unauthorized access to electronic records containing PHI.

The City of Broomfield shall maintain technical safeguards between its health care components and non-covered components such that the non-covered components are unable to access PHI maintained electronically by the covered components.

Compliance: The City of Broomfield as a whole entity must ensure that the health care components of the entity comply with HIPAA. The City of Broomfield's Privacy Officer is responsible for facilitating compliance with this Policy and all questions that arise concerning the designation of health care components and non-covered components, or the disclosure of PHI from a health care component to a non-health care component. The Privacy Officer, in consultation with the City of Broomfield's City Attorney's Office, shall have the authority to make final determinations regarding designation of health care components or the disclosure of PHI from a health care component to a non-health care component. All members of the City of Broomfield workforce are responsible for compliance with this policy.

Employees of the City of Broomfield who violate this policy may be subject to corrective action for misconduct and/or performance based on the administrative process appropriate to their employment or other status.

HIPAA Overview And Timelines

The Health Insurance Portability and Accountability Act (*HIPAA) Privacy Rule* is a set of federal standards to protect the privacy of an individual's medical records and other health information maintained by those departments and agencies within the City and County of Broomfield (CCOB) which are designated health care components (CCOB Health Care Components). These standards provide individuals with access to their health records and with significant control over how their protected health information is used and disclosed. Compliance with the standards was required as of April 14, 2003.

The *HIPAA Security Rule* establishes national standards for the security of electronic protected health information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures to assure the confidentiality, integrity and security of electronic protected health information. The standards are delineated into either required or addressable implementation specifications. Compliance with the standards was required as of April 20, 2005, for most entities covered by HIPAA. The authority to administer and enforce the Security Rule was transferred to Department of Justice Office for Civil Rights on July 27, 2009.

The *HIPAA Enforcement Rule* contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The final interim Enforcement Rule was published in October of 2009 as part of the HITECH Act.

The *HIPAA Breach Notification* for Unsecured Protected Health Information (PHI), as part of 45 CFR (Code of Federal Regulations) Parts 160 and 164, was updated in August of 2009 and governs the actions CCOB would take if a breach occurred within one of its health care components of the designated CCOB Hybrid Entity.

CCOB has designated itself as a "hybrid entity" under HIPAA because it conducts business activities that include both non-covered and covered HIPAA functions. Agencies, departments and subdivisions that are covered health care components and that are required to comply with HIPAA regulations have been identified. CCOB Designation as a Hybrid Entity under HIPAA is included in Section 1 of this document.

Definitions:

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

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.

Authentication: The corroboration that a person is the one claimed.

Availability: Data or information is accessible and useable upon demand by an authorized person.

Breach: A breach generally is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

Business Associate: A business associate is a person or entity who provides certain functions, activities, or services for/to a CCOB health care component involving the use and/or disclosure of PHI. A business associate is not a CCOB employee.

Confidentiality: Property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity: The business units identified in Section 6 of this document are HIPAA covered health care components of the CCOB which means the rules and regulations pertaining to HIPAA must be followed and enforced.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Designated record set: A group of records maintained by the components that includes:

- Medical and billing records
- Enrollment, payment, claims adjudication, and case or medical records
- Other records used to make decisions about an individual's health

Electronic PHI: The electronic form of individually identifiable health information.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Enforcement: All CCOB workforce members with access to PHI are responsible for complying with and enforcing HIPAA Policy and HIPAA Procedures. Individuals who violate this policy will be subject to the disciplinary process for staff.

Facility: The physical premises and the interior and exterior of a building(s).

Health Care Operations: (the "O" in TPO). Any of the following activities:

- Quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination
- Reviewing the competence or qualification of CCOB health care workforce, with access to PHI, including training activities.
- Audit or medical review functions
- Business management and/or cost analysis for developing and improving CCOB functions.
- Customer services provision
- Resolution of complaints/grievances

HIPAA Privacy Officer: Individual responsible for developing and maintaining a HIPAA-compliant privacy program, ensuring privacy policies to protect the integrity of PHI are enforced, delivering or overseeing ongoing employee privacy training, conducting risk assessments, and developing HIPAA-compliant procedures where necessary. Also, monitoring compliance with the privacy program, investigating incidents in which a breach of PHI may have occurred, reporting breaches as necessary, and ensuring patients´ rights in accordance with state and federal laws.

- **Primary** - individual that maintains the HIPAA Compliance Plan and coordinates required activities with the Component HIPAA Privacy Officers
- **Component** - HIPAA Privacy Officers with in the business unit

HIPAA Security Officer: The duties of a HIPAA Security Officer are not dissimilar to those of a Privacy Officer inasmuch as the appointed person will be responsible for the development of security policies, the implementation of procedures, training, risk assessments and monitoring compliance. However, the focus of a Security Officer is compliance with the Administrative, Physical and Technical Safeguards of the Security Rule and responsibility for the continuous management of information security policies, procedures and technical systems in order to maintain the confidentiality and integrity of CCOB information systems.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity: The condition that data or information have not been altered or destroyed in an unauthorized manner.

Malicious Software: Software, for example, a virus, designed to damage, disrupt or infiltrate a system.

Minimum Necessary: When using or disclosing PHI, or when requesting PHI, CCOB workforce must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use/disclosure/request.

Password: Confidential authentication information composed of a string of characters.

Physical Safeguards: Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Payment: (the “P” in TPO) includes:

- Obtaining and providing reimbursement
- Determination of eligibility or coverage
- Billing, claims management, collection, and related data processing
- Review for medical necessity, coverage, justification of charges and the like
- Utilization review activities

Protected Health Information (PHI): Individually identifiable health information, including information such as demographic data, physical or mental health information, and other information used to identify a patient or provide health care services or health care coverage.

Public Health Authority: An agency granted authority and is responsible for public health matters as part of its official mandate.

Security or Security Measures: Encompass all of the administrative, physical, and technical safeguards in an information system.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

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

Treatment: (the "T" in TPO) The provision, coordination, or management of health care and related services by one or more health care provider; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

TPO: **T**reatment, **P**ayment and Healthcare **O**perations. The three categories where use and disclosure of PHI and IIHI is allowed for a covered entity, with certain limits and protections, in order to avoid interference with an individual's access to quality health care or efficient payment for such health care.

User: A person or entity with authorized access.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity or a business associate.

Workstation: An electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Section 2: Policy and Procedures - Privacy Rule

Privacy of Individually Identifiable Health Information (reference 45 CFR Part 164 – Subpart E)

Permitted Uses and Disclosures Without Authorization

Policy: CCOB Health Care Components may not use or disclose PHI without written authorization of the individual, except as permitted by applicable law. Permitted uses and disclosures without written authorization include:

- To the individual (or the individual's legal guardian, parent or other designated personal representative of the individual, with the legal authority to act on behalf of an individual).
- For treatment, payment, or healthcare operations (TPO).
- Under circumstances where the individual is provided an opportunity to agree, acquiesce or object.
- Where the individual is incapacitated, in an emergency situation, or unavailable, provided that the use or disclosure is determined to be in the best interests of the individual.
- Incident to a use or disclosure otherwise permitted.
- Certain public interest and benefit activities or as required by law(s):
    - Public health activities or protection
    - Report abuse and neglect
    - Audit and health oversight reviews
    - Judicial or administrative hearings
    - Reporting crime or certain other law enforcement purposes
    - To respond to certain requests by law enforcement officers
    - Coroners and medical examiners
    - To avert a serious threat to health or safety
    - Workers' compensation as established by law
    - For approved research purposes (must meet criteria of 45 CFR 164.512(i))

Procedure: Circumstances where no authorization is required to share PHI. CCOB Health Care Components may, without the individual's authorization:

- Use or disclose PHI for the Component's treatment, payment, and health care operations activities.
- CCOB may disclose PHI for the treatment activities of a healthcare provider (including providers not covered by the Privacy Rule if the providers are CCOB business associates). For example:
    - CCOB may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
- CCOB may disclose PHI to another covered entity for certain health care operational activities of the entity that receives the information if:
    - Each entity either has or had a relationship with the individual who is the subject of the information, and the PHI pertains to the relationship; and the disclosure is for a quality-related health care operations activity or for the purpose of health care fraud and abuse detection or compliance.
- CCOB may disclose PHI to another Covered Entity or a health care provider for the payment activities of the entity receiving the information.

Enforcement: All CCOB workforce members with access to PHI are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.502; 164.506

Uses and Disclosures of PHI Subject to an Agreed Upon Restriction

Policy: If CCOB has agreed to a restriction on the use or disclosure of PHI, CCOB must honor that restriction unless the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment. CCOB may use the PHI, or may disclose such information to a health care provider, to provide such treatment to the individual. If restricted PHI is disclosed to a health care provider for emergency treatment, CCOB must request that the health care provider not further use or disclose the information.

Restrictions agreed to by CCOB are not effective to prevent uses or disclosures that are permitted or required as part of an investigation or to determine CCOB's compliance with HIPAA (e.g., an audit by the U.S. Department of Health and Human Services Office for Civil Rights) or pursuant to certain uses and disclosures for which an individual's authorization or opportunity to agree or object is not required (e.g., uses and disclosures required by law, for public health activities, about victims of abuse, neglect or domestic violence, for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, about decedents, for research purposes, to avert a serious threat to health or safety, for specialized government functions, or for workers' compensation).

Procedure: Please see Policy and Procedure on Uses and Disclosures for which an Authorization Form is required.

Reference: 45 CFR 164.502(c); 45 CFR 164.512

Disclosures to Business Associates

Policy: CCOB may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI on its behalf, so long as CCOB obtains satisfactory assurance that the business associate will appropriately safeguard the information.

Procedure: **In general:**

- A business associate is a person or entity who performs certain functions, activities, or services for, to or on behalf of the CCOB designated health care component that involve the use and/or disclosure of PHI.
- A business associate is not a CCOB employee of the designated health care component.
- CCOB is not required to actively monitor or oversee the means by which its business associates carry out safeguards, or the extent to which the business associates abide by the requirements of the contract. However, CCOB is required to act if it becomes aware of a material breach of HIPAA or of a violation of the business associate agreement.

All personnel must strictly observe the following standards relating to business associates:

- CCOB must enter into contracts with business associates that contain specific language. The contract must include language that provides that the business associate will:
    - Comply with the permitted and required uses and disclosures of PHI;
    - Not use or further disclose the information other than as permitted or required by the contract or as required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
    - Report to CCOB any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured PHI;
    - Ensure that any agents, including any subcontractors, that create, receive, maintain, or transmit PHI on behalf of the business associate, agree to the same restrictions and conditions that apply to the business associate with respect to such information;
    - Make available PHI in accordance with CCOB policy on Access to PHI, located herein;
    - Make available PHI for amendment and incorporate any amendments to PHI in accordance with the CCOB policy on individual's Right to Amend or Correct PHI;
    - Make available the information required to provide an accounting of disclosures in accordance with the CCOB policy on Accounting of PHI disclosures;
    - Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created by or on behalf of CCOB, available for purposes of determining compliance;
    - At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of CCOB that the business associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information feasible; and
    - Comply with termination provisions of the business associate agreement if CCOB determines that the business associate has violated a material term of the agreement.

Business Associates are responsible for compliance with HIPAA Enforcement Rule and Breach Notification. Should CCOB become aware of a breach of PHI, the policy and procedures for Breach Notification will be followed.

Reference: 45 CFR 164.502(e)

Disclosures by Whistleblowers and Workforce Member Crime Victims

Policy: CCOB will not be considered to have violated use/disclosure of PHI if a workforce member believes in good faith that CCOB has violated professional or clinical standards or otherwise engaged in unlawful conduct and the workforce member makes the disclosure to:

- A health oversight agency or other public health authority; or
- An attorney retained by workforce member

CCOB is not considered to have violated use/disclosure of PHI if a member of CCOB workforce, who is the victim of a criminal act, discloses PHI to a law enforcement official, so long as:

- PHI disclosed is about the suspected perpetrator of the crime; and
- Minimum necessary rule is used

Procedure: CCOB is committed to an organizational culture that encourages the raising and fair resolution of matters which are perceived to be or are violative of professional or clinical standards or other unlawful conduct. Employees who have issues of concerns are encouraged to first raise them with their supervisor, other management, or HIPAA Privacy Compliance Officer. CCOB will assess and investigate the conduct, while complying with anti-retaliation laws.

Reference: 45 CFR 164.502(j)

Uses and Disclosures Requiring an Authorization Form

Policy: Except as otherwise described herein, unless otherwise permitted by law, CCOB must have proper, written authorization from the individual before it may use or disclose an individual's PHI. A "consent" document is not a valid permission to use or disclose PHI for a purpose that requires an "authorization" under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of PHI. Valid Authorization Forms must meet strict criteria. There are some circumstances where CCOB may use or disclose PHI provided that the individual is informed, in "plain language", in advance of the use/disclosure and has the opportunity to agree, prohibit or restrict the use/disclosure of PHI.

PHI may not be used or disclosed except when at least one of the following conditions is true:

1. The individual, who is the subject of the information, has authorized the use or disclosure.
2. The individual who is the subject of the information has received a Notice of Privacy Practices and acknowledged receipt of the Notice or good faith efforts and the refusal to acknowledge receipt is documented. This is required to allow the use or disclosure and the use or disclosure is for treatment, payment, or health care operations.
3. The PHI is used or disclosed incident to a permitted use or disclosure, as long as reasonable safeguards have been adopted as required by the Privacy Rule, and the information being shared is limited to the "minimum necessary."
4. For certain disclosures to family, personal representatives, or other caregivers, unless the disclosure would be inconsistent with any known prior expressed preference of the individual and provided the individual has been given an opportunity to opt out.
5. The disclosure is to the individual who is the subject of the information or to the U.S. Department of Health and Human Services for compliance-related purposes.

6. The use or disclosure is for limited data sets, from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.

7. The use or disclosure is for one of the HIPAA designated public health purposes, law enforcement purposes, and other limited (national priority) purposes for which permission of the individual is not required.

Upon verification that an individual has been authorized to act as a personal representative of an individual, CCOB shall treat the personal representative as the individual with respect to the use and disclosure of his/her PHI.

Procedure for Valid Authorization Form: Valid Authorization to Use/Disclose Information Form Elements:

- For uses and disclosures that are not expressly permitted or required, CCOB must obtain the individual's authorization for permission to use particular PHI for a specified purpose or to disclose PHI to a specified third-party for such purpose.
- An authorization must be obtained on the correct form to ensure that it complies with the law. Therefore, CCOB shall use the approved HIPAA Authorization to Disclose Information Form at all times.
- An authorization form that is signed by the individual's personal representative must state the personal representative's name and the relationship that gives the personal representative authority to act on the individual's behalf, in addition to the other information required.
- Upon request, CCOB must give the individual (or the personal representative) a copy of the signed authorization form.
- A copy of the signed authorization form must be retained.

Additionally there are Required Statements for a valid Authorization to Use/Disclose Information Form. The authorization must contain statements adequate to place the individual on notice of all of the following:

- The individual's right to revoke the authorization in writing (reference CCOB Notice of Privacy Practices).
- The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
    - CCOB may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
    - The consequences to the individual of a refusal to sign the authorization when CCOB can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected.

Defective Authorization Form/Invalid Authorization Form: An authorization is not valid, if the document submitted has any of the following defects:

- It is not signed or dated;
- The expiration date has passed or the expiration event is known by the covered entity to have occurred;
- The authorization has not been filled out completely;
- The authorization is known by the covered entity to have been revoked;
- The authorization violates privacy policy as per 45 CFR § 164.508(b)(2)(iv);
- Any material information in the authorization is known by the covered entity to be false.

Psychotherapy Notes: An authorization is generally required for use and disclosure of psychotherapy notes except CCOB may use psychotherapy notes without obtaining an individual's authorization to carry out its own treatment, payment, or operations as follows:

- Use by the originator of the notes for treatment;
- Use or disclosure by CCOB for its own training programs in which mental health students, trainees, or practitioners learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
- Use or disclosure by CCOB to defend a legal action or other proceedings brought by the individual.

Marketing: CCOB must obtain an authorization for any use or disclosure of PHI for marketing except if the communication is a face-to-face communication made by CCOB to the individual or a promotional gift of nominal value. If the marketing involves financial remuneration to CCOB from a third-party, the authorization must state that such remuneration is involved.

Revocation of an Authorization: An individual may revoke an authorization at any time by providing written notice to the CCOB's HIPAA Privacy Officer or his/her designee. The individual's Authorization is no longer valid once the CCOB knows of the revocation, except to the extent CCOB has already taken action in reliance of the Authorization or to the extent the Authorization was obtained as a condition of obtaining insurance and other law provides the insurer the right to contest the policy or claim under the policy.

Documentation: CCOB must retain any signed authorization or revocation. The documentation must be retained for at least six years from the date it was created or from the date it was last in effect, whichever is later.

Reference: 45 CFR 164.508

Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object

Policy: CCOB may use or disclose PHI as noted below so long as the individual has the opportunity to agree, prohibit or restrict the use or disclosure. CCOB may verbally inform the individual of and obtain the individual's verbal agreement or objection to a use/disclosure permitted by this section.

- Certain types of facility directories (e.g., inpatient care).

- Disclosure to family members (i.e., after surgery a Doctor can provide family members updates).
- The individual has the ability to object and does not expressly object, or based on reasonable inferences and the exercise of professional judgment, the individual does not object to the disclosure.
- Individual not present or incapacitated.
    - If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, CCOB may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. CCOB staff may use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.
- Coordination of disaster relief.
    - CCOB may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.
- Uses and disclosures when the individual is deceased.
    - If the individual is deceased, CCOB may disclose to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Procedure: Individuals will be provided an opportunity to agree and/or object to uses or disclosures of PHI (see Notice of Privacy Practices). If CCOB is faced with an emergency or other situation described in the bullet points above, CCOB may use and disclose PHI.

Reference: 45 CFR 164.510

Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object is not Required

Policy: There are delineated situations where CCOB may use or disclose PHI without the written authorization of the individual, or the opportunity for the individual to agree or object. When CCOB is required to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, information and the individual's agreement may be given verbally.

Permitted Uses and Disclosures where no authorization or opportunity to agree/object is required.

- Uses and disclosures required by law.
- Uses and disclosures for Treatment, Payment and Health Care Operations (TPO).
- To the individual who is the subject of the information;

- Required disclosures to the Secretary of Health and Human Services for enforcement of the Privacy Rules;
- About immunizations of a student or prospective student to their school;
- Coroners, Medical Examiners, and Funeral Directors regarding decedents;
- Organ, eye, or tissue donation purposes;
- Research purposes;
- To avert a serious threat to health or safety;
- Specialized government functions (military, veterans' activities, national security, intelligence activities);
- Workers compensation;
- Food and Drug Administration;
- Uses and disclosures for certain public health activities. (for full list of all items, please see 45 CFR 164.512, for brevity purposes, only those activities that are currently under the purview of CCOB have been noted).
    - A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;
- Disclosures about victims of abuse, neglect or domestic violence.
    - CCOB may disclose PHI about an individual whom CCOB reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence.
- Uses and disclosures for health oversight activities. CCOB may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
    - The health care system (e.g., HR in administering employee health insurance claims).
    - Government benefit programs for which health information is needed to determine eligibility (e.g., Medicaid, Long Term Care).
    - Entities subject to government regulatory programs for which PHI is necessary for determining compliance. (e.g., program audits, HCPF audits, A-133 Audits).
    - Entities subject to civil rights laws for which health information is necessary for determining compliance, (e.g., WIC and Food Assistance Program compliance with Civil Rights).
- Disclosures for judicial and administrative proceedings. CCOB may share information in response to a valid judicial or administrative order.
- Disclosures for limited law enforcement purposes. CCOB may disclose PHI for a law enforcement purpose to a law enforcement official:

- As required by law including laws that require the reporting of certain types of wounds or other physical injuries.
- In compliance with and as limited by the relevant requirements of:
  - A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
  - A grand jury subpoena; or
  - An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
- The information sought is relevant and material to a legitimate law enforcement inquiry;
  - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
  - De-identified information could not reasonably be used.

Reference: 45 CFR 164.512

Other Requirements Relating to Uses and Disclosures of Protected Health Information (PHI)-Minimum Necessary

Policy: Under the Minimum Necessary Standard, when using or disclosing PHI or when requesting PHI from another covered entity or business associate, CCOB must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. CCOB shall delineate procedures related to:

- Minimum necessary uses of PHI
- Minimum necessary disclosures of PHI
- Minimum necessary requests for PHI
- Use of Limited Data Set for purposes of research, public health or health care operations
- Verification requirements prior to disclosure

Procedure:

Minimum necessary ***uses*** of PHI by CCOB:

- CCOB, by way of CCOB HIPAA Component Privacy Officers, shall identify and ensure that only persons or classes of persons, as needed, have access to PHI.
- CCOB, by way of CCOB HIPAA Component Privacy Officers, shall ensure that the appropriate CCOB Workforce has access to the category or categories of PHI needed to complete business needs.
- CCOB workforce will be trained to use the minimum necessary PHI to complete business needs.

Minimum necessary ***disclosures*** of PHI from CCOB to another entity:

- CCOB shall ensure that only persons or classes of persons, as needed, have access to PHI.
- CCOB shall only disclose PHI as allowed by HIPAA rules and regulations and shall only disclose the PHI reasonably necessary to accomplish the purpose for which the disclosure is sought.
- Requests for disclosure must be reviewed in accordance with criteria designed to limit disclosures to the minimum necessary.

- **CCOB shall document in the individual's record any and all disclosures**. Documentation shall include:
  - Verification that PHI disclosure is allowable.
  - Purpose of disclosure request.
  - Information disclosed.
  - Confirmation that minimum necessary was disclosed.
  - Name of CCOB staff disclosing information and date.

Minimum necessary ***requests*** of PHI by CCOB:

- CCOB shall limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made.
- CCOB shall not make blanket requests for an entire medical record, rather CCOB shall carefully determine the minimum information needed to complete the business need.

Use of Limited Data Set (with valid data use agreement):

- CCOB may use or disclose a limited data set of PHI, **with an approved data use agreement**, for research, public health functions and health care operations.
- Limited data set is PHI that excludes the following direct identifiers: Name, postal address information (not including zip code), telephone number, fax number, email address, social security number, medical record number, health plan beneficiary number, account number, certificate/license number(s), VIN and license plate numbers, device identifiers and serial numbers, URLs, IP address numbers, biometric identifiers (finger or voice prints), full face photographic images.
- Data use agreements must:
  - Establish the permitted uses and disclosures of information by the recipient of the information and may not authorize the recipient to use or further disclose the information in a manner that would otherwise violate HIPAA's Privacy Rule;
  - Establish who is permitted to use/receive the limited data;
  - Provide that the recipient of the data will:
    - only use data as permitted
    - use appropriate safeguards to prevent unauthorized use/disclosure
    - ensure any agents/subcontractors it gives data set to follows same restrictions
    - not identify the information or contact the individuals
    - report to CCOB any unauthorized use/disclosure

Verification Requirements:

- **Prior to any disclosure, CCOB must**:
  - Verify the identity of the person requesting PHI and the authority of the person to have access to the PHI.
  - Obtain documentation, statements, or representations, whether oral or written, from the person requesting the PHI.
- If the documentation is an authorization, be sure it is valid (see policy/procedure for valid authorization forms).
- If request is made in person, verify identification (ID badge if government official).
- CCOB workforce will rely on the exercise of professional judgment in making a use or disclosure of PHI, or act on a good faith belief in making a disclosure.
- **CCOB will document in the individual's record the verification process**.

Reference: 45 CFR 164.514

Notice of Privacy Practices (NPP) for PHI

Policy: The HIPAA Privacy Rule protects an individual's medical records and other individually identifiable health information created or received by or on behalf of CCOB, known as PHI. The Privacy Rule protects an individual's health information by regulating the circumstances under which CCOB may use and disclose PHI and by requiring CCOB to have safeguards in place to protect the privacy of the information.

Individuals generally have a right to adequate notice of the uses and disclosures of their PHI and CCOB's legal duties with respect to such PHI. The law dictates a specified set of core elements that a valid Notice of Privacy Practices must contain. CCOB agencies with a direct treatment relationship with a patient must have a Notice of Privacy Practices. These covered health care components shall disclose PHI only in conformance with the contents of the Notices of Privacy Practices. CCOB will promptly revise its Notice of Privacy Practices whenever there is a material change to the uses or disclosures of PHI, to the individuals' rights, to its legal duties, or to other privacy practices that render the statements in the Notice no longer accurate.

Section 164.520 of the Privacy Rule sets out the requirements for most covered entities to have and to distribute a notice of privacy practices (NPP). The NPP must describe the uses and disclosures of PHI that CCOB is permitted to make, CCOB's legal duties and privacy practices with respect to protect PHI, and the individual's rights concerning PHI.

There are two exceptions to the general rule that an individual has the right to CCOB's notice of the uses and disclosures of PHI that may be made by CCOB: (1) for group health plans, certain other notice requirements apply; and (2) inmates do not have a right to a notice of privacy practices.

Purpose: The purpose of this amended policy is to provide updated information to CCOB employees, volunteers and interns about the privacy rights that individuals have regarding the use and disclosure of their PHI and to describe the process for filing a complaint. The Notice of Privacy Practices outlines the following:

- Uses and disclosures of PHI
- Individual's rights with respect to PHI
- Complaint process, including who to contact
- CCOB Responsibilities

Procedure: **All CCOB staff, volunteers, and interns will use the Notice of Privacy Practices to inform individuals about how CCOB may use and/or disclose their PHI**. The Notice of Privacy Practices also describes the actions an individual may take, or request the City and County of Broomfield to take, with regard to the use and/or disclosure of their information.

CCOB will distribute its Notice of Privacy Practices as follows:

- Provide the Notice to any person who requests it.
- Provide the Notice to each individual that has a direct treatment relationship with a CCOB agency no later than the first service delivery. If an individual requests service electronically, the Notice shall be provided automatically and contemporaneously in response to the request.
- In emergency treatment situations, the Notice shall be provided to the individual as soon as reasonably practicable after the emergency treatment situation.
- Updated Notices will be provided at the next visit or contact with the patients

- If there is a physical service delivery site, have the Notice available for individuals to request to take with them and post the Notice in a prominent location at the physical service site for individuals to reasonably be able to read the Notice
- Prominently post and make electronically available the Notice on any website CCOB maintains that provides information about its services or benefits.
- CCOB may provide the Notice to an individual by email but only if the individual agrees to electronic notice in writing and such agreement has not been withdrawn. Recipients of electronic notice shall retain the right to obtain a paper copy upon request.

All CCOB workforce with access to PHI will participate in a HIPAA training covering HIPAA Privacy Rule, HIPAA Security Rule and HIPAA Enforcement Rule. Upon the discretion of the CCOB Manager or CCOB Supervisor, HIPAA refresher training may be provided on an as needed basis for any and all CCOB workforce. The standard organizational HIPAA training will be administered by the Diversity Equity and Organizational Development Department, while any component specific HIPAA training will be maintained by the Component HIPAA Privacy Officers. A record of these training participants also will be maintained.

The NPP shall be posted in a "clear and prominent location where it is reasonable to expect" individuals to be able to read the notice.

Broomfield CCOB shall document compliance with providing NPP to individuals in records with a signed Acknowledgement of Receipt of the NPP, or if not signed, documentation of the good faith efforts made to obtain such written acknowledgment. The individual's record shall also have a copy of the NPP or if the notice is not obtained due to an emergency treatment situation, CCOB must document its good faith efforts to obtain such written acknowledgement and the reason why the acknowledgment was not able to be obtained.

For CCOB employer sponsored group health plans, CCOB must provide each participant in its self-funded group plan a NPP at the time of enrollment, to individuals who are new enrollees. CCOB must also provide revised notices to individuals within 60 days of any material revisions. At least once every three years, CCOB must notify individuals covered by its sponsored health plans of the availability of and how to obtain the Notice. CCOB is not required to provide a NPP where the group plan is fully insured or if an administrator agrees by contract to provide such Notice.

Reference: 45 CFR 164.520

Requests for Privacy Protection, Access, Amendment and Accounting of Disclosures

Purpose: The HIPAA Privacy Rights Request Form allows the individuals to formally request specific actions as it relates to accessing, altering or restricting access to their PHI.

Policy and Procedure: HIPAA Privacy Rule specifies the rights of individuals in accessing, altering and restricting their PHI.

I. Right to Request Privacy Protection Policy. Individuals have the right to request restrictions on how CCOB will use and disclose PHI about them for treatment, payment, and health care operations (TPO). CCOB is not required to agree to an individual's request for a restriction, but is bound by any restrictions to which it agrees. See 45 CFR 164.522(a) for further details.

- **Right to Request Privacy Protection Procedures**: Upon receipt of a written Privacy Rights Request Form where an individual has requested restriction of uses and disclosure of PHI,

CCOB will make reasonable efforts to comply with the request. CCOB will inform the individual that it will agree/disagree with the request.

- If CCOB agrees to request, it is only valid to PHI created or received *after* the date of the written request. If an individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed, CCOB may still use or disclose it to a health care provider to provide such treatment, but will request that such provider not further use or disclose the information.
- CCOB will document in the individual's case record the individual's request, the outcome of the request, and the date the request was effective.
- CCOB will keep a copy of the written request in the individual's file and retain the record for six years from the date of its creation or the date when it was in effect, whichever is later.

- **Terminating a restriction.** CCOB may terminate a restriction, if:
  - The individual agrees to or requests the termination in writing;
  - The individual orally agrees to the termination and the oral agreement is documented; or
  - CCOB informs the individual that it is terminating its agreement to a restriction, except that such termination is:
    - Not effective for PHI restricted under rules governing health plans (e.g., for TPO); and
    - Only effective with respect to PHI created or received after it has so informed the individual.

- **Confidential Communication Policy**: Individuals also may submit a written request to receive confidential communications from CCOB, either at alternative locations or by alternative means. For example, an individual may request that CCOB call him/her at their place of employment, rather than home. See 45 CFR 164.522(b). CCOB will not require an explanation from the requesting individual as to the basis for the request.
  - **Confidential Communication Procedure**:
    - Upon receipt of a written Privacy Rights Request form for confidential communication, CCOB will make reasonable efforts to comply with the request.
    - CCOB will document in the individual's case record the individual's request, the outcome of the request, and the date the request was effective.
    - CCOB will keep a copy of the written request in the individual's file and retain the record for six years from the date of its creation or the date when it was in effect, whichever is later.

II. Accounting of Disclosures Policy: CCOB shall make available to an individual upon request, an accounting of certain disclosures of the individual's PHI over the past six years. Exceptions to an individual's right to receive an accounting are disclosures:

- To carry out treatment, payment and health care operations;
- To individuals of PHI about them as otherwise provided under the Privacy Rule;
- Incident to a permitted use or disclosure;
- Pursuant to an authorization;
- For a facility directory, to persons involved in the individual's care or certain other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement offices as permitted under HIPAA; or
- As part of a limited data set.

- For each disclosure, the accounting must include: (1) The date of the disclosure; (2) the name (and address, if known) of the entity or person who received the PHI; (3) a brief description of the information disclosed; and (4) a brief statement of the purpose of the disclosure (or a copy of the written request for the disclosure). See 45 CFR 164.528 for further exceptions and details.
    - **Accounting of Disclosure Procedure**: Upon receipt of a written request of Privacy Rights Request Form for accounting of disclosures, CCOB will make reasonable efforts to comply with the request.
        - CCOB will have 60 days from the date of the written request to take action.
        - Request will be routed to CCOB HIPAA Privacy Officer to verify request and to screen information per 45 CFR 164.528.
        - CCOB must document the following in the individual's case record:
            - The information requested,
            - The CCOB response with the written accounting of disclosures,
            - The name and title of the CCOB workforce member responsible for receiving and processing the request.

III. Right to Access/Restrict Access Policy: Any individual has the right to access, inspect and obtain a copy of PHI in their designated case record except for:

- Psychotherapy notes; and
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

- **Right to Access/Restrict Access Procedure:** Upon receipt of a written Privacy Rights Request Form where an individual has requested access to PHI, CCOB will evaluate and make reasonable efforts to comply with the request. CCOB will document in the case record the request, the title of the CCOB workforce responsible for processing the request and the outcome of the request.
    - Reviewable Grounds for Denial: If CCOB denies the request for access, the individual has a right to have the denial reviewed in the following circumstances:
        - A licensed healthcare professional has determined, in the exercise of professional judgment, that such access is reasonably likely to endanger the life or physical safety of the individual or another person.
        - The request for access is made by a personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is likely to cause substantial harm to the individual or another person.
        - The PHI references another person and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is likely to cause substantial harm to such other person.
        - CCOB will document in the case record the request and the grounds for denial and will inform the individual.
    - Procedure for Denials: If CCOB denies the request in whole or in part, CCOB will:
        - Make other information accessible, after excluding the PHI.
        - The individual has the right to have a designated licensed healthcare professional who did not participate in the original decision review the denial.
        - Provide a timely, written denial with the following three requirements:

- Basis for denial,
- Notification of individual's rights, and,
- Notification of complaint process and procedures.

- Timeliness:
  - CCOB will have 30 days to evaluate and take action on written requests for accounting of disclosure and to notify the individual of the acceptance or denial of the request. This requirement is subject to a 30-day extension if CCOB provides the individual with a written statement of the reasons for the delay.
- Provision of Access:
  - CCOB will make reasonable efforts to accommodate an individual's method of access by providing copies of requested information and/or allow the individual to view the case record.
  - CCOB retains the right to discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely request.

IV. Amendment of PHI Policy:

- An individual has the right to have CCOB amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. (See 45 C.F.R. § 164.526)
  - Amendment of PHI Procedure:
    - Upon written receipt of Request to Amend or Correct Protected Health Information, CCOB will make reasonable efforts to comply with the request.
    - CCOB will make a determination on the request within 60 days of receipt of written request.
    - Accepting the request: CCOB will inform the individual of the acceptance of the request and will alter the PHI per the individual's request. CCOB will make reasonable efforts to notify the individual of other sources of PHI so that the individual can make requests to other entities.
    - Denial of request: CCOB will provide timely written denial of the request and keep written notification in the individual's case record. This letter of denial must:
      - Be in plain language,
      - Explain the basis for the denial,
      - Provide notification of individual's rights, and,
      - If notified by another covered entity of amendment, CCOB must honor that amendment.
      - Provide information for filing a statement of disagreement and how the individual may complain pursuant to specified procedures established under HIPAA.
    - Reasons for Denial of Request: CCOB may deny an individual's request for amendment, if CCOB determines that the PHI or record that is the subject of the request:

- Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
- Is not part of the designated record set;
- Would not be available for inspection under 45 CFR §164.524; or
- Is accurate and complete.

- Recordkeeping: CCOB must keep documentation of individual's requested amendment, CCOB's action and any further communication to/from the individual regarding the request.

- Complaint Policy Regarding Use and Disclosure of PHI: Persons have a right to submit a complaint if they believe that CCOB has improperly used or disclosed their protected information, or, if they have concerns about the privacy policies of CCOB and CCOB's compliance with such policies. Depending on the type of complaint, the Federal Office of Civil Rights (OCR) and/or Colorado Department of Human Services (CDHS) or other State agency, will be notified of the complaint. CCOB will proceed with forwarding the complaint and/or alerting OCR/CDHS and/or any other governing body in documenting and addressing the individual's specific complaint. Other governing bodies may include: Colorado Department of Health Care Policy and Finance (HCPF), Colorado Department of Public Health and Environment (CDPHE), United States Department of Agriculture (USDA), CDHS, and OCR.

- **Amendment of PHI Procedure:** CCOB will provide to individuals information on how to file a complaint. All complaints will be forwarded to the CCOB HIPAA Privacy Officer, the Component HIPAA Privacy Officer, and the Component Director. All complaints will be logged internally, thoroughly investigated with a written outcome provided to the individual. CCOB will comply with state and federal agencies with jurisdiction over complaints (e.g., SNAP complaints will be reported to USDA and CDHS).

Reference: 45 CFR 164.522 Rights to request privacy protection for protected health information.
45 CFR 164.524 Access of individuals to protected health information.
45 CFR 164.526 Amendment of protected health information.
45 CFR 164.528 Accounting of disclosures of protected health information.

Specific Administrative Requirements Policy and Procedures:

Purpose: HIPAA requires covered entities to establish policies and procedures regarding the specific administrative requirements for successful implementation of all HIPAA rules and regulations.

Privacy Officer:

Policy: CCOB must designate a HIPAA privacy officer who is responsible for the development and implementation of the policies and procedures for CCOB. CCOB must designate a contact person who is responsible for receiving complaints, addressing complaints and follow up as needed.

Procedure: CCOB has designated the HIPAA Privacy Officer, Security Analyst, and Component HIPAA Officers as follows:

- HIPAA Privacy Officer - Finance Risk Administrator
- Security Officer - IT Senior Security Analyst
- Component HIPAA Privacy Officers:
    - Human Resources - Human Resources Director
    - Human Services - Human Services Director
    - Information Technology - IT Senior Security Analyst
    - Police/Detention - Strategic Services Commander
    - Public Health - Deputy Public Health Director

Training:

Policy: CCOB must train all members of its workforce who have access to PHI on the policies and procedures with respect to PHI.

- Train new workforce members within a reasonable timeframe.
- Re-train workforce members when information is updated.
- Provide training on an ongoing basis.

Procedure: CCOB will provide training to all new staff who have access to PHI and will provide ongoing annual training, or as necessary, to the CCOB workforce. Training materials will be available on the CCOB intranet and any CCOB employee will be able to access training materials at will. CCOB will provide self-guided training materials, 1:1 or group training dependent upon the individual needs of the workforce.

The HIPAA Privacy Officer shall maintain organizational HIPAA training content and a record of workforce member training compliance relevant to the entire organization. The Component HIPAA Privacy Officers are responsible for maintaining HIPAA training content and a record of workforce member training compliance relevant for their respective business components.

Safeguards:

Policy: CCOB must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI. Safeguards include measures to ensure that PHI is protected from any intentional or unintentional use or disclosure and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Procedure: CCOB in conjunction with IT will comply with ensuring appropriate and reasonable safeguards are in place.

Complaints to CCOB:

Policy: CCOB must provide a process for individuals to make complaints regarding the policies and procedures for HIPAA compliance. CCOB must document all complaints received and the disposition, if any.

Procedure: As part of the Notice of Privacy Practices policy, procedure and notification, CCOB individuals are provided the information needed to register complaints. All complaints should be directed to the CCOB HIPAA Officer. Further, CCOB must:

- Maintain the policies and procedures in written or electronic form;
- If a communication is required, maintain such writing, or an electronic copy as documentation;
- If an action, activity or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity or designation; and
- Maintain the documentation sufficient to meet the burden of proof under 45 CFR § 164.414(b).

Sanctions:

Policy: CCOB must have and apply appropriate sanctions against CCOB workforce who fail to comply with the privacy policies and procedures.

Procedure: City and County of Broomfield, Human Resources Department Personnel Merit Policy will be used to provide corrective or disciplinary action for workforce members who violated HIPAA privacy rules and regulations.

Mitigation:

Policy: CCOB must mitigate, to the extent practicable, any harmful effect that is known to CCOB of a use or disclosure of PHI in violation of CCOB policies and procedures.

Procedure: As part of breach and breach notification policy and procedures, CCOB Component Privacy Officers, in conjunction with the Privacy Officer and other organizational resources as needed, will conduct a risk assessment and, as appropriate and as reasonable, will take action to mitigate harmful effects of unauthorized disclosure of PHI.

Refraining from Intimidating or Retaliatory Acts:

Policy and Procedure: CCOB will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual who complains or exercises the rights accorded to them in the HIPAA rules and regulations. CCOB workforce who violate this are subject to the corrective and disciplinary actions set forth in the Personnel Merit Policy.

Waiver of Rights:

Policy: CCOB may not require individuals to waive their rights as a condition of the provisions of treatment, payment or eligibility for benefits.

Procedure: CCOB will train the workforce to ensure knowledge and compliance with individual's rights.

Policy, Procedures, and Documentation:

Policy: CCOB will implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications and requirements spelled out in HIPAA 45 CFR rules and regulations.

- CCOB will update policies and procedures as necessary to comply with changes in law and note the original date and the revised date.
- CCOB will document the changes in policy and procedures and will retain outdated versions of policy and procedures for no less than 6 years from the date of creation or date when it was last in effect, whichever is later.

Procedure:

- The HIPAA Privacy Office will:
  - Consult annually, or when regulations change, with external legal counsel who specialize in HIPAA related matters.
  - Coordinate annually, or when regulations change, with the HIPAA Component Privacy Officers to ensure all component HIPAA attachments are updated.
  - Maintain current and past copies of the HIPAA Compliance Plan Policies & Procedures for a period of six years.

Reference: 45 CFR 164.530 Administrative Requirements

Disposal of Paper Protected Health Information (PHI), Individually Identifiable Health Information (IIHI), Personal Identifiable Information (PII)

Purpose: The purpose of this policy is to provide updated information to CCOB employees, volunteers and interns about the shredding PHI, IIHI, and PII as well as the process, procedures and suggested best practices for safeguarding paper PHI, PII or IIHI.

Policy: The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form. This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited uses and disclosures of PHI, including in connection with the disposal of such information.
For PHI in paper records, CCOB has determined that shredding is the method of destruction of documents so that PHI, IIHI and PII are rendered essentially unreadable, indecipherable, and otherwise unusable.

CCOB policy is that all CCOB employees will ensure that all documents containing PHI, IIHI, and/or PII are properly disposed of in the CCOB on-site Shred-It bins.

If the Shred-It bins are filled to capacity prior to the scheduled pick up date(s), staff will inform the Operations Accounting Technician so that an additional pick up date can be scheduled.

Procedure: Each CCOB building containing a Component site will have at least one Shred-It bin. All staff will comply with the following procedures:

- Any paper documents designated as 'trash' containing PHI, IIHI or PII shall be shredded. No documents containing PHI, IIHI or PII shall be placed in a trash receptacle.
- Shred-It bins will be available for all CCOB workforce handling PHI.

Best Practices:

- Clean Desk Best Practices – Three P's:
- **PLAN** first thing in the morning.
- Employees should keep just the things they need for the workday on their desk. Employees should start each day with a few minutes of planning so that they can organize the documents they need for immediate work. File all other folders and documents.
- **PROTECT** information whenever you leave your desk.
- Employees will need to leave their desk to attend meetings or to take breaks. But whenever they do, employees should make a quick check to see if there is sensitive information on their desk and place it inside a folder or off your desktop.
- **PICK UP** at the end of the day.

- Employees should not leave documents on their desk in the evening. Documents should be filed, locked and or placed in the shred bin.

Enforcement: All CCOB employees with access to PHI will be required to review this policy and to follow the disposal policies and procedures. Further, all CCOB Supervisors whose direct reports dispose of PHI, must review this policy and ensure their direct reports have been properly advised of the disposal of PHI policy and procedures. All CCOB workforce members with access to PHI are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff as outlined in the Personnel Merit Policy.

Reference: 45 CFR 164.530(c), 164.308(a)(5), and 164.530(b) and (i).

Section 3:

Breach Notification Policy and Procedures

Breach Notification for Unsecured Protected Health Information

Purpose: The Health Information Technology for Economic and Clinical Health (HITECH) Act requires HIPAA covered entities to provide notification to affected individuals and to the Federal Secretary of the Department of Health and Human Services (DHHS) following the discovery of a breach of unsecured PHI. In addition, in some cases, the Act requires covered entities to provide notification to the media.

Definitions:

Breach - A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach."

- The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate, if the acquisition, access, or use was made in good faith, within the scope of authority and does not result in further impermissible use or disclosure.
- The second exception applies to the inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Unsecured Protected Health Information - CCOB must only provide the required notification if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of DHHS in guidance. (45 CFR 160.404)

Workforce Members - Breach Notification rules and the HIPAA Security Rule apply to all "workforce members". Defined in the HITECH Act (45 CFR 160.103), workforce members are defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

Breach Notification Process:

Purpose: CCOB is required to have policies and procedures that educate the CCOB workforce on identification of a breach, how to report a breach, breach risk assessment and breach notification processes.

Policy: All CCOB staff will report any suspected or alleged breach of PHI to the HIPAA Officer within 2 hours of discovery.

Procedure for Determination if a Breach of PHI has Occurred: (45 CFR 160 & 164)

(See attached diagram)

Upon notification that a breach, or potential breach occurred, a team of CCOB management will convene within 24 hours and conduct a risk assessment. While not determinative of whether a breach is reportable, factors to be reviewed, discussed and documented include:

- Nature of the Data Elements Breached
    - CCOB Managers will consider the data element(s) in light of their context and the broad range of potential harm from the breach.
        - Example from HITECH Act: It may be determined that an impermissible use or disclosure of a limited data set that includes zip codes, based on the population features of those zip codes, does not create a significant risk that a particular individual can be identified.
- Number of Individuals Affected
    - CCOB Managers will assess the magnitude of the number of affected individuals as it may impact how to proceed with notification, but will not be the determining factor for whether CCOB will provide notification.
- Likelihood the Information is Accessible and Usable
    - CCOB Managers shall assess the likelihood PHI, PII or ePHI will be or has been used by unauthorized individuals. CCOB will consider facts such as:
        - Information reported as lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals and depends on factors such as physical, technological, and procedural safeguards employed. If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent.
    - CCOB Managers will assess the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.
- Likelihood the Breach May Lead to Harm
    - CCOB Managers shall assess the broad reach of potential harm.
        - Including factors such as: substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. And further include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.
    - CCOB Managers will assess whether a likelihood of harm will occur.
        - Including type of data set disclosed:
            - Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name.
            - If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease.
- Ability of the Agency to Mitigate the Risk of Harm
    - CCOB Managers will assess mitigation efforts.
- The CCOB Managers will document and retain the record of the risk assessment and will recommend an outcome of:
    - Proceed with official Breach Notification; OR
    - Conclude that no breach occurred.

Procedure for Breach Notification by Business Associate: (45 CFR 164.410)

- A business associate shall, following the discovery of a breach of unsecured PHI, notify CCOB of such breach.
- A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).
- Timeliness of notification. A business associate shall provide the notification required without unreasonable delay and in no case later than 14 calendar days after discovery of a breach.
- Content of notification:
    - The notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
    - A business associate shall provide CCOB with any other available information that CCOB is required to include in notification to the individual under 45 CFR § 164.404(c) at the time of the notification or promptly thereafter as information becomes available.

Procedure for Breach Notification Requirements: Following a breach of unsecured PHI, CCOB will provide notification of the breach to affected individuals, and in certain circumstances, to the Secretary of the Department of Health and Human Services, the appropriate State Agency, and City Manager's Office and potentially to the media.

- **Individual Notice -** CCOB must notify affected individuals following the discovery of a breach of unsecured PHI. CCOB must provide this individual notice in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically. If CCOB knows the individual is deceased and has the address of the next of kin or personal representative, written notification shall be provided to that person. If CCOB has insufficient or out-of-date contact information for 10 or more individuals, CCOB must provide substitute individual notice by either posting the notice on the homepage of the CCOB web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If CCOB has insufficient or out-of-date contact information for fewer than 10 individuals, CCOB may provide substitute notice by an alternative form of written notice, telephone, or other means.

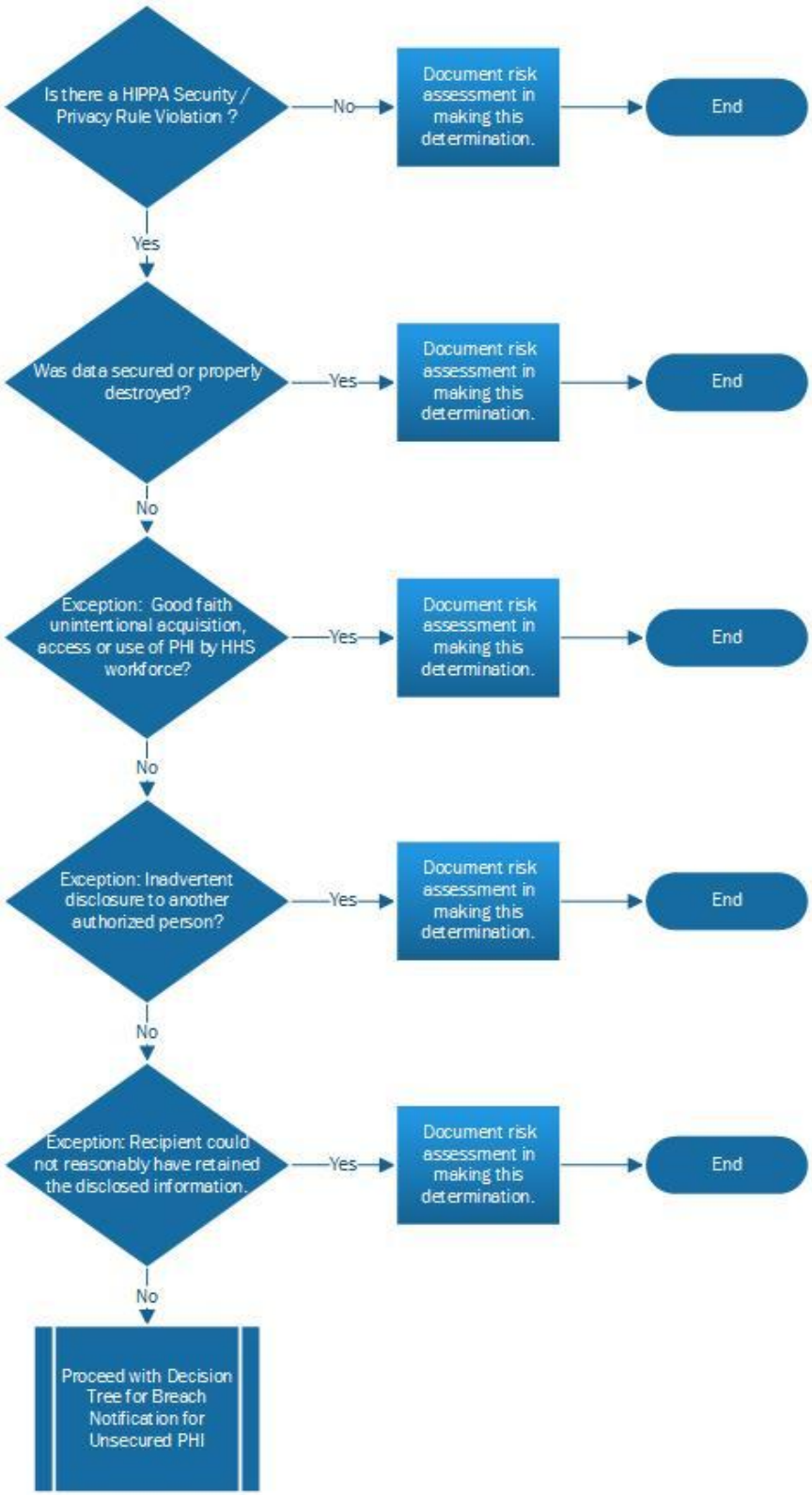
  These individual notifications must be provided without unreasonable delay and in no case later than 30 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what CCOB is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for CCOB. Additionally, for substitute notice

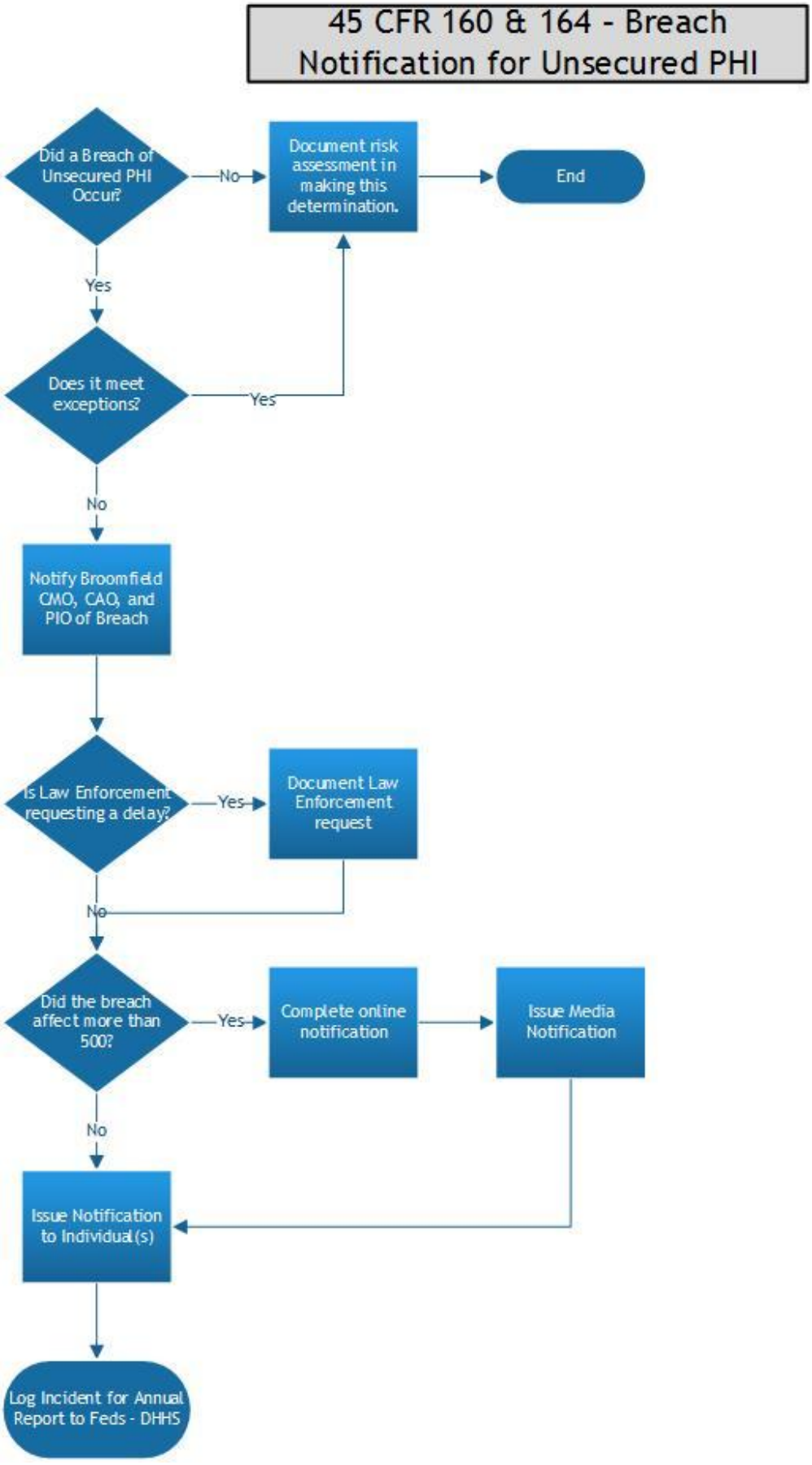
provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact CCOB to determine if their PHI was involved in the breach. (45 CFR 164.404) Colorado law also requires that certain elements be included in the breach notification, such as when the breach occurred, a description of what happened, and the phone numbers of consumer reporting agencies.

- **Media Notice -** If CCOB experiences a breach affecting more than 500 individuals, in addition to notifying the affected individuals, CCOB is required to provide notice to prominent media outlets serving the State or jurisdiction and to the Colorado Attorney General's Office. If the breach affects more than 1000 individuals, under Colorado law additional notification must be made to consumer protection agencies. CCOB will coordinate with the City and County of Broomfield's Public Information Officer to prepare a press release. Media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice. (45 CFR 164.406)

- **Notice to the Secretary -** In addition to notifying affected individuals and the media (where appropriate), CCOB must notify the Secretary of the Department of Health and Human Services (DCCOB) of breaches of unsecured PHI. CCOB will notify the Secretary of DCCOB by visiting the DHHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, CCOB must notify the Secretary of DHHS without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may maintain a log or other documentation of the breaches and notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary of DHHS no later than 60 days after the end of the calendar year in which the breaches occurred. (45 CFR 164.408)

45 CFR 160 & 164 – Determination If A Breach Occurred?




45 CFR 160 & 164 - Breach Notification for Unsecured PHI
Did a Breach of Unsecured PHI Occur?
No
Document risk assessment in making this determination.
End
Yes
Does it meet exceptions?
Yes
No
Notify Broomfield CMO, CAO, and PIO of Breach
Is Law Enforcement requesting a delay?
Yes
Document Law Enforcement request
No
Did the breach affect more than 500?
Yes
Complete online notification
Issue Media Notification
No
Issue Notification to Individual(s)
Log Incident for Annual Report to Feds - DHHS

Section 4:

HIPAA Security Standards

HIPAA Security Standards

Policy: HIPAA requires that CCOB enact policies and procedures regarding the employees, interns and volunteers who access PHI. Security standards require each health care component to ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains or transmits; to protect against any reasonably anticipated threats or hazards to the security or integrity of such information; to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required and to ensure compliance within its workforce. Agencies will meet these requirements through the implementation of Administrative, Physical and Technical Safeguards. Security measures implemented for the reasonable and appropriate protection of ePHI will be reviewed, updated, and modified, as necessary, on a regular basis.

Procedure:

I. **Administrative Safeguards:** Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage workforce conduct in relation to the protection of that information. In furtherance of its security management process, CCOB will develop and implement appropriate administrative safeguards, including but not limited to the following:

- **Risk Analysis:** Consisting of an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
- **Risk Management:** Including the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Disciplinary Action subject to the Personnel Merit System:** To be applied against workforce members who fail to comply with security policies and procedures.
- **Information System Activity Reviews:** Designed to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.
- **Designated Security Officer:** CCOB security official who will be responsible for the development and implementation of the overall CCOB Hybrid Policies and Procedures.
- **Workforce Security, Awareness and Training:** Designed to ensure appropriate access, and to prevent inappropriate access, to ePHI by workforce members.
- **Security Incident Procedures:** Consisting of policies and procedures to address security incidents.
- **Contingency Planning:** To include data backup plans, disaster recovery plans, emergency mode operation plans and other appropriate testing and revision procedures, applications and data analyses.
- **Periodic Evaluations:** Including technical and nontechnical evaluations based upon HIPAA standards and also other responses to environmental or operational changes affecting the security of ePHI at CCOB.

- **Business Associate Agreements:** Written contracts designed to obtain satisfactory assurances that those entities that create, receive, maintain or transmit ePHI on CCOB's behalf will appropriately safeguard the information.

II. **Physical Safeguards:** Physical safeguards are physical measures, policies and procedures to protect electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. CCOB will develop and implement physical safeguards appropriate to its environment, including but not limited to the following:

- Facility Access Controls: Designed to limit physical access to its electronic IT systems and to ensure that proper authorized access is allowed.
- Workstation Use and Security: Implementing physical safeguards for workstations and restricting access to authorized users.
- Device and Media Controls: Including the receipt and removal of hardware and electronic media that contain ePHI and the physical movement of such items within CCOB facilities.

III. **Technical Safeguards:** Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and controls access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Workforce Access to PHI

Policy: Access to computer applications that contain PHI shall be granted to members of the CCOB Workforce only on a need-to-know basis and in compliance with the Minimum Necessary Policy. Role Based Access shall be established for each member of the CCOB Workforce, modified upon that person's change in job functions, and terminated at the end of that person's employment or contract.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate

access to ePHI. The City recognizes that the Workforce Security and Information Access Management requirements within the Security Rule are "Addressable" as that term is defined within applicable HIPAA regulations. The City does not have a health care clearinghouse function, which would otherwise trigger certain implementation requirements.

It is neither reasonable nor appropriate for there to be uniform, City-wide procedures due to the unique variables affecting which workforce members need access to ePHI within certain agencies. Efforts will be undertaken to develop specific access control policies at the agency level to the extent practicable following the below procedures as guidance.

Procedure for Access for CCOB Employees: Granting authorization to access ePHI should focus on factors such as access to a workstation, transaction, program, process, or other similar mechanisms, and to modify such right of access as necessary. Access authorization should be established, documented, reviewed, and modified as necessary on a regular basis. CCOB Managers and/or CCOB Division Supervisors will alert the Component HIPAA Privacy Officer of an employee's need to access secured databases containing PHI. The HIPAA Component Privacy Officer will be responsible for the following:

- Liaison between the Component and the CCOB IT Department.
- Work with Division Supervisor and CCOB workforce members to complete the necessary training, authorization forms, and certifications of the employee's legitimate need to access secured PHI for ongoing business purposes.
- Educating CCOB employee on:
    - Password use and best practices, log-in monitoring 45 CFR 164.308
    - City and County of Broomfield's virus protection (protection from malicious software) CFR 154.308
    - Access control and validation:
        - Use of ID badge to access building (45 CFR 164.310)
        - Use of unique CCOB username and log-in (computer will lock after set amount of time, ctrl-alt-delete to log back on). (Reference 45 CFR 164.312 Unique User Identification)
        - Encrypted flash drive use (Reference 45 CFR 164.312 (e) Transmission Security)
        - Encrypted email use (Reference 45 CFR 164.312 (e) Transmission Security)
- Maintaining CCOB workforce records to include: access request forms (for all databases with PHI requested), signed statements of compliance, any access ID's verifications sent from the access control center and access revocations forms.

Any operating procedures relating to PHI data access that are unique to the component that differ from this standard, including access to any State, Federal, or third-party systems required by the component, shall be addressed in the component attachment.

Supervision: Once determined which workforce members are authorized to have access to ePHI, access control procedures will be implemented for the supervision of these workforce members to ensure that the appropriate level of access is maintained to individuals working on, or near, ePHI or other PHI.

The extent of screening process prior to granting access clearance is dependent on an assessment of risk, cost, benefit and feasibility, as well as other protective measures in place. Depending on the level of

access to PHI, it may be necessary to conduct background checks on permanent or temporary staff prior to hiring and/or to have workforce members sign confidentiality or non-disclosure agreements as part of the terms and conditions of employment.

Procedure for Terminating Access for CCOB Employees: Access will be terminated when the employment of or relationship with a workforce member ends, or when a workforce member moves from one healthcare component to another agency of the City. CCOB Managers and/or CCOB Division Supervisors will be responsible for informing the HIPAA Component Privacy Officer when a CCOB workforce member under their charge with access to PHI changes roles or terminates employment with the CCOB. The HIPAA Component Privacy Officer shall:

- Determine if continued or modified access to PHI data is necessary and work with CCOB IT Department to make the necessary changes.
- Ensure that an IT Help Request is submitted within 24 hours of employment separation to disconnect email access and intranet access.
- Ensure that all access devices are returned at the time of termination or any transfer.
- In the event of a uniquely adverse staff termination, IT will be notified prior to informing the workforce member of his or her termination to ensure that information and systems are protected from potential retaliation.
- Retain documentation of termination documents in the file and retain for six (6) years for auditing purposes.

Any operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, shall be addressed in the component attachment.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.308(a)(3) & (a)(4).

Workforce Training for Volunteers and Interns

Purpose: HIPAA requires that CCOB enact policies and procedures regarding the training of employees, interns and volunteers who access PHI, Personal Identifiable Information (PII) and Individually Identifiable Health Information (IIHI).

Policy for CCOB Volunteers and Interns: It is the responsibility of the CCOB Component HIPAA Privacy Officers to manage, monitor, train and oversee the work of any interns or volunteers, as well as to ensure that volunteers and interns receive the training and education required by this policy.
It is the responsibility of the CCOB Component HIPAA Privacy Officer to either:

- Access the training materials on the CCOB intranet and provide HIPAA training to the volunteer or intern prior to the volunteer or intern accessing PHI, or

- Refer any interns or volunteers to the HIPAA Privacy Officer for HIPAA training, delaying the start of the volunteer or intern duties until successful completion of HIPAA training.

Procedure: All CCOB interns and volunteers will be provided HIPAA training by the HIPAA Component Privacy Officer or designated CCOB staff. Upon completion of training, CCOB volunteers and interns will sign a HIPAA Confidentiality Agreement. Documentation shall be retained and if applicable, forwarded on to law enforcement and/or the State of Federal entities responsible for HIPAA enforcement.

Documentation: All training must be documented. The CCOB HIPAA Component Privacy Officers will forward the verification of training to the CCOB HIPAA Privacy Officer to be included in the HIPAA training compliance file.

Sanctions:

- Should a CCOB intern or volunteer violate HIPAA or confidentiality they will be immediately terminated from accessing CCOB facility and/or any database, technology or information.
- If a HIPAA breach was involved, CCOB will notify the appropriate authorities and will follow the procedures in the Breach Notification Policy.
- The volunteer or intern could be liable for civil monetary penalties.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.308(a)(3) & (a)(4).

Policy for Security Awareness and Training of CCOB Employees

Purpose: The purpose of this policy is to provide educational and training procedures for management and CCOB employees.

Policy: The CCOB Security Officer (IT Senior Security Analyst) is responsible for the development of a security awareness and training program for members of the City's workforce which have access to ePHI. The program includes, but is not limited to, the elements described below. All policies, processes and standards related to Security Awareness and Training will be reviewed for updates to the content on an annual basis.

CCOB recognizes that the Security Awareness and Training requirements within the Security Rule are "Addressable" as that term is defined within applicable HIPAA regulations. However, in the event that the IT Department determines that any of the measures described below are not reasonable or appropriate for a particular agency, IT will document the basis for this determination and will decide if equivalent measures can be implemented in the alternative.

All CCOB employees are required to attend and complete all applicable education, training, and/or courses as defined and required by local, state and federal laws, or as identified on an as needed basis by CCOB Managers. CCOB employees have access to all policies and procedures, as well as training materials, on the CCOB intranet. (45 CFR 164.316)

The Information Technology Department will utilize various monitoring tools and software to guard against, detect and report malicious software or other similar threats. Examples of such threats are viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures. The Information Technology Department is responsible for ensuring that any system that has been infected by malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

The Information Technology Department will also employ various procedures for monitoring log-in attempts and reporting discrepancies for CCOB maintained systems. For example, systems may be implemented wherein after five failed log-in attempts, a user is locked out of his or her account and must call the Information Technology Department help desk to have the password reset. Log-in monitoring, logging and review procedures may be detailed in an audit control and review plan. Failed log-in attempts of a suspicious nature must be reported immediately to the Chief Information Security Officer or his or her designee.

The Information Technology Department will implement procedures for creating, changing, and safeguarding workforce members' passwords. For example, passwords will expire on a regular basis and there will be a minimum complexity character requirement for all passwords. Generic user identification and passwords will not be utilized for access to shared or common area workstations that have access to ePHI.

Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following: (i) passwords are only to be used for legitimate access to networks, systems, or applications; (ii) passwords must not be disclosed to other workforce members; (iii) workforce members must not allow others to use their passwords; (iv) passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad which is accessible by other workforce members.

Procedure: Trainings include, but are not limited to:

- HIPAA and Security Awareness Training – Upon initiation of employment.
- Annual HIPAA and Security Awareness Training – For any and all CCOB staff that have access to PHI.
- Component specific training materials shall be addressed in the component attachment.
- Periodic security updates will be sent to workforce members. For example, procedures to ensure that warnings are issued that relate to discovered or reported threats, breaches or other HIPAA security incidents.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.308.

Risk Assessment and Security Incident Procedures

Policy: CCOB will implement policies and procedures to address security incidents involving the improper use and/or disclosure of ePHI. CCOB will identify and respond to suspected or known security incidents, mitigate harmful effects and document the outcome of each incident. It is the policy of CCOB that any discovered impermissible acquisition, access, use or disclosure of unsecured PHI, under circumstances where no exception applies, is presumed to be a breach, and the City will either: (a) treat the presumed breach as a reportable breach and provide all required notifications, or (b) conduct a thorough Risk Assessment of the circumstances to determine whether or not there is greater than a low probability the PHI has been compromised in order to determine whether notice is required.

Procedure: Response and Reporting - CCOB's Information Technology Department will maintain an incident response plan designed to investigate, identify and respond to security incidents, and to mitigate, to the extent practicable, any harmful effects of known security incidents that affect the CCOB or any of its business associates.

Definition of Breach

> A breach is, generally, an impermissible acquisition, access, use or disclosure of unsecured PHI under the Privacy Rule that compromises the security or privacy of PHI. An impermissible acquisition, access, use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised (LoProCo).

Factors to Consider: A risk assessment to determine the likelihood PHI has been compromised must consider at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually accessed or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Discretion: HIPAA allows covered entities and business associates, including CCOB, discretion to provide the required breach notifications following an impermissible acquisition, access, use or disclosure without performing a risk assessment to determine the probability that the PHI has been compromised. The decision regarding whether to provide breach notification or conduct a Risk Assessment prior to determining whether notification is required will be made by the Privacy Officer.

Breach Notification: If the risk assessment of the impermissible acquisition, access, use or disclosure demonstrates there is no more than a low probability the PHI has been compromised, the incident is not considered a breach under the Breach Notification rule, and notice is not required. However, documentation of the impermissible acquisition, access, use or disclosure and the risk assessment must be maintained.

Exceptions: There are three exceptions to the definition of "breach" for purposes of the Breach Notification Rule:

1. The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.

2. The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

When an exception applies, the impermissible action is not considered a breach and no notification is required.

Documentation: All security incidents and their outcomes will be ticked and otherwise documented. Such documentation will be maintained for a minimum of six years.

Device and Media Controls

Policy: Electronic media includes, but is not limited to: (1) electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and (2) transmission media used to exchange information already in electronic storage media (*e.g.*, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media). Certain transmissions (*e.g.*, paper, facsimile, and voice via telephone) are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. CCOB healthcare components will implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a CCOB building or other premises where CCOB workforce members access ePHI, as well as the movement of these items with such locations.

Procedure:

Security for Portable Devices and Media: Portable devices such as smartphones and tablets can be used for many of the same functions as a standard computer. Sensitive information they contain must be protected, as these devices are at a greater risk for loss or theft than larger devices. Memory sticks and external hard drives store a lot of data into small packages. CCOB healthcare components must only store ePHI on portable devices, memory sticks or other portable media in limited circumstances. If ePHI is stored on such devices, it must be de-identified or encrypted. All portable devices should be password protected and protected from theft and loss to the maximum extent possible.

Disposal: CCOB healthcare components will implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. At a minimum, when destroying ePHI which is no longer needed, hard-drives, CDs, zip disks, or back-up takes will be "cleaned" before recycling or re-using electronic media. An IT professional must overwrite, degauss or destroy digital media before discarding it via magnets or special software tools.

Media Re-Use: Agencies will implement procedures for the removal of ePHI from electronic media before the media are made available for re-use.

Accountability: Agencies will maintain a record of the movements of hardware and electronic media containing ePHI and any person responsible therefore. Consideration should be given to whether all types of hardware and electronic media that can be tracked have been identified, and if there are multiple devices of the same type, whether there is a way to identify individual devices and log or record them separately (*e.g.*, via the use of serial numbers). If maintenance of such records is not reasonable and appropriate, the agency is responsible for documenting why and will implement other equivalent alternative measures if reasonable and appropriate.

Data backup and storage: Agencies will create a retrievable, exact copy of ePHI, when needed, before movement of equipment. If such a measure is not reasonable and appropriate, the agency is responsible for documenting why and will implement other equivalent alternative measures if reasonable and appropriate.

Facility Access Controls

Policy: CCOB recognizes the importance of evaluating security controls in place through an accurate risk analysis and of determining whether physical vulnerabilities require that certain controls be implemented. When evaluating and implementing physical safeguards, agencies will consider all physical access to ePHI, which may extend outside of offices and likely includes workforce members' homes or other physical locations where ePHI is accessed.

CCOB healthcare components will implement procedures that limit physical access to its electronic information systems and the physical premises in which they are housed, while ensuring that properly authorized access to ePHI is allowed. Procedures will be developed and implemented that address allowing authorized and limiting unauthorized physical access to ePHI systems, identifying individuals with authorized access by title and/or job function. The Facility Access Controls standard under HIPAA has four implementation specifications which are "Addressable" as that term is defined within applicable HIPAA regulations. Where reasonable and appropriate, CCOB healthcare components will implement the specifications below. If not reasonable and appropriate, components will document why and implement an equivalent alternative measure if reasonable and appropriate.

Procedure:

Contingency Operations: Components will establish and implement, as needed, policies and procedures that allow facility access in support of restoration of lost data under CCOB's disaster recovery plan and emergency mode operations plan in the event of an emergency. Contingency operations may be set in motion during or immediately following a disaster or emergency situation. During contingency operations, it may be important to maintain physical security and appropriate access to ePHI while allowing for data restoration activities. For example, it may be necessary to post guards at entrances to the premises or have escorts for authorized individuals to access the premises for data restoration purposes.

Facility Security Plan: Components will establish and implement policies and procedures to safeguard the premises and equipment from unauthorized physical access, tampering, and theft. In general, physical access controls allow individuals with legitimate business needs to obtain access to the premises and deny access to those without legitimate business needs. Some common controls to prevent unauthorized physical access, tampering, and theft include measures such as locked doors, signs warning of restricted areas, surveillance cameras and alarms.

Access Control and Validation Procedures: Components will implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. Functional or role-based access control and validation procedures should be closely aligned with the component's security plan. Personnel controls such as identification badges, visitor badges and/or escorts may also be utilized.

Maintenance Records: Components will implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (*e.g.*, hardware, walls, doors, and locks). Documentation may simply be a logbook that notes the date, reason for repair, or modification and who authorized it. Or, various repairs and modifications of physical security components may need to be documented in more detail and maintained in a database.

Contingency and Data Backup Planning

Policy: A contingency plan is an alternate way of doing business when established routines are disrupted. CCOB's Information Technology Department will establish policies and procedures for responding to an emergency or other occurrence that could damage systems that contain ePHI. Examples of such occurrences include, but are not limited to, fire, vandalism, system failures, and natural disasters.

Procedure:

Data Backup Plan: At a base level, the proper technology must be implemented to ensure that ePHI is backed up regularly and can be restored. Procedures will be established and implemented that allow for exact copies of ePHI to be retrieved and maintained. As technical infrastructure is upgraded, new applications are implemented, and systems otherwise change, the contingency plan will be updated to reflect significant changes. Changes must be addressed in the context of the contingency plan, verifying that the plan can accommodate the additions and changes in the case of a disaster or system outage.

Disaster Recovery Plan: The various disaster recovery options applicable to the CCOB's environment will be assessed in order to select the most appropriate disaster recovery approach to ensure that critical applications are recoverable at acceptable levels of risk. Procedures will be established and implemented, as needed, to restore any loss of data. The approach should assess emergency procedures, business and technical processes, organizational and staffing requirements, duplication, and continued access to required physical assets. It should also address technical solutions that include duplicated systems, applications, networks, and data and the ability to switch processing from a failed system to the duplicate system.

Emergency Mode Operation: Procedures to enable the continuation of critical business processes for protection of the security of ePHI while operating in emergency mode will be established and as needed, implemented.

Testing: Backup and recovery procedures will be tested on a regular basis for CCOB maintained systems. To the extent reasonable and appropriate, contingency plans will be revised after problems are identified in order to correct issues or minimize their impact. If revisions are not reasonable and appropriate, IT will document why and will implement other equivalent alternative measures if reasonable and appropriate.

Applications and Data Criticality Analysis: The relative criticality of specific applications and data in support of other contingency plan components will be assessed if reasonable and appropriate. If not reasonable and appropriate, IT will document why and will implement other equivalent **alternative** measures if reasonable and appropriate.

Policy for Employee Adherence to HIPAA Safeguards

Purpose: HIPAA Security Rule requires that CCOB provide clear policy, procedures and training to CCOB workforce with access to HIPAA related data on the use of safeguards to protect PHI.

Policy: All CCOB employees with access to HIPAA related data will receive training on the HIPAA Security Rule and will be responsible for appropriate physical, technical and administrative safeguards are in place to protect PHI.

Procedure: Each CCOB employee with access to HIPAA related data will be knowledgeable and able to enforce security measures within their work environment. Each Employee with access to PHI will apply the following safeguards, which include but are not limited to, the following:

- Ensure they wear the City and County of Broomfield Identification Badge allowing access to secured work stations.
- Ensure that all visitors will be monitored and escorted through secured work areas.
- Alert the CCOB Managers and/or CCOB Directors if they are aware of any unauthorized access to secured work area.
- Direct visitors to the building reception area to be checked in and routed to appropriate CCOB service.
- Comply with the minimum necessary rule.
- Authenticate the identity and validity of the requester or receiver of PHI prior to transmitting PHI.
- Be responsible for their personal workstation.
    - Keep passwords secure
    - Keep PHI documents in secure area or inaccessible to others
    - PHI that is set to be disposed of will be shredded. Should the employee have a shred box, the shred box items will either be destroyed daily or secured upon the employee leaving the workstation so that unauthorized access to PHI does not occur.
- Comply with City and County of Broomfield IT policies and procedures.
- Understand the key concepts of confidentiality, integrity and availability as it relates to the Security Measures and safeguards to protect PHI by completing annual HIPAA training.
- Be responsible for adhering to the disposal of paper PHI, PII and IIHI by utilizing the Shred-It bins.
- Be responsible for adhering to the Personnel Merit policy and procedures established by Human Resources.
- Be responsible for reporting to their supervisor and/or division managers any breaches of security, inappropriate use of PHI by others or any deviation from the established PHI safeguards.
- Be responsible for adhering to HIPAA safeguards, pursuant to Federal statute: .
    - Federal ruling: “The Federal common law of agency does not permit the imputation of knowledge to the principal where the agent consciously acts in a manner that is adverse to the principal.”
    - In this citation, the principal is CCOB; the agent is the individual employee.

Enforcement:

All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.310, 312, and 316.

Policy for Employee Use of Mobile Devices

Purpose: The Health Insurance Portability and Accountability Act (HIPAA) Security Rule as amended by the American Recovery and Reinvestment Act of 2009/HITECH Act requires that CCOB provide clear policy, procedures and training to CCOB workforce with access to PHI on the use of safeguards to protect protected health information (PHI) and electronic protected health information (ePHI). Titles 15, 19, 25, 25.5 and 26 of the Colorado Revised Statutes and related regulations require all information relative to CCOB individuals requesting information about potential services or receiving services remain confidential.

Policy: All CCOB employees who are issued a mobile phone or other mobile device are to abide by administrative, technical and security safeguards to ensure the protection of confidential individual information and available ePHI that may be on the mobile phone and/or mobile device. This policy is in addition to the City and County Technology Systems Policy; employees must follow both the city and county wide rules AND this policy aimed at protecting individual confidentiality.

Information covered under this confidentiality provision may include, but is not limited to:

- Names and addresses of individuals.
- Services provided to any individual.
- Information related to the social, economic or financial conditions or circumstances of any individual.
- Agency records or evaluations about individuals or businesses.
- Court records.
- Foster care placement records.
- Current or past medical, psychological or social information including diagnosis relative to any individual.
- Any information or records related to the operation of CCOB.

Steps to Protect Mobile Phones:

1. Currently, each CCOB employee that requires a mobile phone or mobile device for CCOB business will be issued a mobile phone, and, in some instances, an iPad or tablet that will be registered with the CCOB mobile device management system. Most CCOB applications are configured to require a second factor to login. Additional safeguards include the following:

    - Password protection
    - FIPS-140-2 encryption
    - Location tracking, remote disable, and remote wipe

It is the responsibility of each employee to maintain a password to protect their mobile phone and/or mobile device and to ensure that the mobile device management is active.

2. *Web connections*. To the greatest extent possible, all web access from the smart phones should only use SSL (Secure Sockets Layer) protected websites. Employees are prohibited from accessing or managing PHI from unsecure and/or non-business related websites. After clicking on a web link, pay

close attention to the address to make sure it matches the website it claims to be, especially if you are asked to enter account or login information.

Note: Some common business related websites are not HTTPS. Employees may access state, federal and/or local government websites as needed for business purposes.

3. Employees are prohibited from accessing links sent from suspicious emails or text messages. These links may lead to malicious websites.

4. *Data storage*. Employees are encouraged to minimize PHI data stored on mobile phones.

5. Employees are prohibited from texting an individual's PHI even if the employee receives a text from the individual.

6. Employees are expected to maintain physical control of the mobile phone or mobile device, especially in public or semi-public areas.

7. Employees may not 'root' or 'jailbreak' devices. This refers to 3rd party device firmware, which is sometimes used to get access to device features that are locked by default and can contain malicious code or unintentional security vulnerabilities.

8. *Passcode*. Employees will maintain a password so that if the phone is lost or stolen, data is more difficult to access.

9. *Firmware updates*. Employees will download and install firmware updates as recommended by the CCOB IT Department.

Lost Mobile Phones/Devices:

The CCOB employee who loses and/or misplaces a county issued smartphone or tablet shall:

1. Immediately report the loss to the IT Department and follow up with their division supervisor/manager.
    - As soon as the phone is discovered lost or stolen, the employee will request the CCOB IT Department to remotely disable the phone. The Customer Success Specialist can assist staff with this process, if necessary.
    - Division Manager and division staff will conduct an initial risk analysis and determine the likelihood of an ePHI breach or a confidentiality breach. (See Breach Process). Division Manager shall alert Operations Manager within one business day and share results of initial risk analysis.
    - If the lost phone risk analysis is determined to have a high likelihood of an ePHI breach and the phone has not been found, the CCOB IT Department will be contacted to remotely wipe the device

2. Contact the CCOB IT Department to order a replacement phone.

The HIPAA Officer shall determine if breach occurred and follow breach policy and procedures. Consultation with legal counsel is recommended.

Access and Audit Controls

Policy: CCOB Health Care Components must implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted appropriate access rights. Agencies must also implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Procedure:

Unique User Identification

Each workforce member who has a need to access ePHI should be assigned a unique name and/or number for identifying and tracking user identity. Each user's access to ePHI system(s) must be appropriate and authorized. Access should be "role-based" and limited to only the information needed to perform job responsibilities. Unauthorized access to ePHI by former employees must be prevented by immediate termination of access. User access to information systems must be logged and audited for inappropriate access or use.

Emergency Access Procedures

CCOB Health Care Components must establish and as needed, implement, procedures for obtaining necessary ePHI during an emergency.

Automatic Logoff

CCOB Health Care Components must maintain electronic procedures that terminate an electronic session after a predetermined time of inactivity. Devices must be configured to lock or auto log-off and require a user to re-authenticate if left unattended for a certain amount of time (*e.g.*, 10 minutes). Automatic screen savers must also be similarly set.

Encryption and Decryption

CCOB Health Care Components must implement a mechanism to encrypt and decrypt ePHI. Encryption is required for protection of ePHI in transit across email, unsecured networks and communication systems. If such measures are not reasonable and appropriate, the agency is responsible for documenting why and will implement other equivalent alternative measures if reasonable and appropriate.

All remote access of ePHI must be encrypted, which may be accomplished by using a Virtual Private Network (VPN) or other secure connection methods. Remote access to ePHI requires departmental approval. Coffee shop, hotel, airport and similar wireless connections are not encrypted and workforce members must not access systems containing ePHI utilizing such connections. Workforce members must also avoid connecting to unknown wireless hot spots/access points.

Network Segmentation

Transfer of PHI held by an agency to another component of the hybrid entity is a disclosure under the HIPAA Privacy Rule, and thus, allowed only to the same extent such a disclosure is permitted to a separate entity. Adequate separation provided by the use of firewalls between external networks and the CCOB networks must be maintained in order to protect the inappropriate access, use, or

disclosure of ePHI. Group Policies that control access based on position or role are currently in place limiting access to internal CCOB network resources and applications.

Integrity, Person/Entity Authentication and Transmission Security

Policy: Risks to integrity of confidential information include, but are not limited to, data corruption, destruction, and unavailability of patient information in an emergency. Healthcare components must implement policies and procedures to protect ePHI from improper alteration or destruction and to verify that a person or entity seeking access to ePHI is the one claimed. Agencies must also implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Procedure: Healthcare components should identify electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner and otherwise implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. If implementing such measures is not reasonable and appropriate, each component is responsible for documenting why and will implement other equivalent alternative measures if reasonable and appropriate.

Section 5: Forms

- HIPAA AUTHORIZATION TO DISCLOSE INFORMATION FORM (English)
- HIPAA AUTHORIZATION TO DISCLOSE INFORMATION FORM (Spanish)
- HIPAA BUSINESS ASSOCIATE ADDENDUM TO AGREEMENT (English)
- HIPAA CONFIDENTIALITY AGREEMENT (English)
- HIPAA NOTICE OF PRIVACY PRACTICES FORM (English)
- HIPAA NOTICE OF PRIVACY PRACTICES FORM (Spanish)
- HIPAA PRIVACY RIGHTS REQUEST FORM (English)
- HIPAA PRIVACY RIGHTS REQUEST FORM (Spanish)
- HIPAA REQUEST TO AMEND OR CORRECT PROTECTED HEALTH INFORMATION (English)
- HIPAA REQUEST TO AMEND OR CORRECT PROTECTED HEALTH INFORMATION (Spanish)

Section 6: Component HIPAA Attachments

HEALTH CARE COMPONENTS FOR
THE CITY AND COUNTY OF BROOMFIELD
DESIGNATION AS A HYBRID ENTITY UNDER HIPAA

The following are designated healthcare components:

HUMAN RESOURCES (Leave Benefits Administration)	Attachment 1
HUMAN SERVICES	Attachment 2
INFORMATION TECHNOLOGY (General Administrative Systems Access)	Attachment 3
POLICE (Detention - Inmate Health Services)	Attachment 4
PUBLIC HEALTH	Attachment 5

CITY AND COUNTY OF BROOMFIELD
One DesCombes Drive • Broomfield, CO 80020 • 303.469.3301 • www.broomfield.org

Policy and Procedures for updated HIPAA Authorization to Disclose Information Form - February 2017

Purpose:

HIPAA prohibits the City and County of Broomfield (CCOB) from using or disclosing PHI without a valid authorization except in certain circumstances. When the CCOB obtains a valid authorization, such use or disclosure of PHI must be consistent with the purpose of the authorization. 45 CFR 164.508 (updated 2/2017)

Policy:

The CCOB may voluntarily choose, but is not required, to obtain an individual's consent for it to use and disclose information about a client for treatment, payment, and health care operations (TPO). A "consent" document is not a valid permission to use or disclose protected health information for a purpose that requires an "authorization" under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of protected health information.

Definitions From DHHS and OCR Website
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpp.html

Treatment: Generally means the provision, coordination, or management of health care and related services among health care providers or by a healthcare provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Payment: Encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
- Utilization review activities; and
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

Health care operations: Are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501,include:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing healthcare costs, and case management and care coordination;
- Reviewing the competence or qualifications of healthcare professionals, evaluating provider and health plan performance, training health care and non health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- Conducting or arranging for medical review, legal, and auditing services,including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. General Provisions at 45 CFR 164.506.

Circumstances where no authorization is required to share PHI (besides TPO noted above). The CCOB may, without the individual's authorization:

- Use or disclose protected health information for its own treatment, payment, and health care operations activities. For example:
  - A hospital may use protected health information about an individual to provide healthcare to the individual and may consult with other health care providers about the individual's treatment.
  - A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
  - A health plan may use protected health information to provide customer service to its enrollees.
- The CCOB may disclose protected health information for the treatment activities of any healthcare provider (including providers not covered by the Privacy Rule). For example:
  - A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
  - A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred.
  - A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information. For example:
    - A covered entity may disclose protected health information to another covered entity for certain health care operation activities of the entity that receives the information if:
      - Each entity either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship; and the disclosure is for a quality-related health care operations activity (i.e., the activities listed in paragraphs (1) and (2) of the definition of "health care operations" at 45 CFR 164.501) or for the purpose of health care fraud and abuse detection or compliance. For example: A healthcare provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.

Circumstances where an <u>Authorization to Disclose Information</u> is mandated:

1. Authorization for any use or disclosure of <u>psychotherapy</u> notes, except:
   - To carry out the following treatment, payment, or health care operations:
     - (A) Use by the originator of the psychotherapy notes for treatment;
     - (B) Use or disclosure by the CCOB for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
     - (C) Use or disclosure by the CCOB to defend itself in a legal action or other proceeding brought by the individual; and
2. Authorization required: Marketing.
   - The CCOB must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
     - A face-to-face communication made by the CCOB to an individual; or
     - A promotional gift of nominal value provided by the CCOB.
   - If the marketing involves direct or indirect remuneration to the CCOB from a third party, the authorization must state that such remuneration is involved.

Documentation Requirements:

1. The CCOB must document and retain any signed authorization in the client's file.

Elements of a valid Authorization to Disclose Information Form:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
3. The name or other specific identification of the person(s), or class of persons, to whom the CCOB may make the requested use or disclosure.

4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information including for the creation and maintenance of a research database or research repository.
6. Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

Additionally, there are Required Statements for a valid Authorization to Disclose Information Form. The Authorization must contain statements adequate to place the individual on notice of all of the following:

1. The individual's right to revoke the authorization in writing.
2. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
    - The CCOB may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
    - The consequences to the individual of a refusal to sign the authorization when the CCOB can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
3. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected.

The Authorization must be in "plain language".

A copy is provided to the CCOB client. If the CCOB seeks an authorization from an individual for a use or disclosure of protected health information, then the CCOB must provide the individual with a copy of the signed authorization.

AUTHORIZATION TO DISCLOSE INFORMATION

To allow a THIRD PARTY to have access to Protected Health/Personal Information

CLIENT INFORMATION

Client Name: _____ Date of Birth: _____ State ID #, Client #, or Social Security#:_____

Address, City, State, Zip: _____

The City and County of Broomfield is authorized to disclose my Protected Health/Personal Information as specified below to the following person(s) or organization(s):

NAME: _____ PHONE NUMBER: _____

ORGANIZATION: _____

ADDRESS: _____

Information to be disclosed:

_____

_____

PURPOSE OR NEED FOR INFORMATION BEING REQUESTED: (If you prefer not to state a purpose, please state "At the request of the individual")

_____

_____

EXPIRATION OF AUTHORIZATION: This Authorization will expire in one year from the date signed below, unless another date or event is listed.

From _____ To _____.

REQUIRED STATEMENTS:

I understand that the information provided based on this Authorization may be re-disclosed to another party by the authorized recipient,and that the City and County of Broomfield has no control over that additional disclosure and can not protect the information after it is released based on this Authorization.

I understand that I may revoke this Authorization at any time in writing to the address below.I understand that I can verbally revoke this Authorization by contacting the CCOB office at 303-438-6286. I understand that any revocation can only apply to future disclosures or actions regarding the disclosure of my information and cannot cancel actions take or disclosures made while the authorization was in effect.

I understand that the City and County of Broomfield may not condition my health care treatment or payment, or my enrollment or eligibility for benefits on my executing this Authorization.

I understand that if I request my complete medical record to be disclosed and my record contains information related to HIV infection, AIDS or AIDS-related conditions, psychological or psychiatric conditions, or genetic testing, this disclosure will include that information. I also understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment, payment for services,or my eligibility for services.

I certify that this request has been made voluntarily and that the information given is accurate to the best of my knowledge. A copy of this executed Authorization is as effective as the original.

CLIENT SIGNATURE:_____ **DATE:** _____

Parent or Legal Guardian may sign on behalf of minor child. Legal Guardian, Power of Attorney, or equivalent may sign on behalf of adult -documentation is required.

Personal Representative _____ *Relationship* _____

_____

Revocation by Client:

I,_____, hereby revoke this authorization to disclose protected health/personal information.

CLIENT SIGNATURE:_____ **DATE:** _____

Verbal Revocation by Client:

I attest to the verbal request to revoke this authorization to disclose protected health/personal information on this date.

Print Name of Staff: _____ **DATE:** _____

Signature of Staff: _____

Política y procedimientos para el Formulario actualizado de autorización para la revelación de información de HIPAA (febrero de 2017)

Propósito:

La HIPAA prohíbe a la Ciudad y el Condado de Broomfield (City and County of Broomfield, CCOB) usar o revelar la información médica protegida (PHI) sin una autorización válida, excepto en ciertas circunstancias. Cuando CCOB recibe una autorización válida, dicho uso o revelación de la PHI debe ser coherente con el propósito de la autorización. 45 CFR 164.508 (actualizada en 2/2017)

Política:

La CCOB puede elegir voluntariamente, pero no está en la obligación, de obtener un consentimiento de una persona para usar y revelar información sobre un cliente para tratamiento, pagos y operaciones de atención médica (TPO). Un documento de "consentimiento" no es un permiso válido para usar o revelar información médica protegida para un propósito que necesita una "autorización" según la Regla de Privacidad (consulte 45 CFR 164.508) o cuando existen otros requisitos o condiciones según la Regla para el uso o revelación de la información médica protegida.

Definiciones del sitio web del DHHS y OCR
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpp.html

Tratamiento: En general, significa la prestación, coordinación o gestión de atención médica y servicios relacionados entre proveedores de atención médica o de un proveedor de atención médica a un tercero, la consulta entre proveedores de atención médica sobre un paciente o la remisión de un paciente de un proveedor de atención médica a otro.

Pago: Incluye las diversas actividades de los proveedores de atención médica para obtener un pago o reembolso por sus servicios y de un plan médico para recibir primas, cumplir sus responsabilidades de cobertura ofrecer beneficios bajo el plan, y para recibir o dar reembolso por la prestación de atención médica. Además de la definición general, la Regla de Privacidad da ejemplos de actividades frecuentes de pago, que incluyen, por ejemplo:

- Determinar elegibilidad o cobertura bajo un plan y adjudicación de reclamos;
- Ajuste de riesgo;
- Facturación y actividades de cobro;
- Revisión de los servicios de atención médica para una necesidad médica, cobertura, justificación de gastos y cosas similares;
- Actividades de revisión del uso; y
- Revelaciones a agencias de informes del consumidor (limitado a información de identificación específica de la persona, su historial de pagos e información de identificación de la entidad cubierta).

Operaciones de atención médica: Son ciertas actividades administrativas, financieras, legales y de mejora de calidad de una entidad cubierta que son necesarias para que su negocio funcione y para apoyar las funciones básicas de tratamiento y pagos. Estas actividades, que son limitadas a las actividades incluidas en la lista que aparece en la definición de "operaciones de atención médica" en 45 CFR 164.501, incluyen:

- Desarrollo de evaluación de calidad y actividades de mejora, actividades basadas en la población relacionadas con la mejora de la salud o reducción del costo de la atención médica, y la administración de casos y la coordinación de atención;
- Revisión de las capacidades o calificaciones de los profesionales de atención médica, evaluación del desempeño de los proveedores y planes médicos, capacitación para profesionales de atención médica y profesionales que no son de atención médica, actividades de acreditación, certificación, concesión de licencias o credenciales;
- Redacción y otras actividades relacionadas con la creación, renovación o reemplazo de un contrato de seguro médico o beneficios médicos, y la transferencia, garantía o colocación de un contrato para reaseguración de riesgos relacionados con reclamos de atención médica;
- Dirigir u organizar servicios de revisión médica, legales y de auditoría, incluyendo programas de detección de fraude y abuso y de cumplimiento;
- Planificación y desarrollo empresarial, cómo hacer análisis de administración de costos y planificación relacionados con la administración y operación de la entidad; y
- Actividades de gestión empresarial y de administración general, incluyendo las relacionadas con la implementación y cumplimiento de la Regla de privacidad y otras Reglas de simplificación administrativa, servicio al cliente, resolución de quejas internas, venta o transferencia de activos, creación de información médica no identificable o un conjunto de datos limitados, y recaudación de fondos en beneficio de la entidad cubierta. Disposiciones generales en 45 CFR 164.506.

Circunstancias en las que no se necesita autorización para compartir la PHI (además de TPO que se menciona arriba). CCOB puede, sin autorización de la persona:

- Usar o revelar información médica protegida para sus propias actividades de tratamiento, pagos y operaciones de atención médica. Por ejemplo:
  - Un hospital puede usar información médica protegida sobre una persona para darle atención médica y puede consultar a otros proveedores de atención médica sobre el tratamiento de la persona.
  - Un proveedor de atención médica puede revelar información médica protegida sobre una persona como parte de un reclamo de pago a un plan médico.
  - Un plan médico puede usar información médica protegida para prestar servicio al cliente a sus afiliados.
- CCOB puede revelar información médica protegida para actividades de tratamiento a cualquier proveedor de atención médica (incluyendo proveedores no cubiertos por la Regla de privacidad). Por ejemplo:
  - Un proveedor de atención primaria puede enviar una copia del registro médico de una persona a un especialista que necesite la información para tratarla.
  - Un hospital puede enviar instrucciones de atención médica de un paciente a un asilo de ancianos al que se transfiera el paciente.
  - Una entidad cubierta puede revelar información médica protegida a otra entidad cubierta o a un proveedor de atención médica (incluyendo proveedores no cubiertos por la Regla de privacidad) para las actividades de pago de la entidad que recibe la información. Por ejemplo:
    - Una entidad cubierta puede revelar información médica protegida a otra entidad cubierta para ciertas actividades de operación de atención médica de la entidad que recibe la información si:
      - Cada entidad tiene o tuvo una relación con la persona que es beneficiaria de la información y la información médica protegida pertenece a la relación; y la revelación es para una actividad de las operaciones de atención médica relacionada con la calidad (p.ej., las actividades que se listan en los párrafos (1) y (2) de la definición de "operaciones de atención médica" en 45 CFR 164.501) o con el propósito de detectar fraude y abuso en la atención médica o el cumplimiento de esta. Por ejemplo: Un proveedor de atención médica puede revelar información médica protegida a un plan médico para fines del Conjunto de datos e información del plan médico del empleador (Health Plan Employer Data and Information Set, HEDIS), siempre y cuando el plan médico tenga o haya tenido una relación con la persona que es sujeto de la información.

Circunstancias en las que se necesita una <u>Autorización para revelar información</u>:

1. Autorización para cualquier uso o revelación de notas de <u>psicoterapia,</u> excepto:
   - Para hacer los siguientes tratamientos, pagos u operaciones de atención médica:
     - (A) Uso por parte del autor de las notas de psicoterapia para tratamiento;
     - (B) Uso o revelación de CCOB para sus propios programas de capacitación en el que los estudiantes, practicantes o proveedores de salud mental aprenden bajo supervisión a practicar y mejorar sus competencias en consejería grupal, conjunta, familiar o individual; o
     - (C) Uso o revelación de la CCOB para defenderse en una acción legal u otro procedimiento iniciado por la persona; y
2. Se necesita autorización: Marketing.
   - CCOB debe obtener una autorización para cualquier uso o revelación de información médica protegida para el marketing, excepto que la comunicación sea:
     - Una comunicación cara a cara hecha por CCOB a una persona; o
     - Un regalo de promoción de valor nominal de la CCOB.
   - Si el marketing involucra una remuneración directa o indirecta a la CCOB de un tercero, la autorización debe indicar dicha remuneración involucrada.

Requisitos de documentación:

1. La CCOB debe documentar y conservar cualquier autorización con firma en el archivo del cliente.

Elementos de un Formulario de autorización para revelar información:

1. Una descripción de la información que se usará o revelará que identifique la información de forma específica y significativa.
2. El nombre u otra identificación de la persona específica, o clase de persona, autorizada para hacer el uso o revelación que se solicitó.
3. El nombre u otra identificación específica de la persona, o clase de persona, para las que la CCOB puede hacer el uso o revelación que se solicitó.

4. Una descripción de cada propósito del uso o revelación solicitada. La declaración "a pedido de la persona" es una descripción suficiente para el propósito cuando una persona inicia la autorización y no presenta, o decide no presentar, una declaración del propósito.
5. Una fecha o evento de vencimiento que se relacione con la persona o el propósito del uso o revelación. La declaración "fin de la investigación", "ninguno", o frase similar es suficiente si la autorización es para el uso o revelación de información médica protegida incluyendo la creación y mantenimiento de una base de datos o un repositorio de una investigación.
6. Firma de la persona y fecha. Si un representante de la persona firma la autorización, también se debe presentar una descripción de dicha autoridad representativa para actuar en nombre de la persona.

Además, existen declaraciones necesarias para que un Formulario de autorización para revelar información tenga validez. La Autorización debe tener declaraciones adecuadas para notificar a la persona todos los siguientes puntos:

1. El derecho de la persona de anular la autorización por escrito.
2. La capacidad o incapacidad de condicionar el tratamiento, pago, inscripción o elegibilidad para beneficios en la autorización, afirmando:
    - CCOB no puede condicionar el tratamiento, pago, inscripción o elegibilidad para beneficios dependiendo de si la persona firma la autorización cuando rige la prohibición de la condición de autorizaciones; o
    - Las consecuencias de la persona del rechazo a firmar la autorización cuando la CCOB puede condicionar el tratamiento, inscripción en el plan médico o elegibilidad para beneficios si no se obtiene dicha autorización.
3. La posibilidad de revelación de la información de acuerdo con la autorización de que el sujeto vuelva a revelarla y ya no esté protegida.

La Autorización debe estar en "lenguaje claro".

Se entrega una copia al cliente de la CCOB. Si la CCOB busca una autorización de una persona para el uso o revelación de información médica protegida, debe entregar a dicha persona una copia de la autorización firmada.

AUTORIZACIÓN PARA REVELAR INFORMACIÓN

Para permitir que un TERCERO tenga acceso a Información personal/médica protegida

INFORMACIÓN DEL CLIENTE
Nombre del cliente: _____ Fecha de nacimiento: _____
Número de identificación estatal, Número de cliente o Seguro social: _____

Dirección, Ciudad, Estado, Código postal:
_____

La ciudad y el condado de Broomfield tiene autorización para revelar mi Información personal/médica protegida como se especifica abajo a las siguientes personas u organizaciones:
NOMBRE: _____ NÚMERO DE TELÉFONO: _____
ORGANIZACIÓN: _____
DIRECCIÓN: _____
Información que se revelará:
_____
_____

PROPÓSITO O NECESIDAD DE SOLICITAR LA INFORMACIÓN: (Si prefiere no indicar un propósito, escriba "A pedido de la persona")
_____
_____

VENCIMIENTO DE AUTORIZACIÓN: Esta Autorización vencerá en un año desde la fecha de la firma de abajo, a menos que se incluya otra fecha o evento. Desde _____ Hasta _____.

AFIRMACIONES REQUERIDAS:

Entiendo que la información que se dio con base en esta Autorización puede volver a revelarse a otra parte por medio del beneficiario autorizado, y que la Ciudad y el condado de Broomfield no tiene control de esa revelación y no puede proteger la información después de entregarse con base en esta Autorización.

Entiendo que puedo anular esta Autorización en cualquier momento por escrito a la dirección de abajo. Entiendo que puedo anular verbalmente esta Autorización comunicándome con la oficina de la CCOB al 303-438-6286. Entiendo que cualquier revocación sólo puede aplicar a revelaciones o acciones futuras sobre la revelación de mi información y no puede cancelar las acciones o revelaciones hechas mientras esta autorización estaba en vigencia.

Entiendo que la Ciudad y el condado de Broomfield no pueden condicionar mi tratamiento o pago de atención médica, o mi inscripción o elegibilidad para beneficios por el hecho de que ejecute esta Autorización.

Entiendo que si solicito que se revele mi expediente médico completo y mi expediente tiene información relacionada con la infección de VIH, SIDA o condiciones relacionadas a esta, condiciones psicológicas o psiquiátricas o pruebas genéticas, esta revelación incluirá dicha información. También entiendo que puedo negarme a firmar esta autorización y que mi negación a firmar no afectará mi posibilidad de recibir tratamiento, pago de servicios o mi elegibilidad para servicios.

Confirmo que esta solicitud se hizo voluntariamente y que la información que di es correcta a mi entender. Una copia de esta Autorización en ejecución está en efecto como la original.

FIRMA DEL CLIENTE:_____ **FECHA:** _____

El padre, madre o tutor legal deben firmar en nombre del menor. El tutor legal, poder notarial o equivalente debe firmar en nombre del adulto (se necesita documentación).

Representante personal _____ *Relación* _____

_____

Revocación del Cliente:
Yo, _____, revoco por medio de la presente esta autorización para revelar información personal/médica protegida.
FIRMA DEL CLIENTE:_____ **FECHA:** _____

Revocación verbal del Cliente:
Yo doy fe de la solicitud verbal de revocar esta autorización para revelar información personal/médica protegida desde esta fecha.
Nombre del personal en letra de molde: _____ **FECHA:** _____
Firma del personal: _____

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("Addendum") is a part of the Contract dated _____, 20__ between the City and County of Broomfield and _____. For purposes of this Addendum, Broomfield is referred to as "Covered Entity" or "CE" and the Contractor is referred to as "Associate". Unless the context clearly requires a distinction between the Contract document and this Addendum, all references herein to "the Contract" or "this Contract" include this Addendum.

RECITALS

A. CE wishes to disclose certain information to Associate pursuant to the terms of the Contract, some of which may constitute Protected Health Information ("PHI") (defined below).

B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d – 1320d-8 ("HIPAA") as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA")/HITECH Act (P.L. 111-005), and its implementing regulations promulgated by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162 and 164 (the "HIPAA Rules") and other applicable laws, as amended.

C. As part of the HIPAA Rules, the CE is required to enter into a written contract containing specific requirements with Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 160.103, 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Addendum.

The parties agree as follows:

1. Definitions.

a. Except as otherwise defined herein, capitalized terms in this Addendum shall have the definitions set forth in the HIPAA Rules at 45 C.F.R. Parts 160, 162 and 164, as amended. In the event of any conflict between the mandatory provisions of the HIPAA Rules and the provisions of this Contract, the HIPAA Rules shall control. Where the provisions of this Contract differ from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Contract shall control.

b. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.501.

c. "Protected Information" shall mean PHI provided by CE to Associate or created, received, maintained or transmitted by Associate on CE's behalf. To the extent Associate is a covered entity under HIPAA and creates or obtains its own PHI for treatment, payment and health care operations, Protected Information under this Contract does not include any PHI created or obtained by Associate as a covered entity and Associate shall follow its own policies and procedures for accounting, access and amendment of Associate's PHI.

d. "Subcontractor" shall mean a third party to whom Associate delegates a function, activity, or service that involves CE's Protected Information, in order to carry out the responsibilities of this Agreement.

2. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Contract and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the HIPAA Rules if so used by CE, except that Associate may use Protected Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE. Additional provisions, if any, governing permitted uses of Protected Information are set forth in Attachment A to this Addendum. Associate accepts full responsibility for any penalties incurred as a result of Associate's breach of the HIPAA Rules.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the HIPAA Rules if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Contract; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 C.F.R. Section 164.502(j)(1). To the extent that Associate discloses Protected Information to a third party Subcontractor, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances through execution of a written agreement with such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and that such third party will notify Associate within two (2) business days of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.

c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Contract. Associate shall comply with the requirements of the HIPAA Security Rule at 45 C.F.R. Sections 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities. Associate shall review, modify, and update documentation of, its safeguards as needed to ensure continued provision of reasonable and appropriate protection of Protected Information.

d. Reporting of Improper Use or Disclosure. Associate shall report to CE in writing any use or disclosure of Protected Information other than as provided for by this Contract within five (5) business days of becoming aware of such use or disclosure.

e. Associate's Agents. If Associate uses one or more Subcontractors or agents to provide services under the Contract, and such Subcontractors or agents receive or have access to Protected Information, each Subcontractor or agent shall sign an agreement with Associate containing the same provisions as this Addendum and further identifying CE as a third party beneficiary with rights of enforcement and indemnification from such Subcontractors or agents in the event of any violation of such Subcontractor or agent agreement. The Agreement between the Associate and Subcontractor or agent shall ensure that the Subcontractor or agent agrees to at least

the same restrictions and conditions that apply to Associate with respect to such Protected Information. Associate shall implement and maintain sanctions against agents and Subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

f. Access to Protected Information. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate shall make Protected Information maintained by Associate or its agents or Subcontractors in such Designated Record Sets available to CE for inspection and copying within ten (10) business days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.524. If such Protected Information is maintained by Associate in an electronic form or format, Associate must make such Protected Information available to CE in a mutually agreed upon electronic form or format.

g. Amendment of PHI. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate or its agents or Subcontractors shall make such Protected Information available to CE for amendment within ten (10) business days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, and shall incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or Subcontractors, Associate must notify CE in writing within five (5) business days of receipt of the request. Any denial of amendment of Protected Information maintained by Associate or its agents or Subcontractors shall be the responsibility of CE.

h. Accounting Rights. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate and its agents or Subcontractors shall make available to CE within ten (10) business days of notice by CE, the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.528. In the event that the request for an accounting is delivered directly to Associate or its agents or Subcontractors, Associate shall within five (5) business days of the receipt of the request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.

i. Governmental Access to Records. Associate shall keep records and make its internal practices, books and records relating to the use and disclosure of Protected Information available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's or Associate's compliance with the HIPAA Rules. Associate shall provide to CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary when the Secretary is investigating CE. Associate shall cooperate with the Secretary if the Secretary undertakes an investigation or compliance review of Associate's policies, procedures or practices to determine whether Associate is complying with the HIPAA Rules, and permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including Protected Information, that are pertinent to ascertaining compliance.

j. Minimum Necessary. Associate (and its agents or subcontractors) shall only request, use and disclose the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure, in accordance with the Minimum Necessary requirements of the HIPAA Rules including, but not limited to 45 C.F.R. Sections 164.502(b) and 164.514(d).

k. Data Ownership. Associate acknowledges that Associate has no ownership rights with respect to the Protected Information.

l. Retention of Protected Information. Except upon termination of the Contract as provided in Section 4(d) of this Addendum, Associate and its Subcontractors or agents shall retain all Protected Information throughout the term of this Contract and shall continue to maintain the information required under Section 2(h) of this Addendum for a period of six (6) years.

m. Associate's Insurance. Associate shall maintain insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI. All such policies shall meet or exceed the minimum insurance requirements of the Contract (e.g., occurrence basis, combined single dollar limits, annual aggregate dollar limits, additional insured status and notice of cancellation).

n. Notice of Privacy Practices. Associate shall be responsible for reviewing CE's Notice of Privacy Practices, available on CE's external website, to determine any requirements applicable to Associate per this Contract.

o. Notification of Breach. During the term of this Contract, Associate shall notify CE within two (2) business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Associate shall not initiate notification to affected individuals per the HIPAA Rules without prior notification and approval of CE. Information provided to CE shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during the breach. Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

p. Audits, Inspection and Enforcement. Within ten (10) business days of a written request by CE, Associate and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Associate has complied with this Addendum; provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; and (ii) CE shall protect the confidentiality of all confidential and proprietary information of Associate to which CE has access during the course of such inspection. The fact that CE inspects, or fails to inspect, or has the right to inspect, Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract.

q. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted pursuant to the Contract, in accordance with the standards and requirements of the HIPAA Rules.

r. Restrictions and Confidential Communications. Within ten (10) business days of notice by CE of a restriction upon uses or disclosures or request for confidential communications pursuant to 45 C.F.R. Section 164.522, Associate will restrict the use or disclosure of an individual's Protected Information. Associate will not

respond directly to an individual's requests to restrict the use or disclosure of Protected Information or to send all communication of Protect Information to an alternate address. Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to Associate.

3. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted pursuant to the Contract, in accordance with the standards and requirements of the HIPAA Rules.

b. Notice of Changes. CE maintains a copy of its Notice of Privacy Practices on its website. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent that it may affect Associate's permitted or required uses or disclosures. To the extent that it may affect Associate's permitted use or disclosure of PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 C.F.R. Section 164.522.

4. Termination.

a. Material Breach. In addition to any other provisions in the Contract regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of this Contract and shall provide grounds for immediate termination of this Contract by CE pursuant to the provisions of the Contract covering termination for cause, if any. If the Contract contains no express provisions regarding termination for cause, the following terms and conditions shall apply:

(1) Default. If Associate refuses or fails to timely perform any of the provisions of this Contract, CE may notify Associate in writing of the non-performance, and if not promptly corrected within the time specified, CE may terminate this Contract. Associate shall continue performance of this Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services elsewhere.

(2) Associate's Duties. Notwithstanding termination of this Contract, and subject to any directions from CE, Associate shall take timely, reasonable and necessary action to protect and preserve property in the possession of Associate in which CE has an interest.

(3) Compensation. Payment for completed supplies delivered and accepted by CE shall be at the Contract price. In the event of a material breach under paragraph 4a, CE may withhold amounts due Associate as CE deems necessary to protect CE against loss from third party claims of improper use or disclosure and to reimburse CE for the excess costs incurred in procuring similar goods and services elsewhere.

(4) Erroneous Termination for Default. If after such termination it is determined, for any reason, that Associate was not in default, or that Associate's action/inaction was excusable, such termination shall be treated as a termination for convenience, and the rights and obligations of the parties shall be the same as if this Contract had been terminated for convenience, as described in this Contract.

b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement and does not terminate this Contract pursuant to Section 4(a), then CE shall take reasonable steps to cure such breach or end such violation.. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall either (i) terminate the Contract, if feasible or (ii) if termination of this Contract is not feasible, CE shall report Associate's breach or violation to the Secretary of the Department of Health and Human Services. If Associate knows of a pattern of activity or practice of a Subcontractor or agent that constitutes a material breach or violation of the Subcontractor's or agent's obligations under the written agreement between Associate and the Subcontractor or agent, Associate shall take reasonable steps to cure such breach or end such violation, if feasible.

c. Judicial or Administrative Proceedings. Either party may terminate the Contract, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules or other security or privacy laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of the HIPAA Rules or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

d. Effect of Termination.

(1) Except as provided in paragraph (2) of this subsection, upon termination of this Contract, for any reason, Associate shall return or destroy all Protected Information that Associate or its agents or Subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If Associate elects to destroy the PHI, Associate shall certify in writing to CE that such PHI has been destroyed.

(2) If Associate believes that returning or destroying the Protected Information is not feasible, Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. Associate shall continue to extend the protections of Sections 2(a), 2(b), 2(c), 2(d) and 2(e) of this Addendum to such Protected Information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

5. Injunctive Relief. CE shall have the right to injunctive and other equitable and legal relief against Associate or any of its Subcontractors or agents in the event of any use or disclosure of Protected Information in violation of this Contract or applicable law.

6. No Waiver of Immunity. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-101 *et seq.* or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.* as applicable, as now in effect or hereafter amended.

7. Limitation of Liability. Any limitation of Associate's liability in the Contract shall be inapplicable to the terms and conditions of this Addendum.

8. Disclaimer. CE makes no warranty or representation that compliance by Associate with this Contractor the HIPAA Rules will be adequate or satisfactory for Associate's own purposes. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

9. Certification. To the extent that CE determines an examination is necessary in order to comply with CE's legal obligations pursuant to the HIPAA Rules relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which Associate's security safeguards comply with the HIPAA Rules or this Addendum.

10. Amendment.

a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of the HIPAA Rules and other applicable laws relating to the confidentiality, integrity, availability and security of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected Information and that it is Associate's responsibility to receive satisfactory written assurances from Associate's Subcontractors and agents. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of the HIPAA Rules or other applicable laws. CE may terminate this Contract upon thirty (30) days written notice in the event (i) Associate does not promptly enter into negotiations to amend this Contract when requested by CE pursuant to this Section, or (ii) Associate does not enter into an amendment to this Contract providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Rules.

b. Amendment of Attachment A. Attachment A may be modified or amended by mutual agreement of the parties in writing from time to time without formal amendment of this Addendum.

11. Assistance in Litigation or Administrative Proceedings. Associate shall make itself, and any Subcontractors, employees or agents assisting Associate in the performance of its obligations under the Contract, available to CE, at no cost to CE up to a maximum of 30 hours, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of the HIPAA Rules or other laws relating to security and privacy or PHI, except where Associate or its Subcontractor, employee or agent is a named adverse party.

12. No Third Party Beneficiaries. Nothing express or implied in this Contract is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

13. Interpretation and Order of Precedence. The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. Together, the Contract and this Addendum shall be interpreted as broadly as necessary to implement and comply with the HIPAA Rules. The parties agree that any ambiguity in this Contract shall be resolved in favor of a meaning that complies and is consistent with the HIPAA Rules. This Contract supercedes and replaces any previous separately executed HIPAA addendum between the parties.

14. Survival of Certain Contract Terms. Notwithstanding anything herein to the contrary, Associate's obligations under Section 4(d) ("Effect of Termination") and Section 12 ("No Third Party Beneficiaries") shall survive termination of this Contract and shall be enforceable by CE as provided herein in the event of such failure to perform or comply by the Associate. This Addendum shall remain in effect during the term of the Contract including any extensions.

15. Representatives and Notice.

a. Representatives. For the purpose of the Contract, the individuals identified elsewhere in this Contract shall be the representatives of the respective parties. If no representatives are identified in the Contract, the individuals listed below are hereby designated as the parties' respective representatives for purposes of this Contract. Either party may from time to time designate in writing new or substitute representatives.

b. Notices. All required notices shall be in writing and shall be hand delivered or given by certified or registered mail to the representatives at the addresses set forth below.

Covered Entity Representative:

Name: _____
Title: _____
Department and Division: Broomfield Health and Human Services, Operations
Address: 100 Spader Way
Broomfield, CO 80020

Contractor/Business Associate Representative:

Name: _____
Title: _____
Address: _____
_____

ATTACHMENT A

This Attachment sets forth additional terms to the HIPAA Business Associate Addendum, which is part of the Contract dated _____, 20__ between the City and County of Broomfield and _____ and is effective as of _____, 20__ (the "Attachment Effective Date"). This Attachment may be amended from time to time as provided in Section 10(b) of the Addendum.

1. Additional Permitted Uses. In addition to those purposes set forth in Section 2(a) of the Addendum, Associate may use Protected Information as follows:
None except as otherwise directed in writing by the City and County of Broomfield and in accordance with 42 CFR part 11.

2. Additional Permitted Disclosures. In addition to those purposes set forth in Section 2(b) of the Addendum, Associate may disclose Protected Information as follows:
None except as otherwise directed in writing by the City and County of Broomfield and in accordance with 42 CFR part 11.

3. Subcontractor(s). The parties acknowledge that the following subcontractors or agents of Associate shall receive Protected Information in the course of assisting Associate in the performance of its obligations under this Contract:
None except as otherwise directed in writing by the City and County of Broomfield and in accordance with 42 CFR part 11.

4. Receipt. Associate's receipt of Protected Information pursuant to this Contract shall be deemed to occur as follows, and Associate's obligations under the Addendum shall commence with respect to such PHI upon such receipt:
Upon the effective date of the contract.

5. Additional Restrictions on Use of Data. CE is a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, Associate shall comply with the following restrictions on the use and disclosure of Protected Information:
As may be directed in writing by the City and County of Broomfield

6. Additional Terms. *[This section may include specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security of privacy specifications, de-identification or re-identification of data and other additional terms.]*
None

CITY AND COUNTY OF BROOMFIELD
One DesCombes Drive • Broomfield, CO 80020 • 303.469.3301 • www.broomfield.org

STATEMENT OF CONFIDENTIALITY

Employees, interns, and volunteers of the City and County of Broomfield (CCOB) often have access to clients and client information that is sensitive and confidential. Any client or other information shared and received during the course of assisting with CCOB business is NOT for dissemination to any other person or entity including coworkers who are not involved with the case. Confidentiality rules apply during and after your service with the CCOB.

Ordinances of the City and County of Broomfield and Titles 15, 19, 25, and 26 of the Colorado Review Statutes require all information relative to clients requesting information about potential services or receiving services remain confidential. State rules have been promulgated that restrict the use or disclosure of information as it relates to individual applicants or recipients of services. It is unlawful for any person to solicit, disclose, make use of, to authorize, knowingly permit, participate in, or acquiesce in the use of any lists, names, or individual information derived from this department. Information covered under this confidentiality provision includes:

1. Names and address of current or past applicants and recipients.
2. Services provided to any client or applicant.
3. Information related to the social, economic, or financial conditions or circumstances of any client or applicant.
4. Agency records or evaluation about clients or businesses.
5. Court records.
6. Foster care placement records.
7. Current or past medical, psychological, or social information including diagnosis relative to any client or applicant.
8. Any information or records related to the operation of the CCOB.

I have read and understand the above statement concerning confidentiality of information retained by the Broomfield Health and Human Services Department. Failure to comply with any portion of this confidentiality policy may be grounds for disciplinary action, including possible termination of employment. By signing below, I agree that I understand and consent to these requirements.

Employee Signature: _____ ***Date:*** _____

Employee Printed Name: _____

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.

YOUR RIGHTS

When it comes to your health information, you have certain rights.
This section explains your rights and some of our responsibilities to help you.

Contact for CCOB HIPAA related questions or complaints	• Risk Management 303.438.6286 riskmanagement@broomfield.org
Inspect or get an electronic or paper copy of your medical record	• You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this. • We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.
Ask us to correct your medical record	• You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this. • If we say "yes," we'll tell you that the correction was accepted and notify other relevant people, such as anyone you tell us needs the correction and others who have and may rely on the incorrect information. • We may say "no" to your request, but we'll tell you why in writing within 60 days.
Request confidential communications	• You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address. • You do not have to provide an explanation for the request. • We will say "yes" to all reasonable requests.

Ask us to limit what we use or share	• You can ask us **not** to use or share certain health information for treatment, payment, or our operations. • We are not required to agree to your request, and we may say "no" if it would affect your care. • If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. • We will say "yes" unless a law requires us to share that information.
Get a list of those with whom we've shared information	• You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, and the who, what, when, and why of the shared information. • Within 60 days, unless an extension is needed, we will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.
Get a copy of this privacy notice	• You can ask for a paper copy of this notice at any time. We will provide you with a paper copy promptly.
Choose someone to act for you	• If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. • We will make sure the person has this authority and can act for you before we take any action.
File a complaint if you feel your rights are violated	• You can complain if you feel we have violated your rights by contacting us using the information on page 1. • You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints** • We will not retaliate against you for filing a complaint.

YOUR CHOICES

For certain health information, you can tell us your choices about what we share.
If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Contact you for fundraising efforts

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we *never* share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

OUR USES AND DISCLOSURES

How do we typically use or share your health information?
We typically use or share your health information in the following ways.

Treat you	• We can use your health information and share it with other professionals who are treating you.	***Example:*** *A doctor treating you for an injury asks another doctor about your overall health condition.*
Run our organization	• We can use and share your health information to run our practice, improve your care, and contact you when necessary.	***Example:*** *We use health information about you to manage your treatment and services.*
Bill for your services	• We can use and share your health information to bill and get payment from health plans or other entities.	***Example:*** *We give information about you to your health insurance plan so it will pay for your services.*

How else can we use or share your health information? We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.**

Help with public health and safety issues	• We can share health information about you for certain situations such as: • Preventing disease • Helping with product recalls • Reporting adverse reactions to medications • Reporting suspected abuse, neglect, or domestic violence • Preventing or reducing a serious threat to anyone's health or safety
Do research	• We can use or share your information for health research.
Comply with the law	• We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.
Respond to organ and tissue donation requests	• We can share health information about you with organ procurement organizations.
Work with a medical examiner or funeral director	• We can share health information with a coroner, medical examiner, or funeral director when an individual dies.
Address workers' compensation, law enforcement, and other government requests	• We can use or share health information about you: • For workers' compensation claims • For law enforcement purposes or with a law enforcement official • With health oversight agencies for activities authorized by law • For special government functions such as military, national security, and presidential protective services
Respond to lawsuits and legal actions	• We can share health information about you in response to a court or administrative order, or in response to a subpoena.

OUR RESPONSIBILITIES

We are required by law to maintain the privacy and security of your protected health information.

- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

We reserve the right to change the terms of this notice and to make a new notice effective. If we do, you will be provided with the new notice via mail, email or in person notice.

I have read and agree to the Privacy Practice Rules and Regulations.
I can request a copy of the Privacy Practice Rules and Regulations at any time.

Receipt of Notice of Privacy Practices

Individual Name (Print): _____

Signature of individual or individual's Legal Representative: _____

Date: _____

Aviso de prácticas de privacidad

Este aviso describe cómo se puede usar y revelar su información médica y cómo puede obtener acceso a esta.
Léalo con atención.

SUS DERECHOS

Cuando se trata de su información médica, usted tiene ciertos derechos.
Esta sección le explica sus derechos y algunas de nuestras responsabilidades para ayudarlo.

Comuníquese si tiene alguna pregunta o queja relacionada con la HIPAA de la CCOB

- Gestión del riesgo
  303.438.6286
  riskmanagement@broomfield.org

Revisar o recibir una copia electrónica o impresa de su expediente médico

- Puede pedir ver o recibir una copia electrónica o impresa de su expediente médico y otra información médica que tengamos de usted. Pregúntenos cómo hacerlo.
- Le daremos una copia o un resumen de su información médica, en general en un plazo de 30 días desde su solicitud. Podemos cobrar un cargo razonable basado en los costos.

Pídanos corregir su expediente médico

- Puede pedirnos corregir su información médica si cree que es incorrecta o que está incompleta. Pregúntenos cómo hacerlo.
- Si decimos que “sí”, le diremos que aceptamos la corrección e informaremos a las personas correspondientes, como alguien que usted nos diga que necesita la corrección u otros que tengan o pueden basarse en la información incorrecta.
- Podemos decir que “no” a su solicitud, pero le informaremos el motivo por escrito en un plazo de 60 días.

Pida comunicaciones confidenciales

- Puede pedirnos que nos comuniquemos con usted de una manera específica (por ejemplo, al número de casa o trabajo) o enviar correo a una dirección diferente.
- No tiene que dar una explicación de la solicitud.
- Diremos que “sí” a todas las solicitudes razonables.

Pídanos que limitemos lo que usamos o compartimos

- Puede pedirnos **no** usar o compartir cierta información médica para un tratamiento, pago o para nuestras operaciones.
- No estamos obligados a aceptar su solicitud y podemos decirle que “no” si afecta su atención.
- Si paga de su bolsillo en su totalidad por un servicio o artículo para atención médica, puede solicitarnos que no compartamos esa información para efectos del pago o de nuestras operaciones con su compañía de seguro médico.
- Le diremos que “sí”, a menos que estemos obligados a compartir esa información por ley.

Obtenga una lista de las personas a las que compartimos información

- Puede pedir una lista (informe) de las veces que hemos compartido su información médica hasta seis años antes de la fecha de solicitud, y el quién, qué, cuándo y porqué de la información que se compartió.
- En un plazo de 60 días, a menos que se necesite una extensión, incluiremos todas las revelaciones, excepto las relacionadas con tratamientos, pagos y operaciones de atención médica, y otras revelaciones (como las que usted nos haya solicitado hacer). Daremos un informe por año gratis, pero si pide otro dentro de los 12 meses siguientes, cobraremos un cargo razonable basado en el costo.

Reciba una copia de este aviso de privacidad

- Puede pedir una copia impresa de este aviso en cualquier momento. Le daremos una copia impresa de inmediato.

Elija a alguien que lo represente

- Si le dio poder legal médico a alguien o si tiene un representante legal, esa persona puede ejercer sus derechos y tomar decisiones sobre su información médica.
- Nos aseguraremos de que la persona tenga esta autoridad y pueda decidir en nombre de usted antes de tomar cualquier acción.

Presente una queja si siente que se incumplieron sus derechos

- Puede quejarse si siente que faltamos a sus derechos comunicándose con nosotros usando la información de la página 1.
- Puede presentar una queja en la Oficina de Derechos Civiles del Departamento de Salud y Servicios Sociales de los EE. UU. (U.S. Department of Health and Human Services Office for Civil Rights) enviando una carta a 200 Independence Avenue, S.W., Washington, D.C. 20201, llamando al 1-877-696-6775 o visitando **www.hhs.gov/ocr/privacy/hipaa/complaints**
- No tomaremos represalias en su contra por presentar una queja.

SUS DECISIONES

Para cierta información médica, puede decirnos sus preferencias sobre qué compartimos.
Si tiene una preferencia clara de cómo compartimos su información en las situaciones que se describen abajo, contáctenos. Díganos lo que quiere que hagamos y seguiremos sus instrucciones.

En estos casos, tiene el derecho y puede elegir decirnos que:

- Compartamos información con su familia, amigos cercanos u otros que participan en su atención
- Compartamos información en una situación de ayuda en catástrofes
- Comunicarnos con usted para recaudación de fondos

Si no puede decirnos su preferencia, por ejemplo, si está inconsciente, podremos proceder a compartir su información si creemos que es para su beneficio. También podremos compartir su información cuando sea necesario para reducir el peligro grave e inminente para su salud o seguridad.

En estos casos, *nunca* compartimos su información, a menos que nos dé un permiso por escrito:

- Fines publicitarios
- Venta de su información
- La mayoría de intercambios de notas de psicoterapia

NUESTROS USOS Y REVELACIONES

¿Cómo usamos o compartimos normalmente su información médica?
Normalmente, usamos o compartimos su información médica de las siguientes formas.

Para tratarlo:	• Podemos usar su información médica y compartirla con otros profesionales que lo estén tratando.	***Ejemplo:*** *Un médico que lo trata por una lesión le pregunta a otro médico sobre su estado de salud general.*
Dirigimos nuestra organización	• Podemos usar y compartir su información médica para dirigir nuestra práctica, mejorar su atención y comunicarnos con usted cuando sea necesario.	***Ejemplo:*** *Usamos su información médica para gestionar su tratamiento y servicios.*
Cobrar sus servicios	• Podemos usar y compartir su información médica para facturar y recibir el pago de planes médicos u otras entidades.	***Ejemplo:*** *Damos información sobre usted a su plan de seguro médico para que este pague por sus servicios.*

¿De qué otra forma podemos usar o compartir su información médica? Se nos permite o exige compartir su información de otras formas, generalmente para contribuir al bien público, como la salud pública y la investigación. Debemos cumplir por ley con numerosas condiciones antes de poder compartir su información para estos fines. Para obtener más información visite: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.**

Colaboramos con asuntos de salud y seguridad públicas	• Podemos compartir su información médica para ciertas situaciones, como:
	  • Prevenir enfermedades
	  • Ayudar con retiros de productos
	  • Informar de reacciones adversas a medicamentos
	  • Informar de un presunto abuso, negligencia o violencia doméstica
	  • Prevenir o reducir una amenaza grave para la salud o la seguridad

Investigamos	• Podemos usar o compartir su información para investigaciones médicas.
Cumplimos con la ley	• Compartiremos información sobre usted si así lo exige la ley estatal o federal, incluyendo el Departamento de Salud y Servicios Humanos de los Estados Unidos (United States Department of Health and Human Services) si quiere ver que estamos cumpliendo con la ley de privacidad federal.
Respondemos a solicitudes de donación de órganos o tejidos	• Podemos compartir su información médica con organizaciones de obtención de órganos.
Trabajamos con un examinador médico o director de funeraria	• Podemos compartir información médica con un forense, examinador médico o director de funeraria cuando una persona muere.
Atendemos indemnización de trabajadores, de orden público y otras solicitudes del gobierno	• Podemos usar o compartir su información médica: • Para reclamos de indemnización de trabajadores • Para fines de orden público o con un oficial público • Con agencias de control de salud autorizados por la ley • Para funciones especiales del gobierno, como militar, seguridad nacional y servicios de protección presidencial
Responder a demandas y acciones legales	• Podemos compartir su información médica en respuesta a una orden judicial o administrativa, o en respuesta a una citación.

NUESTRAS RESPONSABILIDADES

La ley nos exige mantener la privacidad y seguridad de su información médica protegida.

- Le haremos saber inmediatamente si hay un incumplimiento que pudo afectar la privacidad y seguridad de su información.
- Debemos seguir las obligaciones y prácticas de privacidad que se describen en este aviso y darle una copia.
- No usaremos o compartiremos su información de una forma que no se describe aquí, a menos que usted nos diga lo contrario por escrito. Si nos dice que podemos, puede cambiar de opinión en cualquier momento. Díganos por escrito si cambia de opinión.

Nos reservamos el derecho de cambiar los términos de este aviso y hacer que un nuevo aviso entre en vigor. Si lo hacemos, recibirá el nuevo aviso por correo, correo electrónico o en persona.

Leí y acepto el Reglamento de prácticas de privacidad.
Puedo solicitar una copia del Reglamento de prácticas de privacidad en cualquier momento.

Recibo del Aviso de prácticas de privacidad

Nombre de la persona (letra de molde): _____

Firma de la persona o su representante legal: _____

Fecha: _____

Policy and Procedures for updated HIPAA Privacy Rights Request Form - updated March 2022

Purpose:

The HIPAA Privacy Rights Request Form allows individuals to formally request six specific actions as it relates to accessing, altering or restricting access to their Protected Health Information (PHI).

Policy:

HIPAA Privacy Rule specifies the rights of individuals in accessing, altering and restricting their PHI.

1. Right to Request Privacy Protection: Individuals have the right to request restrictions on how the City and County of Broomfield (CCOB) will use and disclose protected health information about them for treatment, payment, and health care operations (TPO). The CCOB is not required to agree to an individual's request for a restriction, but is bound by any restrictions to which it agrees. See 45 CFR 164.522(a) for further details.
2. Confidential Communication: Individuals also may request to receive confidential communications from the CCOB, either at alternative locations or by alternative means. For example, an individual may request that CCOB call her at her office, rather than her home. See 45 CFR 164.522(b).
3. Accounting of Disclosures: The CCOB shall make available to an individual upon request an accounting of certain disclosures of the individual's protected health information over the past six years. For each disclosure, the accounting must include: (1) The date of the disclosure; (2) the name (and address, if known) of the entity or person who received the protected health information; (3) a brief description of the information disclosed; and (4) a brief statement of the purpose of the disclosure (or a copy of the written request for the disclosure). See 45 CFR 164.528 for exceptions and details.
4. Restrict Access: The CCOB has the authority to release PHI for TPO. Any individual has the right to ask for that sharing of information be restricted. The CCOB is not required to agree to a restriction. If the CCOB does agree to a restriction, the CCOB may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment. The CCOB may use the restricted PHI itself or the CCOB may disclose such restricted PHI to a health care provider to provide such treatment to the individual. See 45 CFR. §164.522
5. Amendment of protected health information: An individual has the right to have CCOB amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set. 45 CFR. § 164.526
6. Complaint: Persons have a right to submit a complaint if they believe that the CCOB has improperly used or disclosed their protected information,or if they have concerns about the privacy policies of the City and County of Broomfield, Health and Human Services Department's compliance with such policies. Depending on the type of complaint, the Federal Office of Civil Rights (OCR) and/or CDHS will be notified of a complaint. The CCOB will proceed with OCR/CDHS and/or any other governing body in documenting and addressing the client's specific complaint. Governing bodies may include: HCPF, CDPHE, USDA, CDHS, OCR.

HIPAA Privacy Rights Request Form

Client Name: _____ Social Security: _____

Home Address: _____

_____

Home Phone: _____ Cell Phone:_____

Type of Request:

__ Access Health Information __ Accounting Disclosures __ Complaint

__ Confidential Communication __ Restriction Access __ Amendment of Information

Please describe the nature of action requested (type of information requested; nature of amendment, restriction, alternative communication, or complaint, etc.).

[Note: If this is an alternative communications request, please list alternative location/address for receiving personal health information below.]

_____

_____

_____

_____

_____

_____

_____

Client Signature: _____ Date: _____

_____

For CCOB Use Only. Date Received: _____

Action Taken:

_____

_____

Date Action Taken: _____ Staff: _____

Privacy Official signature: _____ Date: _____

[Attach additional documentation, if applicable.]

City and County of Broomfield
Request for an Accounting of Disclosures

Date of Request: _____

Client Name: _____ Date of Birth:_____

Client Address: _____

_____

Medical Record Number: _____

Send Information to This Address: _____

(If different from above) _____

Date Requested: *(Note: The maximum timeframe that can be requested is six years prior to the date of the request, but not before **April 14, 2003**.)*

I would like an accounting of all disclosures for the following timeframe beginning on _____ _

and ending on _____ . _____

Fee: There is a fee for this request. The fee is $1.00 per page of the accounting log that is copied.

The fee for the request on this date is: $_____

I understand that there will be a fee for today's request and wish to proceed. I also understand that the accounting will be provided to me within 72 hours unless I am notified in writing that an extension of up to 30 days is necessary.

_____ _____

Signature of Client or Legal Representative Date

For Department Use Only:
What did the client use to verify identity? _____
(Copy item and attach to this request.)

Date Received: _____ Date Sent: _____

Staff member processing this request:_____

Política y procedimientos para el Formulario actualizado de solicitud de derechos de privacidad de HIPAA (actualizado en marzo de 2022)

Propósito:

El formulario de solicitud de derechos de privacidad de HIPAA permite a las personas solicitar formalmente seis acciones específicas, que se relacionan con acceder, alterar o restringir el acceso a su Información médica protegida (Protected Health Information, PHI).

Política:

La Regla de privacidad de HIPAA especifica los derechos de las personas a acceder, alterar y restringir su PHI.

1. Derecho a solicitar protección de privacidad: Las personas tienen el derecho a solicitar restricciones en cómo la Ciudad y Condado de Broomfield (City and County of Broomfield, CCOB) usará y revelará la información médica protegida sobre ellos para tratamiento, pagos y operaciones de atención médica (TPO). No es necesario que la CCOB acepte la solicitud de restricción de una persona, pero debe cumplir las restricciones que sí aceptó. Consulte 45 CFR 164.522(a) para más información.
2. Comunicación confidencial: Las personas también pueden pedir recibir comunicaciones confidenciales de la CCOB, ya sea en lugares o medios alternativos. Por ejemplo, una persona puede pedir que la CCOB la llame a su trabajo en lugar de a su casa. Consulte 45 CFR 164.522(b).
3. Informe sobre las revelaciones: La CCOB pondrá a disposición, de la persona que lo pida, un informe sobre ciertas revelaciones de la información médica protegida de los últimos seis años. Para cada revelación, el informe debe incluir: (1) La fecha de la revelación; (2) el nombre (y dirección si se conoce) de la entidad o persona que recibió la información médica protegida; (3) una descripción breve de la información revelada; y (4) una declaración breve del propósito de la revelación (o una copia de la solicitud escrita de la revelación). Consulte 45 CFR 164.528 para ver las excepciones y más información.
4. Restringir el acceso: La CCOB tiene la autoridad de entregar la PHI para TPO. Cualquier persona tiene el derecho de pedir que se restrinja la información que se comparte. No es necesario que la CCOB acepte una restricción. Si la CCOB acepta una restricción, no podrá usar o revelar la PHI que infrinja esa restricción, excepto que la persona que la pidió necesite tratamiento de emergencia y se necesite la PHI restringida para dar servicios de emergencia. La CCOB puede usar la PHI restringida por su cuenta o puede revelar dicha PHI restringida a un proveedor de atención médica para dar dicho tratamiento a la persona. Consulte 45 CFR. §164.522
5. Modificación de la información médica protegida: Una persona tiene el derecho de que la CCOB modifique información médica protegida o el registro sobre la persona en un conjunto de registros designado durante el tiempo en que la información médica protegida esté en el conjunto de registros designado. 45 CFR. § 164.526
6. Reclamo: Las personas tienen el derecho de presentar una queja si creen que la CCOB usó o reveló su información protegida de forma indebida, o si tienen preocupaciones sobre las políticas de privacidad de la Ciudad y Condado de Broomfield, el cumplimiento de dichas políticas del Departamento de salud y servicios humanos (Health and Human Services Department). Según el tipo de queja, se notificará de este a la Oficina de Derechos Civiles (Office of Civil Rights, OCR) federal o a CDHS. La CCOB proseguirá con OCR/CDHS o con cualquier otra entidad del gobierno para documentar y tratar el reclamo específico del cliente. Las entidades del gobierno pueden incluir: HCPF, CDPHE, USDA, CDHS, OCR.

Formulario de solicitud de derechos de privacidad de HIPAA

Nombre del cliente: _____ Seguro Social: _____

Dirección de la casa: _____

_____

Teléfono de casa: _____ Teléfono celular: _____

Tipo de solicitud:

__ Acceso a información médica __ Lista de revelaciones __ Queja

__ Comunicación confidencial __ Restricción de acceso __ Modificación de información

Describa la naturaleza de la acción que solicita (tipo de información que solicita; naturaleza de la modificación, restricción, comunicación alternativa o queja, etc.).

[Nota: Si esta es una solicitud de comunicación alternativa, escriba abajo el lugar/dirección alternativa para recibir información médica personal.]

_____

_____

_____

_____

_____

_____

_____

Firma del cliente: _____ Fecha: _____

_____

Solo para uso de la CCOB. Fecha de recepción: _____
Acción tomada:

_____

Fecha de la acción tomada: _____ Personal: _____

Firma del oficial de privacidad: _____ Fecha: _____

[Adjunte documentación adicional, si corresponde.]

Ciudad y Condado de Broomfield
Solicitud de una Lista de revelaciones

Fecha de solicitud: _____

Nombre del cliente: _____ Fecha de nacimiento: _____

Dirección del cliente: _____

_____

Número de expediente médico: _____

Enviar información a esta dirección: _____

(Si es diferente a la de arriba) _____

Fecha de solicitud: *(Nota: El plazo máximo que se puede solicitar es de seis años previos a la fecha de la solicitud, pero no antes del **14 de abril de 2003)**.*

Me gustaría recibir una lista de todas las revelaciones en el plazo desde el _____

y hasta el _____

Cargo: Hay un cargo por esta solicitud. El cargo es de $1.00 por página del registro de la lista copiada.

El cargo por la solicitud de esta fecha es: $_____

Entiendo que habrá un cargo por la solicitud de hoy y quiero proceder. También entiendo que recibiré la lista en un plazo de 72 horas, a menos que se me notifique por escrito que es necesaria una extensión de hasta 30 días.

_____ _____

Firma del cliente o representante legal Fecha

Solo para uso del departamento:
¿Qué usó el cliente para verificar la identidad? _____
(Copie el artículo y adjúntelo a esta solicitud).

Fecha de recepción: _____ Fecha de envío: _____

Miembro del personal que procesa esta solicitud: _____

CITY AND COUNTY OF BROOMFIELD
One DesCombes Drive • Broomfield, CO 80020 • 303.469.3301 • www.broomfield.org

Request to Amend or Correct Protected Health Information

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), you have a right to request that the City and County of Broomfield (CCOB) change or amend protected health information (PHI) about you that CCOB maintains in a client/resident file. PHI includes enrollment information, benefit payments, case or medical records, appeals and/or complaint files, and other records that are used in whole or in part to make decisions about your case.

Use this form to request that CCOB change or correct information we have about you that you believe is incomplete or inaccurate. For example, information is incorrectly stated in case file notes or there is an incorrect diagnosis in your record.

CCOB may deny your amendment request if the PHI that is the subject of the request:

1. Was not created by CCOB;
2. Is not part of the CCOB client/resident file;
3. Would not be available for inspection (including, but not limited to, exempt items and situations in which the PHI at issue is no longer maintained in the client/resident file); or
4. Is accurate and complete.

When completing this form, please:

- Complete all sections entirely;
- Print information clearly;
- Provide us with your most current information

You can only request to correct or amend your own PHI, unless you are authorized to amend information about someone else. We will respond to requests from a personal representative authorized by a member to receive his or her PHI (e.g., parent, court appointed representative, family member). However, we may ask for more information from you or your authorized representative to verify the right to act on your behalf.

Please note: If you are a guardian or court appointed representative for the individual, you must attach copies of your authorization to represent the individual in order to obtain access to his/her Protected Health Information.

Additionally, we will amend only PHI relating to benefits and services provided by CCOB. To correct or amend PHI concerning other benefits and programs not managed by CCOB, you must contact the entity that administers those benefits directly.

We will respond to your request for an amendment of PHI or provide a status update within 60 days from the date we receive your request.

If you have questions about this form, please contact the CCOB Primary HIPAA Privacy Officer, at (303) 438-6286 or riskmanagement@broomfield.org.

Request to Amend or Correct Protected Health Information

This form is used to request an amendment to Protected Health Information contained in a client/resident file that has been maintained by the City and County of Broomfield (CCOB). To amend PHI concerning benefits or programs not managed by CCOB you must contact the entity that administers those benefits directly. Once the decision to grant or deny your request has been made, a letter explaining our decision will be mailed to you or your authorized personal representative. Please print. Be sure to complete both pages of this form.

Section 1: Amendment of Protected Health Information Requested For:

Name _____ Address _____

City _____ State ____ Zip _____Phone (_____)-_____

Date of Birth _____ Male ___ Female ____

Relationship to Client/Resident: Self ____ Spouse ____ Child____ If other, describe type of relationship
_____

Section 2: Amendment Requested:

Please indicate the Protected Health Information that you believe is inaccurate and/or incomplete and describe the error. Please attach a copy of the information you would like amended.

_____

_____

_____

If you know that someone else has this information and should be notified if we make an amendment, please list them below:

Name	Address	Relationship (e.g. Provider, plan sponsor, etc.)

Section 3: Signature of Member or His/Her Personal Representative:

Authorized Signature of individual or personal representative of individual, for whom the amendment is being requested:

I authorize the amendment of the indicated Protected Health Information to be sent to me; to others as directed in a signed authorization; or to others legally authorized to act on my behalf, at the address stated in Section 1 of this form. Denial of Request: I understand and acknowledge that CCOB IS UNDER NO OBLIGATION TO AGREE TO THIS REQUEST FOR AMENDMENT OF MY PHI, under the following conditions:

1. **the information is not part of my client/resident file (unless I provide a reasonable belief that the originator of my PHI is no longer available to act on this requested amendment);**
2. **the information is not accessible to me; and**
3. **the information is accurate and complete.**

Rev (04/2021)

I further understand and acknowledge MY REQUEST FOR AN AMENDMENT MAY BE DECLINED IF:

1. **the request is not reasonable;**
2. **the information I provide is not accurate;**
3. **this form is not completed in its entirety; and/or**
4. **I do not sign below.**

If CCOB denies this request, it will provide me with the following:

1. **a written explanation of the reason(s) for denial;**
2. **my right to submit and file a written statement disagreeing with the denial or a request by me that CCOB provide my request and denial of the amendment with any future disclosures of my PHI that is the subject of amendment; and**
3. **whether I have a right to further review.**

Rights and Acknowledgement. With certain exceptions, I have the right to have my client/resident file amended. By signing below, I
hereby authorize my records to be amended as described on this form. I understand and acknowledge that CCOB will have up to sixty (60) days after receiving this request to act on it, and that in certain circumstances, CCOB may be permitted a one (1)-time thirty (30)-day extension. If CCOB accepts this request, it will abide by the amendment from the date upon which CCOB approves the request and CCOB will make reasonable efforts to inform others of the amendment, including individuals and/or entities I name. I understand and acknowledge this request shall not apply to information that has already been released or affect actions taken by CCOB prior to this request. I further understand and acknowledge that CCOB is not responsible for any action taken by any authorized recipient and/or disclosure of the information released pursuant to any signed authorization to use and/or disclose my PHI. The information described on this form is protected by law and shall only be amended as indicated above, unless otherwise required and/or permitted by law.

Signature of Individual: X _____ Date _____

If you are signing as a personal representative, complete the section below. A parent/legal guardian must sign below for a minor under the age of eighteen (18). You may be required to provide additional documentation to show that you have a legal right to request the information, unless you have a Designation of Personal Representative signed by the Member naming you as personal representative. Examples of these documents include Letters of Representation or Guardianship Papers.

Signature of Personal Representative, if applicable: X _____ Date _____

Representative's Name _____ Address _____

City_____ State ____ Zip _____ Phone (_____)_____

Relationship to individual and authority to act for individual:_____

Important: A personal representative, including a parent, legal guardian, or executor of an estate, may be required to attach a copy of legal documentation to this request form.

Please return the completed form to:

- Fax: (303) 438-6328

Or

- Mail to: City and County of Broomfield Primary HIPAA Privacy Officer
  1 DesCombes Drive
  Broomfield, CO 80020

If you have any questions, please contact the CCOB Primary HIPAA Privacy Officer at (303) 438-6286.

Rev (04/2021)

TO BE COMPLETED BY CCOB

_ Request is Approved. Effective Date: _____

_ Request is Denied. Reason: _____

_ Additional Comments: _____

CCOB Representative Signature: _____

Rev (04/2021)

CITY AND COUNTY OF BROOMFIELD
One DesCombes Drive • Broomfield, CO 80020 • 303.469.3301 • www.broomfield.org

Solicitud para modificar o corregir la información médica protegida

Según la Ley de Portabilidad y responsabilidad del seguro médico (Health Insurance Portability and Accountability Act, HIPAA) de 1996, usted tiene derecho a solicitar que la Ciudad y Condado de Broomfield (City and County of Broomfield, CCOB) cambie o modifique información médica protegida (protected health information, PHI) sobre usted que la CCOB tenga en un archivo de cliente/residente. PHI incluye información de inscripción, pagos de beneficios, registros médicos o de su caso, archivos de apelaciones o reclamos y otros registros que se usaron por completo o en parte para tomar decisiones sobre su caso.

Use este formulario para solicitar que la CCOB cambie o corrija información que tenemos sobre usted que crea incompleta o imprecisa. Por ejemplo, información descrita de forma incorrecta en las notas del caso archivado o si hay un diagnóstico incorrecto en su registro.

La CCOB puede rechazar su solicitud de modificación si la PHI que es el objeto de la solicitud:

1. No la creó la CCOB;
2. No forma parte del archivo del cliente/residente de la CCOB;
3. No está disponible para la inspección (incluyendo, artículos y situaciones exentas en las que la PHI en cuestión ya no está en el archivo del cliente/residente); o
4. Es precisa y completa.

Cuando complete este formulario:

- Complete todas las secciones;
- Escriba de forma clara; y
- Denos su información más actual.

Solo puede solicitar corregir o modificar su propia PHI, a menos que tenga autorización para modificar la información de alguien más. Responderemos a las solicitudes hechas por un representante personal autorizado por un miembro para recibir su PHI (p.ej., padre, representante designado por el tribunal o familiar). Sin embargo, podemos pedirle más información a usted o su representante autorizado para verificar el derecho de actuar en su nombre.

Tenga en cuenta: Si usted es un tutor o representante designado de la persona por un tribunal, debe adjuntar copias de su autorización para representar a la persona y tener acceso a su Información médica protegida.

Además, modificaremos solo la PHI relacionada con los beneficios y servicios que presta la CCOB. Para corregir o modificar la PHI en relación a otros beneficios y programas que no administra la CCOB, debe comunicarse directamente con la entidad que administra esos beneficios.

Responderemos a su solicitud de modificación de la PHI o presentaremos una actualización de estado en un plazo de 60 días desde la fecha en que recibamos su solicitud.

Si tiene alguna pregunta sobre este formulario, comuníquese con el responsable primario de privacidad de HIPAA, al (303) 438-6357 o visite riskmanagement@broomfield.org.

Solicitud para modificar o corregir la información médica protegida

Este formulario se usa para solicitar una modificación de la Información médica protegida de un archivo de cliente/residente que tenga la Ciudad y Condado de Broomfield (CCOB). Para modificar la PHI en relación a otros beneficios o programas que no administra la CCOB, debe comunicarse directamente con la entidad que administra esos beneficios. Una vez que se tome la decisión de aceptar o rechazar su solicitud, se le enviará por correo a usted o su representante personal autorizado una carta explicando nuestra decisión. Escriba y asegúrese de completar ambas páginas de este formulario.

Sección 1: Enmienda de Información médica protegida solicitada:

Nombre _____ Dirección _____

Ciudad _____ Estado _____ Código postal _____Teléfono (_____)-_____

Fecha de nacimiento _____ Masculino ____ Femenino ____

Relación con el cliente/residente: Yo _____ Cónyuge _____ Hijo____ Otra, describa el tipo de relación
_____

Sección 2: Modificación solicitada:

Indique la Información médica protegida que crea que es imprecisa o incompleta y describa el error. Adjunte una copia de la información que quiera modificar.

_____

_____

_____

Si sabe que alguien más tiene esta información y se le debe notificar si hacemos una modificación, nombrarlos abajo:

Nombre	Dirección:	Relación (p.ej., proveedor, patrocinador del plan, etc.)

Sección 3: Firma del Miembro o su Representante personal:

Firma autorizada de la persona o su representante personal, para quien se solicita la modificación:

Autorizo que me envíen la modificación de la Información médica protegida indicada; a otros como se indica en la autorización con firma; o a otros legalmente autorizados para actuar en mi nombre, a la dirección que se indica en la Sección 1 de este formulario.
Rechazo de la solicitud: Entiendo y reconozco que la CCOB NO TIENE NINGUNA OBLIGACIÓN DE ACEPTAR ESTA SOLICITUD DE MODIFICACIÓN DE MI PHI, bajo las siguientes condiciones:

1. **la información no es parte del archivo de mi cliente/residente (a menos que haya una creencia razonable de que el emisor de mi PHI ya no está disponible para responder a esta solicitud de modificación);**
2. **la información no es accesible para mí; y**
3. **la información es precisa y completa.**

Rev (04/2021)

También entiendo y reconozco que MI SOLICITUD DE MODIFICACIÓN PUEDE RECHAZARSE SI:

1. **la solicitud no es razonable;**
2. **la información que doy no es precisa;**
3. **el formulario no se completó totalmente; o**
4. **no firmo abajo.**

Si la CCOB rechaza esta solicitud, me dará lo siguiente:

1. **una explicación escrita con la razón del rechazo;**
2. **mi derecho a enviar y presentar una declaración escrita en desacuerdo con el rechazo o una solicitud de mi parte para que la CCOB proporcione una copia de mi solicitud y rechazo de la modificación con cualquier declaración futura de mi PHI que es sujeto de modificación; y**
3. **si tengo derecho a una revisión adicional.**

Derechos y Aceptación. Tengo el derecho de modificar mi archivo de cliente/residente, con ciertas excepciones. Firmando abajo, yo
autorizo por medio de la presente que mis registros se modifiquen como se describe en este formulario. Entiendo y reconozco que la CCOB tendrá hasta sesenta (60) días después de recibir esta solicitud para tomar una decisión, y que en ciertas circunstancias, se permitirá que la CCOB tenga una extensión de treinta (30) días. Si la CCOB acepta esta solicitud, respetará la modificación desde la fecha en la que apruebe la solicitud y hará esfuerzos razonables para informar a otros de la modificación, incluyendo personas o entidades que yo mencioné. Entiendo y reconozco que esta solicitud no aplicará a información que ya se entregó ni afectará las acciones que la CCOB tomó antes de esta solicitud. También entiendo y reconozco que la CCOB no es responsable de ninguna acción que tome un beneficiario autorizado o revelación de la información entregada de acuerdo a cualquier autorización firmada para usar o revelar mi PHI. La información descrita en este formulario está protegida por la ley y sólo debe modificarse como se indica arriba, a menos que la ley exija o permita lo contrario.

Firma de la persona: X _____ Fecha _____

Si firma como representante personal, complete la sección de abajo. Un padre, madre o tutor legal debe firmar abajo en nombre de una persona menor de dieciocho (18) años. Se le puede exigir que proporcione documentación adicional para demostrar que tiene derecho legal de solicitar la información, a menos que tenga una designación de un representante personal con firma del Miembro que lo nombra representante personal. Ejemplos de estos documentos incluyen Cartas de representación o Documentos de tutela.

Firma del Representante personal, si corresponde: X _____ Fecha _____

Nombre del representante _____ Dirección _____

Ciudad_____ Estado _____ Código postal _____Teléfono (_____)_____

Relación con la persona y autoridad para actuar por la persona:_____

Importante: Se puede exigir que un representante personal, incluyendo padre, madre, tutor legal o ejecutor de un patrimonio, adjunte una copia de documentación legal a este formulario de solicitud.

Por favor enviar el formulario completo a:

- Fax: (303) 438-6328

O

- Correo: City and County of Broomfield Primary HIPAA Privacy Officer
  1 DesCombes Drive
  Broomfield, CO 80020

Si tiene alguna pregunta, comuníquese con el responsable primario de privacidad de HIPAA, al (303) 438-6357.

Rev (04/2021)

LA CCOB DEBE COMPLETAR ESTA SECCIÓN

_ Solicitud aprobada. Fecha que entra en vigencia: _____

_ Solicitud rechazada. Motivo: _____

_ Comentarios adicionales: _____

Firma del representante de CCOB: _____

Rev (04/2021)

Attachment 1

HIPAA Component
Human Resources

Technical Safeguards: Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and controls access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate access to ePHI.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.
Reference: 45 CFR 164.310, 312, and 316.

Public Health Information (PHI) Maintained or Accessed by Workforce Members:

- Leave and benefits administration
- Vendors Include
    - HUB International - Insurance Broker
    - UMR (United Healthcare)
    - Kaiser Permanente
    - Delta Dental of Colorado
    - Vision Service Plan (VSP)
    - Alerus Financial
    - Pinnacol Assurance
    - Empower Retirement
    - Mission Square Retirement

    - Fire & Police Pension Association of Colorado (FPPA)
- Hard copies of documents
    - All are locked in file cabinets with only HR staff access
- Electronic
    - All files are shared via Secure File Sharing or SFTP

Workforce Access to PHI

Policy: Access to applications that contain PHI shall be granted to members of the CCOB Workforce only on a need-to-know basis and in compliance with the Minimum Necessary Policy. Role Based Access shall be established for each member of the CCOB Workforce, modified upon that person's change in job functions, and terminated at the end of that person's employment or contract.

Procedure for Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to data access that are unique to the component, including access to any State, Federal, or third-party systems required by the component, are as follows:

- Individuals with access to PHI: all Human Resources staff
- On-going professional development
- HR/Legal Updates regarding HIPAA compliance for HR Professionals

Safeguards include:

- All access to PHI is password protected per individual login
    - Hard copies of documents
        - All are locked in file cabinets with only HR staff access
    - Electronic
        - Google drive files are limited to HR personnel -- all required to take annual HIPAA training
    - Virtue Secure to email secure documents

Procedure for Terminating Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, are as follows:

- Access is removed by appropriate parties upon separation

Component Specific HIPAA Training Materials:

- Standard City and County of Broomfield HIPAA Compliance Training

Attachment 2

HIPAA Component
Human Services

Technical Safeguards: Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and controls access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate access to ePHI.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.
Reference: 45 CFR 164.310, 312, and 316.

Protected Health Information (PHI) Maintained or Accessed by Workforce Members:

- **Long Term Care Case Files:** In cases where a disability application has been filed, we send the application to ARG to process the disability determination. ARG reviews/determines any disability and provides us with the disability determination information, allowing us to complete the eligibility determination process. Files and documents are scanned into the HSConnects system which is secured by network login requirements and user profiles maintained by the IT and the CCOB Business Solutions & Systems Administrator. Closed case files prior to the HSConnects implementation on November 19, 2018 are kept in the file cabinets in the Self-Sufficiency unit and are scanned into a secured location in Phoenix.
- **Child Welfare Case Files:** Cases are documented in the statewide automated child welfare information system (SACWIS), also known as Trails. Closed case files are kept in locked file cabinets in the Children, Adult, and Family Services unit. Files are

destroyed upon their retention schedule. Active assessment and case files are kept in locked filing cabinets near the caseworkers' desks for access. Caseworkers return files to the locked cabinets when not in use. The CAFS administrative assistant monitors all files for compliance with the aforementioned retention schedule as part of their job duties.

Note: The City and County of Broomfield public assistance programs and Medicaid program, within the Department of Human Services are excluded as health plans, since these are government funded programs not specifically cited under HIPAA as covered entities.

Procedure for Terminating Access for CCOB Employees:

In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, are as follows:

1. CCOB Business Solutions & Systems Administrator will terminate any accounts with state or federal databases using the appropriate forms.
2. CCOB Business Solutions & Systems Administrator will retain documentation of termination documents in the file and retain for six (6) years for auditing purposes.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.310, 312, and 316.

Component Specific HIPAA Training Materials

- Human Services employees with access to PHI take the CCOB HIPAA training on an annual basis

Attachment 3

HIPAA Component
Information Technology

Technical Safeguards: Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and control access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency. At the request of a Department Head or other designated owner of the system, IT (or Taryn Davids for state systems) would grant access on a temporary basis.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate access to ePHI.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy or the Personally Identifiable Information Policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.
Reference: 45 CFR 164.310, 312, and 316.

Public Health Information (PHI) Maintained or Accessed by Workforce Members:

- As administrators, IT personnel may have access to any and all Public Health Information Maintained or Accessed by CCOB Employees.

Workforce Access to PHI

Policy: Access to applications that contain PHI shall be granted to members of the CCOB Workforce only on a need-to-know basis and in compliance with the Minimum Necessary Policy. Role-Based Access shall be established for each member of the CCOB Workforce, modified upon that person's change in job functions, and terminated at the end of that person's employment or contract.

- Administrator access is assigned to IT personnel as follows:

- Domain Admin accounts - All members of the DevOps, GIS, and IT Leadership Teams (except for Business Administrative Staff) are assigned separate Administrator accounts, separate from their regular accounts, with which to perform Administrator duties. Domain Admins have access to all on-premise Windows domain servers and workstations, and all data on those computers.
- Google Admin accounts - All members of the IT Department (except for Business Administrative Staff) have Google Administrator accounts. Google Admin accounts do not have access to any data by default, unless data is shared specifically to each account.
- System specific Admin accounts - Cloud based systems, such as Boris, have system specific administrator accounts created for only those IT Employees who actively administer the system.
- Administrative service accounts - Administrative service accounts may exist for various systems, and IT employees may have access to the credentials of such service accounts in order to perform administrative duties when the primary administrative staff is unavailable, such as in on-call or after-hours situations.
- In addition, all members of the IT Department may have access to PHI when supporting an end-user's computer, whether via remote control software, actively working on an end-user's computer, or when standing behind or in proximity to a user while performing standard computer application troubleshooting. If possible, end users are requested to close any windows that may contain PHI when the IT Department is supporting an end user's computer.

Procedure for Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to data access that are unique to the component, including access to any State, Federal, or third-party systems required by the component, are as follows:

- Per the New User SOP, Administrators are granted access via dedicated Administrator accounts or via shared service accounts. Access is granted only to Administrators needing access to specific systems through the use of Security Groups, or by only creating Administrator accounts on the systems to which the employee needs access.

Procedure for Terminating Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, are as follows:

- Per the Departing User SOP, Dedicated Administrator accounts are disabled within 24 hours of separation. External access to the CCOB network is also disabled within 24 hours of separation.

Component Specific HIPAA Training Materials:

- All IT employees will be required to take an annual, organizational HIPAA training.

Attachment 4

HIPAA Component
Police Department - Detention Inmate Health Services

Technical Safeguards: Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and controls access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate access to ePHI.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.
Reference: 45 CFR 164.310, 312, and 316.

Public Health Information (PHI) Maintained or Accessed by Workforce Members:

- The Detention Center adheres to all relevant HHS requirements including (45 CFR 164.512(k)(5)) as an "excepted" facility.
- The Detention Center does not maintain any specific medical information in the Jail Management Software system beyond what is necessary for the administration and maintenance of the safety, security, and good order of the correctional facility.
- All contracted vendors to include but not limited to inmate health care, mental health care, dental care and discharge services are required to sign and fully execute a "business associate agreement" as clarified under 45 CFR 160.103.
- All physical copies of protected information to include but not limited to inmate files, medical requests, "sick call" forms and referral documents will be stored in the approved vendor file system. Files are in a locked room that requires a key card for access. Files and documents will not be left unattended and will not be removed

from the health care office without express permission from the Health Services Administrator.
- Protected health information files and documents will not be released without authorization from the inmate, BPDC and the vendor.
- Above referenced forms are scanned and uploaded into the vendor's electronic file system.

Workforce Access to PHI

Policy: Access to applications that contain PHI shall be granted to members of the CCOB Workforce only on a need-to-know basis and in compliance with the Minimum Necessary Policy. Role Based Access shall be established for each member of the CCOB Workforce, modified upon that person's change in job functions, and terminated at the end of that person's employment or contract.

Procedure for Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to data access that are unique to the component, including access to any State, Federal, or third-party systems required by the component, are as follows:

- With the exception of basic information permitted to be collected as an excepted facility, sworn staff or other PD personnel do not have access to the collected medical information. CCOB key cards allow PD personnel to enter the medical area but a physical key is required to access the medical records room. Only the medical providers have access to the records room.

Procedure for Terminating Access for CCOB Employees: In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, are as follows:

- The PD/Detention HIPAA Component uses the standard CCOB process for terminating employee access to information systems, as described in the HIPAA Compliance Plan Policies and Procedures.
- Detention staff do not have electronic and/or network access to any protected information. All inmate and arrestee protected information is contained within an approved vendor software system that is not on any CCOB network.
- Any approved vendor who provides services to the inmates as approved by the CCOB, will ensure that software and network access is terminated upon employee separation.

Component Specific HIPAA Training Materials:

- The PD/Detention HIPAA Component employees who are briefed on specific higher risk cases requiring greater detail may occasionally have knowledge of PHI. These individuals are required to take the standard CCOB organizational HIPAA training; recognizing established HIPAA exceptions and previously litigated case law specific to

correctional facilities. This includes the Detention Center's Multi-Disciplinary Review Team consisting of Medical, Mental Health, Security, Classification and Programming staff.

Attachment 5

HIPAA Component
Public Health and Environment

Technical Safeguards: Technical safeguards means the technology and the policies and procedures for its use that protect ePHI and controls access to it. Each CCOB healthcare component will develop and implement technical safeguards appropriate to its environment, including but not limited to the following:

- Access Control/Unique User Identification: Designed to allow access to only appropriate personnel or software programs that have been granted access rights. User identification requires that unique names and/or numbers for identifying and tracking users' identities be maintained.
- Emergency Access Procedures: Required for obtaining necessary electronic PHI during an emergency.
- Transmission Security and Encryption: Where appropriate, such controls should be utilized.
- Audit Controls: Includes hardware, software and procedural mechanisms that examine activity of IT systems that contain PHI.

Each CCOB Health Care Component will implement policies and procedures to ensure that workforce members who need access to ePHI are categorized based upon their roles and responsibilities or are otherwise identified. Procedures will be established to allow access among appropriate workforce members and to prevent those workforce members who do not have access from obtaining inappropriate access to ePHI.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.
Reference: 45 CFR 164.310, 312, and 316.

Public Health Protected Health Information (PHI) Maintained or Accessed by Workforce Members:

- **Reproductive Health Clinic Medical Records:** paper files kept for the current year. All previous years' records have been scanned and uploaded to a secure location in Phoenix. Once scanned, these files are securely shredded in the locked shred bins. Beginning in 2022, Reproductive Health Clinic medical records will be stored on the Athena Health Electronic Medical Record platform, which is HIPAA compliant.
- **Immunization Clinic Medical Records:** Immunization documentation and reporting is conducted in the state's electronic reporting system called CIIS maintained by Colorado Department of Public Health and Environment (CDPHE). Paper copies of client billing sheets and clinic visit records are filed in a secured filing cabinet in the immunization clinic locked offices, which is considered PHI. However, the information passed along to the State is not considered PHI.
- **Epidemiology Communicable Disease Contact Tracing Documentation:** Reporting of contact tracing and disease reporting is done in the state's electronic system called

CEDRS maintained by CDPHE. The Epi team also uses secured Google Sheets located in a Public Health folder on the CCOB Google Drive with access restricted only to the contact tracing team.

- **COVID-19 Community Testing Site Test Results:** Digital registration forms completed in a Google Form that feeds into a Google Sheet. The Google Form and Google Sheet are both located in a Public Health folder on the CCOB Google Drive with access restricted only to the COVID-19 testing team. Results are automatically emailed to the patient from the Google Sheet using Virtru email encryption. The paper copies of the test results registration forms are scanned into a secure location in Phoenix. Once scanned, these forms are securely shredded in the locked shred bins.
- **COVID-19 Vaccine Clinic Records:** Secured Google sheets for the appointment lists for COVID-19 vaccine clinics are located in a Public Health folder on the CCOB Google Drive with access restricted only to the vaccine clinic team members.
- **Resource Navigation and Referral Documentation:** Referrals to community based organizations for resource needs (ex. Food, housing, mental health services) are sent through the electronic platform, UniteUs. The contact tracing and resource navigation team also use a secured Google Sheet for COVID-19 resource referral tracking located in a Public Health folder on the CCOB Google Drive with access restricted only to these teams. UniteUs is HIPAA compliant. Reproductive Health clinic does send some referrals which would be the client name and show they are a patient of the CCOB reproductive health clinic.
- **Family Beginnings Nurse Visitation Program Documentation:** Paper files are secured in a locked file cabinet. Electronic program documentation uses a Google Sheet located in a Public Health folder on the CCOB Google Drive with access restricted to program staff.
- **HCP for Children with Special Health Care Needs Program Documentation:** Paper charts are stored in locked filing cabinets in a locked clinic office. Electronic charting is done in the state's electronic system called CDS maintained by CDPHE.

Procedure for Terminating Access for CCOB Employees:

In addition to the procedure listed in the HIPAA Compliance Plan, operating procedures relating to PHI data access that are unique to the component, such as terminating access to State, Federal, and third-party systems administered by the component, are as follows:

1. CCOB Business Solutions & Systems Administrator will terminate any accounts with state or federal databases using the appropriate forms.
2. CCOB Business Solutions & Systems Administrator will retain documentation of termination documents in the file and retain for six (6) years for auditing purposes.

Enforcement: All CCOB workforce members are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for staff, interns, or volunteers as delineated in the Human Resources Personnel Merit Policy.

Reference: 45 CFR 164.310, 312, and 316.

Attachment 5

Component Specific HIPAA Training Materials

- Public Health employees with access to PHI take the CCOB HIPAA training on an annual basis