Denver Regional Council of Governments

HIPAA Policy and Procedure Manual

Date Created:	01/16/2018	**Category:**	Procedure
Revision:	1.01	**Last Modified:**	08/10/2023
Author:	Tim Feld IT Manager	**Modified by:**	Tim Feld IT Manager

Table of Contents

Index of Forms

1.0 General Policy Statement

Denver Regional Council of Governments (DRCOG) is committed to protecting the privacy, security, confidentiality, integrity, and availability of individually identifiable Protected Health Information (PHI) in compliance with the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) and the regulations described there under. These policies and procedures apply PHI created, acquired, maintained, or disclosed by DRCOG employees and Business Associates. All individuals/agencies conducting business on behalf of DRCOG will take responsibility for safeguarding PHI to which they have access.

The U.S. Department of Health and Human Services (DHHS) published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

DHHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI). Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006, for small health plans).

In 2018, the Colorado General Assembly approved House Bill 1128 (codified at C.R.S. §§ 24-73-101 to 103) concerning protections for personal information (PI) and notifications upon a discovery of a breach.

For purposes of brevity and readability, the term "*applicant*" and "*client*" is synonymous with the phrase "*person applying for services, the parent of a minor, legal guardian, or personal representative."*

For purposes of brevity and readability, the term "*employee(s)*" is synonymous with the phrase "*employee(s), subcontractor(s), intern(s), vendor(s), and volunteer(s).*"

1.1 Minimum Necessary

The Privacy Rule introduces the concept of "*minimum necessary*". This requirement mandates that when using or disclosing PHI, or when requesting PHI from external providers or entities, providers will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule does recognize that providers may need to use all an individual's health information in the provision of the client's care. However, access to PHI by the employee must be limited based on job scope and the need for the information.

1.2 Enforcement

Any employee found to have violated these HIPAA policies may be subject to disciplinary action in accordance with applicable policies and procedures, up to and including termination of employment. Any vendor, subcontractor, or affiliate found to have violated these HIPAA policies may be subject to disciplinary action, up to and including termination of contract or affiliation. Additional civil and/or criminal punishments may be applicable.

2.0 HIPAA Compliance Coordinator - Policy

DRCOG policy complies with HIPAA, as well as requirements of the *Health Information Technology for Economic and Clinical Health Act* (HITECH), which was enacted as part of the *American Recovery and Reinvestment Act of 2009* (ARRA) and C.R.S. §§ 24-73-101 to 103. The confidentiality of PHI is maintained and safeguarded for individuals applying for, or receiving, services.

PHI is any health information collected from an individual, transmitted, or maintained in any form or medium that:

- Is created or received by DRCOG, a healthcare provider, health plan employer or healthcare clearing house
- Relates to the past, present, or future physical or mental health or condition of an individual or the provision of healthcare to an individual, and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual

This definition is a general definition and is not intended to change the definition of PHI under the Privacy Rule.

These policies outline HIPAA rules and regulations regarding the rights of persons applying for or receiving services, including their rights to notification and due process. The parent of a minor, acting on behalf of their child under the age of 18 years, is also accorded the same rights. Legal guardians and personal representatives may also be accorded the same rights if a court has awarded them the right to access or release the PHI of a person applying for or receiving services.

As changes occur in the law, including standards, implementation, specifications, or other requirements of the HIPAA regulations, DRCOG will change its privacy and security policies and procedures as necessary and appropriate.

These policies are to be interpreted and construed consistent with the requirements of HIPAA, its regulations, and any more stringent State law. In the event of any conflict between a provision of these policies and more stringent State laws or requirements, the more stringent law or requirement will prevail.

2.1 Identification of HIPAA Privacy Official - Procedure

DRCOG has appointed a HIPAA Compliance Coordinator who functions as the HIPAA Privacy Official. The Director of Administration and Finance serves as the backup to the Compliance Coordinator. The responsibilities of the HIPAA Privacy Official are as follows:

- Oversees the development, implementation, maintenance and revision of policies and procedures to protect confidential health information in accordance with Federal and State regulations. The HIPAA Compliance Coordinator notifies the management team of any policies, procedures, or implementation issues that need their review
- Performs regular Privacy Rule focused risk assessments to identify issues that need attention
- Develops employee training on HIPAA policies, procedures, and practices
- Ensures all affected employees receive HIPAA training
- Maintains updated Notice of Privacy Practices that is distributed in accordance with these procedures
- Manages any disclosures of information, including the preparation and maintenance of mandatory reporting
- Provides notifications to affected individuals, as well as any local, state or federal authorities, including notification of any PHI data breach to the Colorado Attorney General's Office when 500 or more Colorado residents are impacted
- Responds to requests for Amendments of PHI
- Investigates and responds to complaints regarding the confidentiality of information
- Updates privacy forms and coordinates the placement of these forms on the DRCOG intranet and notifies employees of such updates

DISCLAIMER

These privacy policies, as they exist or may be amended in the future, are intended to be used by DRCOG employees in meeting their responsibilities to DRCOG. Violation of a policy can be the basis for discipline or termination of employment or an association with DRCOG. Because these privacy policies

relate to the establishment and maintenance of high standards of performance, under no circumstances should any policy be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by DRCOG, its employees, interns, volunteers, providers, or its agents to another person.

3.0 Definitions

These definitions are general definitions and not intended to provide complete or legal definitions of terms that are described in the HIPAA Privacy Rules or HITECH Act, or C.R.S. § 24-73-101. Employees, providers, or other persons affiliated with DRCOG should consult with the HIPAA Compliance Coordinator if they have any questions.

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

Amend/Amendment: An amendment to PHI must always be in the form of information added to the existing PHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial PHI more precise, or show some of the original PHI to be incorrect. However, the original PHI is never altered. Changes are indicated by the addition of the amended information.

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

Authorization: A client statement of agreement to the use or disclosure of PHI to a third party.

Breach: The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of PHI.

Business Associate: A person or organization that performs a function or an activity on behalf of DRCOG that involves the use or disclosure of PHI. A business associate might also be a person or entity that provides residential or day programs, community participation, therapy, or support of clients. Business associates may include persons or entities that provide legal, actuarial, accounting, billing, benefit management, claims processing or administration, utilization review, quality assurance, consulting, data aggregation, management, administrative, accreditation or financial services involving the use or disclosure of PHI.

Business Associate Agreement (BAA): An agreement between a covered entity and a business associate, or between a business associate and its business associate subcontractor, that shall:

- Establish the permitted and required uses and disclosures of PHI by the business associate
- Provide that the business associate may use PHI only as permitted by the contract or as required by law, use appropriate safeguards, report any disclosures not permitted by the contract, make certain that agents to whom it provides PHI must abide by the same restrictions and conditions, make PHI available to individuals and make its records available to DHHS
- Authorize termination of the contract by the covered entity (or business associate if a business associate subcontractor is involved) if the covered entity (or business associate) determines that there has been a violation of the agreement

Business Continuity Plan (BCP): The part of a contingency plan that documents the process to restore any loss of data and to recover computer systems if a disaster occurs (i.e., fire, vandalism, natural disaster, or system failure). The document defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process to attain the stated disaster recovery goals.

Client: The person being served by DRCOG

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

Consent: A document signed and dated by the individual that a covered entity obtains prior to using or disclosing PHI to carry out treatment, payment, or healthcare operations. Consent is not required under the privacy rule.

Court Order: An order issued from a competent court that requires a party to do or abstain from doing a specific act.

Covered Entity: A health plan, a healthcare clearinghouse, or a healthcare provider that is covered by the Privacy and Security Rules.

De-Identification: The process of converting individually identifiable information into information that no longer reveals the identity of the client.

De-Identified Health Information: Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

Department of Health and Human Services (DHHS): The US Department of Health and Human Services, of which the Office for Civil Rights is a part. This Federal agency is charged with the development, statement, and implementation of the Privacy Rule.

Designated Record Set: A group of records maintained by or for DRCOG that is:

- The medical records and billing records about individuals maintained by or for DRCOG
- Used, in whole or in part, by or for DRCOG to make decisions about individuals

For purposes of this definition, the term "*record*" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for DRCOG.

Disclosure: The release, transfer, or provision of access to or divulging in any other manner of information outside DRCOG. The two types of disclosure are:

- *Routine Disclosure*: Customary disclosures of PHI that DRCOG discloses on a regular basis
- *Non-Routine Disclosure*: Disclosures of PHI that are not usually disclosed by DRCOG

Electronic Media: Includes, but may not be limited to, the following:

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

Electronic PHI (ePHI): Any PHI that is maintained or transmitted in an electronic media and may be accessed, transmitted, or received electronically.

Electronic Media: Electronic storage media including memory devices in computers such as hard drives and any removable and/or transportable digital memory medium, such as magnetic tape, magnetic disk, optical disk, or digital memory cards.

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.

Financial Records: Admission, billing, and other financial information about a client included as part of the designated record set.

Fundraising: An organized campaign by a private, nonprofit, or charitable organization designed to reach out to certain segments of the population or certain identified populations to raise monies for their organization or for a specific project or purpose espoused by their organization.

Healthcare: Includes, but is not limited to, the following:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription

Healthcare Operations: Any of the following activities of DRCOG to the extent that the activities are related to covered functions:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and clients with information about treatment alternatives; and related functions that do not include treatment
- Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs
- Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies
- Business management and general administrative activities of DRCOG, including, but not limited to:
    - Management activities relating to implementation of and compliance with the requirements of these policies and the HIPAA Regulation
    - Person served service
    - Resolution of internal grievances
    - The sale, transfer, merger, or consolidation of or part of DRCOG with another covered entity, or an entity that following such activity becomes a covered entity and due diligence related to such activity
    - Consistent with the applicable requirements of Section 2.2.2, "De-Identification of Health Information", and creating de-identified health information or a limited data set, and fundraising for the benefit of DRCOG, and marketing for which an individual authorization is not required

Healthcare Provider: An entity that provides healthcare, service or supplies related to the health of an individual, e.g., medical, dental, physical therapy, occupational therapy, speech therapy, behavioral health services or chiropractic clinics or hospitals.

Health Oversight Agency: An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory or an Indian tribe that is authorized by law to oversee the healthcare system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

HIPAA Compliance Coordinator: DRCOG employee who has been designated, pursuant to the Privacy Rule, with responsibility for ensuring DRCOG's compliance with the Privacy Rule.

HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act is a federal law that was designed to promote the adoption and meaningful use of health information technology and address the privacy and security concerns associated with the electronic transmission of health information. This definition is a general definition and is not intended to fully describe the HITECH Act.

Individually Identifiable Health Information (IIHI): Any information, including demographic information, collected from an individual that:

- Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual, and
    - Identifies the individual
    - With respect to which there is reasonable basis to believe that the information can be used to identify the individual

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 property that data or information have not been altered or destroyed in an unauthorized manner.

Limited Data Set (LDS): A data set that includes elements such as dates of application, termination, birth and death as well as geographic information such as the five-digit zip code and the individual's state, county, city, or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

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

Marketing: To make a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service. Face-to-face communications or those where only a gift of nominal value is provided are not considered marketing under the Privacy Rule. Marketing does not include the following:

- Communications by a covered entity for describing the entities participating in a healthcare provider network or healthcare plan network or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits
- Communications tailored to the circumstances of an individual if the communications are made by a healthcare provider to an individual as part of the treatment of the individual and for the purpose of furthering the treatment of that individual

- Communications by a healthcare provider or healthcare plan to an individual while managing the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, healthcare providers or settings of care

Master Record: The collection of documents, notes, forms, evaluations, assessments, and other items which collectively document the services provided to an individual in any aspect of services delivery by a provider; individually identifiable data collected and used in documenting services rendered. The master record includes records of care used by case management while providing client care services, for reviewing client data, or documenting observations, actions, or instructions. Master record consists of two parts: (1) the active record, which is defined as the designated record set and (2) the Administrative Record, which is not part of the designated record set.

Minimum Necessary: The least amount of PHI needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of PHI it uses, discloses, or requests to the minimum necessary to do the job.

Notice of Privacy Practices: A document required by HIPAA that provides the client with information about their rights under the Privacy Rule and how DRCOG generally uses their PHI.

Office of Civil Rights (OCR): The Department of Health & Human Services' enforcement agency for the Privacy, Breach, and Security Rules. OCR investigates complaints, enforces rights, and promulgates regulations, develops policy, and provides technical assistance and public education to make certain understanding of and compliance with non- discrimination and health information privacy laws including HIPAA.

Opt Out: To make a choice to be excluded from services, procedures, or practices. A person served rights under HIPAA include many situations where the client may request to be excluded from a service, procedure, or practice. In most cases, DRCOG must comply or attempt to comply with the request to be excluded.

Order: A mandate, precept; a command or direction authoritatively given; a rule or regulation.

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

Payment: The activities undertaken by a healthcare provider or payer to obtain reimbursement for the provision of care and services.

Person Served: Refers to persons applying, waiting for, or receiving services from DRCOG.

Personal Information (PI): A person's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or biometric data.

Personal Representative: The term used in the Privacy Rule to indicate the person who has authority under law to act on behalf of a client. For purposes of the Privacy Rule, DRCOG shall treat a personal representative as having the same rights as the client unless there is a reasonable belief that the personal representative has subjected the client to abuse or neglect or treating the person as the personal representative could endanger the client.

Physical Safeguards: Physical measures, policies, and procedures to protect electronic information systems, equipment and their data and related buildings and equipment, from threats, natural and environmental hazards, and unauthorized intrusion. They include restricting access to PHI, such as using locks and security cameras, retaining off-site computer backups, implementing, and maintaining workstation security and data backup and storage.

Policy: A high-level overall plan embracing the general principles and aims of an organization.

Privacy Rule: Refers to the regulation issued by the Department of Health and Human Services entitled *Standards for Privacy of Individually Identifiable Health Information*. The effective date for the Privacy Rule was April 14, 2003. Can be referenced as 45 CFR Part 160 and 45 CFR Part 164 and is amended from time to time. This definition is a general definition and is not intended to fully describe the Privacy Rule.

Protected Health Information (PHI): Any health information maintained by DRCOG that is individually identifiable except: (a) employment records held by DRCOG in its role as an employer; and (b) information regarding a person who has been deceased for more than fifty (50) years. PHI means any health information, including demographic information, whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

- Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual
    - That identifies the individual
    - There is a reasonable basis to believe the information can be used to identify the individual

All health information maintained by DRCOG is individually identifiable unless and until it is de-identified.

Psychotherapy Notes: Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes must be kept separate from the rest of the master record of the client.

Re-Identification: The process of converting de-identified health information back to individually identifiable health information. Re-identified health information does reveal the identity of the client and must be treated as PHI under the Privacy Rule.

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge.

Revoke: To cancel or withdraw an authorization to release medical information.

Risk Analysis: The process of identifying, prioritizing, and estimating an organization's exposure to risk arising from the operation of its information technology system to identify threats and vulnerability. Once identified, the risks can be mitigated by security controls (planned or already in place). Security risks can impact, among other things, the organization's operations, and organizational assets (PHI), the agency's employees and individuals, and third-party entities doing business with the organization. Also known as a security assessment.

Safeguarding: To make certain safekeeping of PHI for the client.

Security or Security Measures: 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.

Security Official: A position mandated by HIPAA. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation. The HIPAA Compliance Coordinator serves as the Security Official.

Security Rule: The Federal privacy regulations promulgated under HIPAA that created national standards to protect electronic medical records.

Subcontractor: A person or entity who has contracted with DRCOG to do work on its behalf.

Subpoena: A process to cause a witness to appear and give testimony, commanding him/her to lay aside pretenses and excuses and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof.

Technical Safeguards: The technology and the policy and procedures for its use that protect ePHI and control access to it.

Treatment: The provision, coordination, or management of healthcare and related services by DRCOG, including the coordination or management of services by DRCOG with a third party; consultation with other providers relating to a client; or the referral of a client for services between DRCOG and another authorized care provider.

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of that information within DRCOG. (See also Disclosure)

User: A person or entity with authorized access.

Whistleblower: A person, usually an employee, who reveals wrongdoing within an organization to the public, government agencies, or to those in positions of authority.

Workstation: Generic term used to refer to a desktop PC, laptop, or tablet.

4.0 Referenced Documents

The following documents are referenced in this HIPAA Policy and Procedure Manual:

Acceptable Computer Use Policy

Business Continuity Plan

Data Destruction Procedure

Encrypt, Decrypt, and Secure Delete Procedure

How to Send Encrypted E-mail in Office 365 User Guide

IT Termination Procedure

IT Threat Prevention Procedure

User Access Control Procedure

WorkDocs Monitoring and Auditing Procedure

5.0 Forms

The following forms mentioned in this manual can be found as separate PDF documents:

Amendment of PHI

Authorization to Release PHI

Authorization to use or disclose PHI

E-mail Communication Consent

Notice of Privacy Practices

Notice of Privacy Practices Acknowledgement of Receipt

Request Access to PHI

Request for an Accounting of Disclosures of PHI

Request for Communication by Alternative Means

Request to Restrict Use and Disclosure of PHI

6.0 Privacy and Security Rule Training - Policy

DRCOG conducts mandatory HIPAA privacy and security training to employees who could encounter PHI while performing their job functions.

6.1 Privacy and Security Rule Training - Procedure

The HIPAA Compliance Coordinator shall establish privacy and security training classes.

DRCOG employees shall be trained or retrained:

- Within 15 days of employment with DRCOG
- Within two months after a material change in privacy policies becomes effective and their job duties are affected by the change
- Within 15 days of the HIPAA Compliance Coordinator determining they have disregarded privacy laws, policies, or procedures
- If AAA staff member, annually following initial class. Training conducted by the employee's manager.
- If non-AAA staff member, annually following initial class. Training via online class chosen by HIPAA Compliance Coordinator.

The HIPAA Compliance Coordinator shall document each training class and the names of DRCOG employees that completed the training. Such documentation shall be maintained in DRCOG's 's personnel files maintained by the Human Resources Department. The supervisors of interns and volunteers shall document their HIPAA training when it occurs.

Discipline for Non-Compliance: Human Resources (HR) shall implement the same procedures to discipline and hold DRCOG employees accountable for completing HIPAA training, as with other trainings conditional for employment.

In the event of a material change in DRCOG's Privacy or Security policies or procedures, or in the HIPAA Privacy or Security Regulations, the HIPAA Compliance Coordinator shall work to retrain employees who would be affected by those changes. This additional training must occur within 30 days from the date of the change and no later than the effective date of the new Policies or Regulations. The same requirements for enforcement and documentation of completion, as indicated above, will apply.

Employees must be trained to recognize and respond to a breach of unsecured PHI and to understand the consequences of a security breach.

- If DRCOG employees are involved in a privacy or security incident that was not the result of malicious or willful conduct, the HIPAA Compliance Coordinator will provide the offending individual with additional training regarding DRCOG privacy and security policies and procedures. This training must focus on the areas directly related to the incident and be designed to prevent a recurrence of the incident.

In the event of a privacy or security incident, the HIPAA Compliance Coordinator shall issue a training reminder to employees that focuses on the privacy/security issue involved in the incident and how to avoid it in the future. If the HIPAA Compliance Coordinator becomes aware of recurring security

lapses, the HIPAA Compliance Coordinator will issue a reminder to employees regarding the lapse and the appropriate way to handle the issue considering DRCOG's policies and procedures.

To safeguard ongoing privacy compliance and information security, the HIPAA Compliance Coordinator may provide periodic privacy or security reminders to DRCOG employees. These reminders will be provided on an as needed basis. The reminders will be provided via e-mail or presentation at employee meetings and will focus on practical privacy or security issues, such as handling passwords, dealing with e-mail attachments, releasing information, etc.

7.0 Notice of Privacy Practices Acknowledgement of Receipt - Policy

DRCOG provides a copy of the *Notice of Privacy Practices* to persons applying for services at the time an application for services is being made. These individuals are also notified when the notice of privacy practices changes. DRCOG requests that each person receiving a copy of the *Notice of Privacy Practices* at the time of application acknowledges their receipt in writing.

7.1 Notice of Privacy Practices - Procedure

The *Notice of Privacy Practices* must comply with HIPAA rules and regulations. The *Notice of Privacy Practices* informs the person applying for or receiving services of:

- The uses and disclosures of PHI that may be made by DRCOG
- The rights of a person with respect to his/her PHI
- DRCOG duties in safeguarding such PHI

The Notice shall be written in plain language and made available in languages understood by a substantial number of consumers served by DRCOG. At a minimum, DRCOG shall make certain the Notice is available in Spanish.

At the time the Notice of Privacy Practices is provided, DRCOG intake employee must make a good faith effort to obtain the signature of the applicant on the *Notice of Privacy Practices - Acknowledgement of Receipt Form*. The *Notice of Privacy Practices - Acknowledgement of Receipt Form* must be attached to the person's official record.

If the applicant refuses or is otherwise unable to sign the *Notice of Privacy Practices - Acknowledgement of Receipt Form*, intake employee shall ask them to verbally acknowledge they have received a copy *Notice of Privacy Practices* and write "Verbal" on the appropriate signature line of the *Acknowledgement of Receipt*. Employees must initial and date next to word "Verbal" and attach the form to the person's official record.

DRCOG employees shall provide a copy of the written Notice of Privacy Practices to clients and to other persons upon request.

Whenever the Notice of Privacy Practices is revised, DRCOG's HIPAA Compliance Coordinator must make the revised Notice of Privacy Practices available upon request on or after the effective date of the revision.

Any employee who has knowledge of a violation or potential violation of this Procedure shall make a report directly to the HIPAA Compliance Coordinator.

8.0 Designated Record Set - Policy

Confidential information and records, whether they are in paper or electronic format, that are used for making decisions about a client are considered part of the designated record set.

8.1 Designated Record Set - Procedure

If records from other providers are used by DRCOG to make decisions related to the care and treatment of the client, then these records are considered part of the designated record set for access by employees (if within the scope of their job duties).

The designated record set is to be retained according to State and Federal regulations and following DRCOG's records retention schedule.

Program specific records, which may include active and historical designated records set documentation, are generally maintained by the programs in their administrative locations. Maintenance of privacy and security of these records is coordinated with the HIPAA Compliance Coordinator.

9.0 Minimum Necessary Uses and Disclosures of PHI - Policy

When using or disclosing PHI, DRCOG employees must make reasonable efforts to limit the amount of PHI used or disclosed to the minimum necessary. The following standards (the "Minimum Necessary Standard") apply to the use and disclosure of PHI by DRCOG:

- DRCOG employees may only have access to the amount and type of PHI necessary to carry out their job duties, functions, and responsibilities
- DRCOG limits access to, and use of, the PHI of clients in accordance with its business associate agreements with vendors and providers
- DRCOG employees must restrict their use, access, and disclosure of PHI to the minimum necessary

This Minimum Necessary Standard does not apply in the following situations:

- When the PHI is for use by, or a disclosure to, a healthcare provider for purposes of providing treatment to the client
- When the disclosure is to the client
- When the disclosure is pursuant to a valid authorization requested through the client in which case the disclosure must be limited to the PHI specified in the authorization
- When the disclosure is to the Secretary of the U.S. Department of Health and Human Services (Federal government)
- When the disclosure is to the Colorado Attorney General's Office, for purposes of notification and investigation of a breach of PHI impacting 500 or more Colorado residents
- When the law requires the disclosure; only PHI required to be disclosed by law may be disclosed

9.1 Minimum Necessary Standard When Requesting PHI

When requesting PHI from another entity, DRCOG must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are not on a routine or recurring basis, DRCOG staff, in conjunction with the HIPAA Compliance Coordinator, will evaluate the request to determine if the requirements of the Privacy Rule have been satisfied.

10.0 Safeguarding Verbal and Written PHI and Storing PHI - Policy

All employees and Business Associates are responsible for the privacy and security of PHI of persons receiving services. DRCOG's HIPAA Compliance Coordinator is responsible for periodically monitoring to ensure uses and disclosure of PHI complies with applicable Federal, State, and/or local law or regulation, and these policies.

10.1 Safeguarding Verbal Use of PHI - Procedure

Reasonable measures must be taken so that unauthorized persons do not overhear conversations involving PHI.

During face-to-face conversations, such measures may include but not be limited to:

- When possible, limiting conversations to the secured AAA office area
- Conducting meetings in a room with a door that closes, if possible
- Keeping voices to a moderate level
- Having only employees and others involved in the care of the client, who have a "need to know" the information, present at the meeting
- Limiting the PHI discussed to the minimum amount necessary to accomplish the purpose of the meeting
- If in a public area, moving to a private or semi-private area within DRCOG and lowering the voice to minimize likelihood of inadvertent disclosure

During telephone conversations where PHI is discussed, such measures may include:

- Lowering the voice
- Requesting that unauthorized persons step away from the telephone area
- Using a phone in a private area, or moving to a telephone in a more private area before continuing the conversation
- Limiting the PHI discussed to the minimum amount necessary to accomplish the purpose of the conversation

10.2 Safeguarding Written PHI - Procedure

Documents containing PHI must be stored appropriately to reduce the potential for incidental use or disclosure. Documents may not be easily accessible to unauthorized employees or visitors.

Hardcopy master records are maintained in a secure area that allows authorized employee access as needed and must be protected from loss, damage, and destruction.

Master records, whether in paper or digital formats, may be reviewed by authorized employees, interns, or volunteers. Authorized employees reviewing master records shall do so in accordance with the minimum necessary standards.

Hardcopy master records may not be left unattended in areas where client, visitors, and unauthorized individuals could easily view the records.

When left unattended, hardcopy records must be in a locked room, file cabinet, or drawer. Working documents left on the desk shall be turned face down or otherwise concealed before leaving work so that PHI is not readily observed by unauthorized individuals.

10.3 Storing Written PHI - Procedure

Active and inactive hardcopy master records are filed in a systematic manner in a location that safeguards the privacy and security of the information. The HIPAA Compliance Coordinator shall monitor storage and security of such hardcopy master records.

The HIPAA Compliance Coordinator shall identify and document those employees with keys to the file room and access to stored records. Only employees who must have access to stored records should have keys, keeping the number of persons with access to a minimum to assure that records are secure. Employees with keys must keep them in a secure place so that they are not accessible to unauthorized individuals.

Hardcopy master records must be checked out if removed from the file room. Only authorized persons are allowed to check out hardcopy master records.

- Use of “shadow” or “working copy” records or files is discouraged

Hardcopy master records shall be returned to the File Room at the end of each workday. Exceptions may be made if there is a valid need to keep the record for a longer period.

If the confidentiality or security of PHI stored in an active or inactive master record has been breached, the HIPAA Compliance Coordinator must be notified immediately.

11.0 Safeguarding PHI with Office Equipment and Mobile Devices - Policy

DRCOG employees may have access to PHI through web portals or e-mail accounts through office equipment and mobile devices. Care must be taken that the PHI accessed in these instances is safeguarded from unauthorized use, disclosure, or access. Employees must be familiar with the privacy and security policies and procedures relative to confidentiality of the PHI of clients and educated about the potential privacy and security risks caused by the theft or loss of computers, tablets, flash drives, or other removable media or memory devices.

11.1 Safeguarding PHI When Using Computers - Procedure

Employees who need to use computers to accomplish work-related tasks should have access to computer workstations. Access to computer-based PHI must be limited to employees who need the information for their job function.

- Employees must lock their workstation when leaving the work area
- Employees must lock their office doors when they leave their offices for extended periods of time and when they leave at the end of each workday
- Where possible, computer monitors must be positioned so that unauthorized persons cannot easily view information on the screen
- The access privileges of employees must be removed promptly following their departure from employment, internship, or a contractual relationship

Users of computer equipment must have unique login and passwords.

- Passwords must be changed in accordance with DRCOG security standards
- Posting, sharing, and any other disclosure of passwords and/or access codes is prohibited, and could result in corrective action for violation of security standards

Only authorized employees are allowed into the server room. At the end of each business day and during any period where the room is unattended, IT will lock the door that provides access to the room. The server room may not be left unattended if the room is unlocked.

Employees must immediately report any violations of this procedure to the HIPAA Compliance Coordinator and their Supervisor.

11.2 Safeguarding PHI When Using Printers, Copiers, or Scanners - Procedure

When printing documents containing PHI on the walk-up copiers, the secure print feature of the copier must be used. Scanning documents containing PHI on the walk-up copiers is not allowed. Instead, scanning must be performed in a secure area.

When copying documents containing PHI on the walk-up copiers, the user must ensure the original document as well as all copies are removed from the copier.

11.3 Privacy and Security for Portable Devices and Media - Procedure

Employees shall limit the use of assigned portable computers, cell phones, tablet devices, or any DRCOG provided resource or device that contains or can access client PHI, to DRCOG employees only.

- DRCOG issued portable devices must have appropriate password, security, and encryption programs installed upon them. Any PHI that is accessed from a mobile device must have adequate encryption as approved by the HIPAA Compliance Coordinator.
- Employees must avoid accessing individually identifiable information where it might be seen by persons without a legitimate need to know
- Smart phone users must be sure to close connections to e-mail and other systems/portals that contain PHI immediately when they are finished using the system/portal
- Permanent printed DRCOG asset tags with a device identification number must be installed on portable computers, tablets, and select devices
- If necessary, the HIPAA Compliance Coordinator will provide employees with accessories to protect their portable computers and tablets

Employees must only log in to systems and portals for which they have authority and properly obtained valid access credentials.

Employees may not store PHI on flash drives or other removable media or memory devices unless absolutely necessary and only on devices approved by the HIPAA Compliance Coordinator. When using removable media or memory devices, employees must:

- Ensure the flash drive is encrypted
- Keep the flash drive on their person at all times when in use; ideally on a keychain, neck strap or lanyard, or something else the person carries with him or her
- Not leave an external drive or other removable media or memory device attached to a computer
- Not store older documents on removable media. Removable media may contain only what is needed in the immediate future

The HIPAA Compliance Coordinator maintains a current list of DRCOG issued portable computer and tablet users, assigned equipment serial numbers, and software. DRCOG holds the portable computer or tablet user responsible and accountable for the safety and security of the assigned equipment and information. To prevent possible theft, employees must:

- Transport portable computers in a car's trunk or similar area rather than on a seat, thereby keeping it hidden, and never leave them unattended in a vehicle overnight or for an extended period
- Place unattended portable computers in room safes when leaving a hotel room

Employees must secure DRCOG issued portable computers and tablets when equipment is left unattended in offices and meeting rooms.

Privacy and security training shall emphasize that flash drives and other removable media and memory devices such as smart phones are easy to lose or misplace and that if the drive, media or device contains PHI, its loss or misplacement can create a serious data breach issue.

- The HIPAA Compliance Coordinator will perform loss investigations on stolen equipment

12.0 Transmitting PHI through E-mail or Fax - Policy

While providing services to persons applying for or receiving services, DRCOG employees may communicate PHI via e-mail or fax to clients or providers of service. Care must be taken so that the PHI transmitted in these instances is safeguarded from inappropriate use, disclosure, or access.

12.1 Transmitting PHI through E-mail - Procedure

E-mail users must be set up with a unique identity complete with unique password and file access controls.

E-mail users may not intercept, disclose, or assist in intercepting and disclosing e-mail communications.

Whether the e-mail is to DRCOG employees or to persons external to DRCOG, the amount of PHI disclosed via e-mail correspondence shall be limited to the minimum necessary to accurately communicate the needs or situation of the client.

PHI may be sent via e-mail within DRCOG's secured, internal network.

When sending PHI outside of the DRCOG network, such as over the Internet, every effort must be made to secure the confidentiality and privacy of the information.

- DRCOG e-mail containing PHI that is sent or forwarded to an external e-mail address shall be encrypted by entering *[encrypt]* in the e-mail subject line of Microsoft Outlook
- Refer to the *How to Send Encrypted E-Mail in Office 365* user guide for additional information
- Users must exercise extreme caution when forwarding messages. Sensitive information, including PHI, may not be forwarded to any party outside the agency without using the security safeguards specified above
- Users shall verify the accuracy of the e-mail address before sending any external e-mail containing PHI and, if possible, use e-mail addresses loaded in the system address book

Users shall periodically purge e-mail messages no longer needed for business purposes in compliance with the DRCOG records retention schedule.

Employee e-mail access privileges must be removed promptly following their departure from DRCOG.

Unencrypted e-mail messages, regardless of content, are not considered secure and private.

Employees must immediately report any violations of this policy to their supervisor.

All external e-mail containing PHI must automatically display the DRCOG-approved confidentiality statement.

12.2 Transmitting PHI through Fax - Procedure

Received documents must promptly be removed from the fax machine and, if necessary, forwarded to the appropriate recipient.

Unless otherwise prohibited by State law, information transmitted via facsimile is acceptable and may be included in the master record of the client.

When sending a fax document that includes PHI, the PHI disclosed must be the minimum necessary to meet the requestor's needs and/or communicate information about the needs or situation of a client.

- Highly sensitive health information must not be sent by fax (e.g., information relating to AIDS/HIV, drug and alcohol abuse, and psychotherapy notes)

When sending a fax document that includes PHI, steps must be taken to confirm that the fax transmission is sent to the appropriate destination. These include:

- Pre-programming and testing destination numbers to eliminate errors in transmission due to misdialing
- Asking frequent recipients to notify DRCOG of a fax number change

- Confirming the accuracy of the recipient's fax number before pressing the send function

When transmitting information, a cover page must be attached to any fax document that includes PHI. The cover page needs to include:

- Destination of the fax, including name, fax number, and phone number
- Name, fax number, and phone number of the sender
- Date
- Number of pages transmitted
- DRCOG-approved confidentiality statement

If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system must be checked to obtain incorrect recipient's fax number. Fax a letter to the receiver and ask that the material be returned or destroyed. Notify the HIPAA Compliance Coordinator of a misdirected fax.

13.0 Authorizations to Release PHI and Disclosure of PHI - Policy

In rare circumstances, PHI may be disclosed without authorization for purposes other than continuing care. DRCOG may disclose PHI without authorization only if approved by the HIPAA Compliance Coordinator.

13.1 Exceptions to Authorization Requirements - Procedure

Exceptions may include:

- In limited circumstances, for the healthcare operations of another Covered Entity, if the other Covered Entity has or had a relationship with the client
- To the Secretary of the U.S. Department of Health and Human Services for determining compliance with the Privacy Rule
- To the Colorado Attorney General's Office, for purposes of notification and investigation of a breach of PHI impacting 500 or more Colorado residents
- As required by other State or Federal law
- An administrative request, subpoena, or investigative demand. DRCOG may disclose the requested PHI if the administrative document itself or a separate written statement recites:
    - The information sought is relevant to a lawful inquiry as approved by DRCOG's legal counsel
    - The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry
    - De-identified information could not be used
- A request by a public official, per 45 CFR 164.514(h), if the official presents:
    - A badge or other credential, such as a written statement of the authority under which the information is requested, for example, a copy of the law or regulation. If obtaining a written statement is impractical, an oral statement is sufficient
    - A request on verified government letterhead
    - If the person making the request is acting on behalf of a Public Officer, a written statement on government letterhead that the person is acting on behalf of a Public Officer. If other authority is presented, contact legal counsel for guidance before disclosure.
- If PHI is disclosed to:
    - Prevent or lessen a serious and imminent threat to the health or safety of a person or the public
    - Law enforcement authorities to identify or apprehend an individual upon approval from DRCOG's legal counsel

- PHI may not be used or disclosed in the absence of a valid written authorization if the use or disclosure is:
    - Of psychotherapy notes as defined by the Privacy Rule
    - For marketing purposes
    - For fundraising purposes

13.2 Disclosure Pursuant to an Authorization - Procedure

When the HIPAA Compliance Coordinator determines that a written authorization is required prior to disclosing PHI, the HIPAA Compliance Coordinator may not disclose the PHI until a valid written authorization is received from the client.

- If the request for disclosure is not accompanied by a written authorization, the HIPAA Compliance Coordinator shall notify the requestor that DRCOG is unable to provide the PHI requested. The requestor shall be supplied with an Authorization to Use or Disclose PHI form.
- The HIPAA Compliance Coordinator must make reasonable attempts to verify the identity and the authority of a person/entity making a request for the disclosure of PHI, if the identity or authority of such person is not known. Further, the HIPAA Compliance Coordinator shall request from the person/entity seeking disclosure of PHI such documentation, statement, or representation, as may be required by the Privacy Rule, prior to a disclosure.
    - DRCOG may rely on required documentation, statements, or representations that, on their face, meet the verification requirements, if the reliance is reasonable under the circumstances. If there are concerns regarding the requirements, the HIPAA Compliance Coordinator must contact DRCOG legal counsel.

If the request for disclosure is accompanied by a written authorization, the HIPAA Compliance Coordinator will review the authorization to ensure it is valid. The authorization form must be fully completed and signed and dated by the client before the PHI is used or disclosed.

- The authorization must be written in a language understood by the person signing the authorization. If a client needs interpretation, they need to notify DRCOG employees for assistance.
- If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the HIPAA Compliance Coordinator shall notify the requestor, in writing, of the deficiencies in the authorization. No PHI may be disclosed unless and until a valid authorization is received.
- If the authorization is valid, the HIPAA Compliance Coordinator shall disclose the requested PHI to the requester. Only the PHI specified in the authorization may be disclosed.

Each authorization must be filed in the official record of the person applying for or receiving services.

Other DRCOG employees may not release master records without the approval of the HIPAA Compliance Coordinator except in case of an emergency or because of a specifically approved program area function.

- After hours and on weekends, release of information for instances that include, but are not limited to, emergency transfer, crisis intervention, or similar urgent situation is allowed
- Emergency release of information must be documented as to the justification

In specific program instances whereby, a multi-agency Authorization to Release PHI is utilized, the completed form must not accompany the PHI, as it could identify other agency providers and violate confidentiality.

13.3 Responding to Specific Types of Disclosures - Procedure

Media: No PHI may be released to the news media or commercial organizations without the authorization of the client or his/her personal representative.

Telephone Requests: Employees receiving requests for PHI via the telephone must make reasonable efforts to identify and verify that the requesting party is entitled to receive such information.

13.4 Disclosures to Individuals Involved in the Care of a Person Served - Procedure

DRCOG may disclose PHI to a family member, other relative, close friend, or any other individual identified by the client:

- That is directly relevant to that individual's involvement in the care or payment for care of the client. In such cases, DRCOG must obtain a signed release from the client granting permission to release the information.
- To notify such individual of the location, general condition, or death of a client

If the disclosure is sought by individuals involved in the care of a client and it is relevant to the requesting party's involvement in the care, DRCOG may rely on reasonable professional judgment in verifying the identity and authority of the individual seeking disclosure.

- DRCOG employees must take reasonable steps to confirm the identity of a family member or friend of the client. DRCOG is permitted to rely on the circumstances as confirmation of involvement in care.

Prior to a permitted disclosure, if the client is present for, or otherwise available, then DRCOG employees may use or disclose the PHI if they:

- Obtain the agreement of the client
- Provide the client with an opportunity to object to the disclosure and the client does not express an objection (this opportunity to object and the response may be done orally)
- Based on the exercise of professional judgment, reasonably infer from the circumstances that the client does not object to the disclosure

13.5 Revocation of Authorization - Procedure

The client may revoke his/her authorization at any time. The authorization may be revoked verbally or in writing. If the client informs DRCOG that he/she wants to revoke the authorization, DRCOG employees shall obtain a copy of the official authorization (hardcopy or printed electronic) and complete the shaded area at the bottom of the form. If the client gives verbal revocation, detailed notes to substantiate the verbal revocation shall be maintained in the client's file.

Upon receipt of a written revocation, DRCOG may no longer use or disclose the PHI of the client, pursuant to the authorization.

Each printed or electronic revocation formally completed by employees must be filed in the official record of the client.

The HIPAA Compliance Coordinator will track and maintain a log of these requests.

14.0 Responding to a Subpoena - Policy

From time to time, employees and others associated with DRCOG may be served with a subpoena or receive a letter from a lawyer or a less formal request for information, testimony, or documents. Similarly, employees and others associated with DRCOG may receive notification, or field questions or requests for information and documents, from Federal, State, or local authorities regarding an investigation. DRCOG shall respond to the request in a manner that appropriately addresses the request, while observing the

advice of counsel, the requirements of HIPAA, the needs for confidentiality for clients, and the applicability of any other standards, statutes, court orders, or policies. The HIPAA Compliance Coordinator must always be informed of such requests for information. The HIPAA Compliance Coordinator shall work in conjunction with the Director of Administration and Finance to obtain legal guidance.

14.1 Responding to a Subpoena or Investigative Demand - Procedure

Employees and others associated with DRCOG who are served with a formal or informal request for information, testimony, or documents relating to any client by DRCOG, or to DRCOG itself, shall promptly advise their supervisor, their Division Director, the HIPAA Compliance Coordinator, and the Director of Administration and Finance who will in turn promptly notify DRCOG's Executive Director.

- The Director of Administration and Finance will coordinate responding to the request and provide direction to employees on their response

Employees and others associated with DRCOG who receive notification, or field questions, from Federal, State, or local authorities regarding an investigation must promptly advise the Director of Administration and Finance.

- The Director of Administration and Finance shall coordinate responding to the request and provide direction to employees on their response

The Director of Administration and Finance shall seek the advice of DRCOG's legal counsel and insurance professionals before responding to any subpoenas, court orders, or investigatory requests for information.

15.0 Restrictions to Permitted Uses and Disclosures of PHI - Policy

The client is notified of their right to request restrictions on the use and disclosure of PHI in DRCOG's Notice of Privacy Practices. Specifically, the client may request restrictions on:

- The use and disclosure of PHI for treatment, payment, or healthcare operations
- The disclosures to family, friends, or others for involvement in care and notification purposes

15.1 Restrictions on Uses/Disclosures of PHI - Procedure

Persons served must make their request in writing. The HIPAA Compliance Coordinator will provide a Request to Restrict Use and Disclosure of PHI form to the individual asking to make a restriction.

The HIPAA Compliance Coordinator manages requests for restrictions. A request for restriction may not be reviewed until the Request to Restrict form is completed and signed by the client. The HIPAA Compliance Coordinator may assist the client in completing the form, if necessary.

The HIPAA Compliance Coordinator will review the request in consultation with DRCOG employees providing care or services to the client to determine the feasibility of the request. DRCOG will give primary consideration to the need for access to the PHI for service and payment purposes in making its determination.

If DRCOG agrees to the requested restriction, the HIPAA Compliance Coordinator must document the restriction on the *Request to Restrict Use and Disclosure of PHI* form, provide the individual making a request with a copy and send the original to the master record of the client. The HIPAA Compliance Coordinator must also notify appropriate DRCOG employees of the restriction.

DRCOG employees must abide by the accepted restriction with the following exceptions:

- DRCOG may use the restricted PHI or may disclose such information to an authorized provider if the client needs emergency services or treatment. In this case, DRCOG employees

may release the information, but ask the emergency provider not to further use or disclose the PHI of the client.
- DRCOG may disclose the information to the individual who requested the restriction
- DRCOG may use and disclose the restricted PHI when statutorily required to use and disclose the information under the Privacy Rule

If DRCOG declines the request for restriction, the HIPAA Compliance Coordinator shall complete the "*Facility Response*" section of the *Request to Restrict Use and Disclosure of PHI* form and provide a copy to the individual making the request.

The request and documentation associated with the request must be placed in the master record of the client and retained for a period no less than six years from receipt.

15.2 Terminating the Restrictions on Uses/Disclosures of PHI - Procedure

If the client wishes to terminate the accepted restriction, they may do so in writing or verbally. If the client verbally terminates the restriction, DRCOG employees must document the verbal termination in the record of the client.

The HIPAA Compliance Coordinator must notify the appropriate program and/or case management employee of the termination of the restriction.

The HIPAA Compliance Coordinator must document the termination of the restriction on the *Request to Restrict Use and Disclosure of PHI* form, provide the client with a copy, and maintain the documentation in the record of the client.

Termination of a restriction is effective for PHI created or received by DRCOG.

There may be situations that occur in which DRCOG wishes to terminate the restriction without the agreement of the client.

- The HIPAA Compliance Coordinator shall inform the client that the restriction is being terminated
    - *If by mail*: If the client is informed by mail that DRCOG is terminating the restriction, the notification shall be sent via certified mail, return receipt requested. DRCOG must maintain a copy of the notification and of the return receipt with the *Request to Restrict Use and Disclosure of PHI* form. DRCOG may not terminate the restriction until it receives confirmation that the person(s) listed above have received the notification.
    - *If in person*: If the client is informed in person, it is preferable to have the appropriate individual sign and date a notification of termination of a restriction. However, it may be acceptable to document that the person(s) listed above were notified on the *Request to Restrict Use and Disclosure of PHI* form.
    - *If by telephone*: If the client is informed by telephone, this action shall be documented on the *Request to Restrict Use and Disclosure of PHI* form. In addition, an e-mail, or alternately a letter shall be sent to the appropriate individual listed above. Letters must be sent via certified mail, return receipt requested. The termination will be effective as of the date the appropriate individual listed above is informed by telephone.
    - If by e-mail: If the client is informed by e-mail, this action must be documented on the Request to Restrict Use and Disclosure of PHI form. In addition, a letter must be sent via encrypted e-mail, to a verified e-mail account of the appropriate person listed above. The termination will be effective as of the date of the e-mail.
- Such termination is only effective with respect to PHI created or received after DRCOG has informed the client is informed that it is terminating the restriction. DRCOG shall continue to

abide by the restriction with respect to any PHI created or received before it informed the person(s) listed above about the termination of the restriction.

16.0 Communication and Access to PHI by Persons Served - Policy

Persons served have the right to request communication about their PHI in a variety of ways, such as through phone calls, e-mails, or in writing. A client also has the right to inspect and obtain a copy of PHI in his or her designated record set, except for information compiled in reasonable anticipation of, or for, use in a civil, criminal or administrative action or proceeding.

16.1 Requests for Alternate Communication Methods - Procedure

When a client notifies DRCOG employees of their preferred method of communication, or requests that DRCOG communicate with him or his/her personal representative by some alternate means, DRCOG shall provide the client with a copy of a *Request for Communication by Alternative Means* form. A request may not be evaluated until this form is completed and signed by the client or personal representative.

If the client would like to communicate by e-mail, it is recommended that an *E-mail Communication Consent* form be used.

The HIPAA Compliance Coordinator shall review the completed *Request for Communication by Alternative Means* form to determine if it is a reasonable request. The HIPAA Compliance Coordinator may not require an explanation for the request. The HIPAA Compliance Coordinator may generally accommodate a request determined to be reasonable.

The HIPAA Compliance Coordinator shall complete the response section of the *Request for Communication by Alternative Means* form to inform the client of DRCOG's decision.

The HIPAA Compliance Coordinator must maintain requests and responses in the appropriate location in the official record of the client.

16.2 Access to PHI by Persons Receiving Services - Procedure

A client has the right to inspect the designated record set, except for information compiled in reasonable anticipation of, or for, use in a civil, criminal, or administrative action or proceeding. Although HIPAA regulations do not require the access request to be in writing, the preferred procedure is to complete a *Request Access to PHI* form.

- The HIPAA Compliance Coordinator shall manage the viewing of the designated record set and determine whether the requestor is considered a legal representative based on State law (e.g., guardian, conservator, durable power of attorney)
    - The HIPAA Compliance Coordinator must verify the identity of the requester before access to the record is allowed (e.g., driver's license, identification card, other legal ID)
- The HIPAA Compliance Coordinator must set up a meeting within 24 hours as required by law. If the requestor cannot accommodate a meeting within the 24-hour time frame, the review should be set up at a mutually agreed upon time.
    - If possible, program or case management employees should be in attendance during the meeting, to answer questions, prevent the record from being altered, and to prevent documents from being removed or destroyed
    - The client, or their legal representative shall be allowed to review and read the record without intervention from the employees present

When a client requests a copy of the PHI in the designated record set, they shall be provided with a copy of a DRCOG *Request Access to PHI* form to sign. DRCOG prefers to provide this information in an encrypted e-mail; however, a paper copy request may be accommodated.

- A reasonable cost-based fee may be charged for the paper copies provided. The cost per page may not exceed the State statute for copying costs. One free copy of the designated record set shall be made available to the client or his/her legal representative.

Requests for access to PHI and release of information shall be managed by the HIPAA Compliance Coordinator.

If a former client requests to view or review PHI, DRCOG must respond to the request within 30 days.

- If the PHI is stored off-site or cannot be processed within the allowed 30 days, DRCOG may have a one-time extension of 30 days, provided a written statement of the reasons for the delay are provided and the date by which DRCOG shall complete its action on the request is stated
- The HIPAA Compliance Coordinator must provide the PHI in the form or format requested. If the PHI is not accessible in the format requested, a readable hard copy or a format acceptable to DRCOG and the person making the request shall be provided. A reasonable cost-based fee may be charged for the paper copies provided. The cost per page may not exceed the State statute for copying costs.

16.3 Denying Access to PHI by Persons Receiving Services - Procedure

DRCOG must provide a timely, written denial to the client, which includes the basis for the denial and, if applicable, a statement of the individual's review rights. In addition, it must provide a description of how the individual may complain to DRCOG or to the Secretary of the Office of Civil Rights.

DRCOG may deny the request if the PHI is not contained in its designated record set.

The client has the right to request a review of the denial. If a request is received, the following steps shall be taken:

- HIPAA Compliance Coordinator shall promptly refer the request to have the denial reviewed to the Director of Administration and Finance.
- The request may also be reviewed by a qualified individual who was not directly involved in the denial, if necessary
- DRCOG must promptly provide written notice of the results of the review and based on the review, take any necessary steps required

DRCOG may deny the request for access to the PHI of a client without a right to review if:

- The request is for information compiled in anticipation of a legal proceeding
- The request is for PHI created or obtained during research which includes treatment for as long as the research continues, provided that the client has agreed to the denial of access and DRCOG has informed the client that this right shall be reinstated upon completion of the research
- The request is for PHI obtained from someone other than a provider under the promise of confidentiality and disclosure would likely reveal the source

DRCOG may deny the request for access to the PHI of a client provided the client has been given a right to review the denial if:

- A licensed healthcare professional has determined, in the exercise of professional judgment, that the access of requested PHI is reasonably likely to endanger the life or physical safety of the individual or another person

- The PHI refers to another person (unless such other person is a healthcare provider (for example, a doctor) and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person
- The individual's personal representative makes a request for access and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person

17.0 Amendment of PHI - Policy

Persons served must be notified of the right to amend their electronic as well as hard copy PHI in the Notice of Privacy Practices.

17.1 Evaluating and Responding to a Request for Amendment of PHI - Procedure

The HIPAA Compliance Coordinator shall process all requests for amendment of PHI.

Upon receiving an inquiry from a client regarding the right to amend his/her PHI, the HIPAA Compliance Coordinator must provide the client with a copy of an *Amendment of PHI* form. A request for amendment may not be evaluated until the request form is completed and signed by the client.

The HIPAA Compliance Coordinator must date stamp or write the date received and initial the *Amendment of PHI* form.

The HIPAA Compliance Coordinator shall consult with the Director of Administration and Finance and appropriate employees concerning the validity of the requested Amendment.

The HIPAA Compliance Coordinator must act on the request for amendment no later than 60 days after receipt of the request.

- If the amendment is accepted, the HIPAA Compliance Coordinator must make the amendment and inform the client within 60 days of the written request
- If the amendment is denied, DRCOG must notify the client in writing of the denial within 60 days of the written request

If DRCOG is unable to act on the request for amendment within 60 days of receipt of the request, it may have one extension of no more than 30 days. The HIPAA Compliance Coordinator must notify the client in writing of the extension, the reason for the extension, and the date by which action must be taken.

17.2 Accepting a Request for Amendment of PHI - Procedure

If the HIPAA Compliance Coordinator, in consultation with the Director of Administration and Finance, appropriate division director and/or employees, determines that the request for amendment must be accepted, in whole or in part, the HIPAA Compliance Coordinator shall:

- Place a copy of the amendment in the records of the client or provide a reference to the location of the amendment within the body of the master record
- The client may indicate providers or entities with whom the amendment may be shared (as identified on the original *Amendment of PHI* form)
- This notification shall occur within a reasonable period

The HIPAA Compliance Coordinator shall also identify other persons, including business associates, that he/she knows have the PHI and that may have relied on, or could foreseeably rely on, such information to the detriment of the client. The HIPAA Compliance Coordinator shall determine

whether the client wishes for DRCOG to notify such other persons or organizations of the amendment.

- If the client wishes for DRCOG to notify these individuals, the HIPAA Compliance Coordinator shall obtain a signed *Authorization to Release PHI* form
- This notification shall occur within a reasonable period

17.3 Denying a Request for Amendment of PHI - Procedure

DRCOG may deny the request for amendment in whole or in part if:

- The PHI was not created by DRCOG (e.g., a physical examination, dental record, agency assessment). An exception may be granted if the client provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment and it is apparent that the amendment is warranted. (Note: This is rarely the case.)
    - Every other avenue must be explored before an amendment is made to information that was not created by DRCOG
- The PHI is not part of the designated record set (i.e., information gathered on worksheets or contact notes that do not become a part of the master record)
- The PHI would not be available for inspection under the HIPAA Privacy Rule
- The PHI that is subject to the request for amendment is accurate and complete

If the HIPAA Compliance Coordinator, in consultation with the Director of Administration and Finance, appropriate division director and/or employees, determines that the request for amendment may be denied in whole or in part, the HIPAA Compliance Coordinator shall provide the client with a timely amendment denial letter. The denial must be written in plain language and contain:

- The basis for the denial
- A statement that the client has a right to submit a written statement disagreeing with the denial and an explanation of how to file such a statement
- A statement that, if the client does not submit a statement of disagreement, they may request that DRCOG includes the request for amendment and the denial with any future disclosures of the PHI
- A description of how the client may file a complaint with DRCOG or to the Secretary of the U.S. Department of Health and Human Services. The description must include the name or title and telephone number of the contact person for complaints.

If the client submits a written statement of disagreement, DRCOG may prepare a written rebuttal to the statement. DRCOG must provide a copy of the written rebuttal to the client.

The following documentation must be appended (or otherwise linked) to the PHI that is the subject of the disputed amendment:

- The *Amendment of PHI* form
- DRCOG's amendment denial letter
- The statement of disagreement if any
- DRCOG's written rebuttal if any

If the client submitted a statement of disagreement, DRCOG shall disclose information listed in the previous paragraph or an accurate summary of such information with future disclosures of the PHI to which the disagreement relates.

- If the client did not submit a statement of disagreement and if the client has requested that DRCOG provide the *Amendment of PHI* form and the amendment denial letter with any future disclosures, DRCOG must include these documents (or an accurate summary of that information) with future disclosures of the PHI to which the disagreement relates

17.4 Receiving a Notice of Amendment from Another Entity or Provider - Procedure

If another provider or entity notifies DRCOG of an amendment to the PHI it maintains, the HIPAA Compliance Coordinator shall make the amendment to the designated record set.

- Amendments to the designated record set must be filed with that portion of the PHI to be amended
- Amendments that cannot be physically placed near the original PHI must be filed in an appropriate location. A reference to the location of the amendment must be added near the original information location.

General information regarding requests for amendment, forms relating to amendments and correspondence relating to denial or acceptance of requests to amend must be filed in the record of the client.

18.0 Accounting of Disclosures of PHI - Policy

Clients have the right to receive an accounting of the disclosures of their PHI maintained in their designated record set.

18.1 Accounting of Disclosures of PHI - Procedure

Upon receiving an inquiry about disclosures of PHI, the HIPAA Compliance Coordinator must provide the client with a copy of a Request for an *Accounting of Disclosures of PHI* form.

- Requests are not evaluated until the form is completed and signed by the client
- A current version of DRCOG HIPAA related privacy forms and letter templates shall be maintained on DRCOG's intranet

The HIPAA Compliance Coordinator shall review and process the request.

The written accounting of disclosures is provided to the requestor using a format created and maintained by HIPAA Compliance Coordinator.

- The accounting must include disclosures during the period specified by the client in the request. The specified period may be up to six years prior to the date of the request.
- The HIPAA Compliance Coordinator must include known disclosures made by its Business Associates, if aware of any such disclosures that are required to be included in an accounting of disclosures
- The HIPAA Compliance Coordinator must exclude those disclosures that qualify as an exception
- For each disclosure, the accounting must include:
    - The date the request for disclosure was received
    - The name of provider or entity requesting disclosure and, if known, the address of such person or entity
    - A brief description of the PHI that was disclosed
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure
- If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, the HIPAA Compliance Coordinator may provide:
    - The first disclosure during the accounting period
    - The frequency or number of disclosures made during the accounting period
    - The date of the last such disclosure during the accounting period

The HIPAA Compliance Coordinator must provide the written accounting of disclosures no later than 60 days after receipt of the request.

- If DRCOG is unable to meet the 60-day time frame, DRCOG may extend the time once by no more than 30 days if the individual is provided with a written statement of the reasons for the delay and the date by which DRCOG must provide the accounting

DRCOG provides the first accounting to a client within a 12-month period without charge. However, DRCOG may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided DRCOG has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.

DRCOG must document and retain for six years from the date of the accounting for paper records, and three years from the date of the accounting for electronic records:

- The information required to be included in the accounting
- The written accounting provided to the requesting party

18.2 Exceptions to the Accounting of Disclosures - Procedure

Accounting of disclosure does not include disclosures:

- Necessary to carry out treatment, payment, and healthcare operations
- To the client for whom the PHI was created or obtained
- Pursuant to a signed authorization by the client
- To persons involved in the care of the client
- For national security or intelligence purposes
- To a correctional institution
- Temporarily suspended by a law enforcement official or health oversight agency (exception applies only during the period of suspension)
- That are incidental
- As part of a Limited Data Set

19.0 HIPAA Privacy Complaints - Policy

Any concerned individual has the right to file a formal complaint concerning privacy issues without fear of reprisal. Such issues could include, but are not limited to, allegations that:

- PHI that was used/disclosed improperly
- Access or amendment rights were wrongfully denied
- DRCOG's Notice of Privacy Practices does not reflect current practices accurately

19.1 HIPAA Privacy Complaints - Procedure

DRCOG uses the *Notice of Privacy Practices* form to notify persons receiving services of their right to complain to DRCOG or the Department of Health and Human Services about privacy issues.

All concerns/complaints shall be directed to the HIPAA Compliance Coordinator, by telephone, fax, mail, e-mail, or in person. The person making the complaint must put their complaint in writing, either through a letter or e-mail. The HIPAA Compliance Coordinator must document the complaint in the log of complaints regarding privacy issues.

Once the complaint form and log are completed correctly, the HIPAA Compliance Coordinator shall submit the complaint to the Director of Administration and Finance, who, if necessary, determines whether an investigation is warranted. The Director of Administration and Finance Division Director shall assemble an investigative team, as needed, composed of appropriate individuals based upon the circumstances of the complaint.

Following completion of the investigative team's review, the HIPAA Compliance Coordinator must be notified of the substance of their findings and decision. The HIPAA Compliance Coordinator shall:

- Document the outcome of the complaint
- Complete the log of complaints by entering the resolution and any required follow-up actions

The HIPAA Compliance Coordinator must maintain documentation of complaints received and their disposition for a period of at least six years (from the date of creation) in accordance with Federal regulations.

Employees may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against the client or any other person filing a complaint.

20.0 De-identification of PHI - Policy

DRCOG must convert the PHI of a person receiving services into a format that does not identify (de-identifies) the client when:

- PHI is used or shared for purposes other than treatment, payment or healthcare operations, or authorized exceptions
- Information is used or shared without the authorization of the client

20.1 De-identification of PHI - Procedure

Before employees treat any information as being de-identified, it must be submitted to the HIPAA Compliance Coordinator for determination of whether health information has been de-identified.

The following identifiers of the client, or of relatives, employers, or household members must be removed by one of the following two methods of de-identification:

- Elimination of identifiers:
  - Names.
  - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code if the geographic area contains more than 20,000 people. If less than 20,000 people are found to be in this area based on the first three digits of the zip code, the code shall be changed to 000.
  - Months and dates directly related to a client, including birth date, admission date, discharge date and date of death. For persons over the age of 89, the month, date and year must be removed, except that such ages may be aggregated into a single category of age 90 or older.
  - Telephone and fax numbers
  - E-mail address
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - Web Universal Resource Locators (URLs)
  - Internet Protocol (IP) address numbers
  - Biometric identifiers, including finger and voiceprints
  - Full face photographic images and any comparable images
  - Any other unique identifying number, characteristic, or code

Note: In addition to removing the above identifiers, the HIPAA Compliance Coordinator must verify that the de-identified PHI being shared cannot be used alone or in combination with other information to identify a client.

Statistical de-identification: A process in which a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies such principles and determines that the risk is very small that the information could be used to identify the consumer. The methods and the results of the analysis must be documented.

20.2 Re-identification of PHI - Procedure

During the process of de-identifying PHI, the HIPAA Compliance Coordinator or those performing statistical de- identification, shall assign a code that allows the information to be re-identified by DRCOG if the code is not derived from or related to information about the client, and is not otherwise capable of being translated so as to identify the client. DRCOG may not use or disclose the code or any other means of record identification for any other purpose and may not disclose the mechanism for re-identification.

Whether or not information shall be coded for re-identification and be re-identified is determined by the HIPAA Compliance Coordinator. If information is re-identified, the HIPAA Compliance Coordinator must oversee the process of doing so.

21.0 Business Associates - Policy

Providers that contract with DRCOG are required to sign a Business Associate (BA) Agreement in which they supply assurances that they will create, receive, use, safeguard, disclose, and transmit the PHI of persons receiving services within HIPAA Privacy and Security regulations and as permitted by the BAA.

21.1 Business Associates - Procedure

DRCOG must follow established procedures regarding contract review, revision, and approval to verify that the contract is compliant with State and Federal law, to include any HIPAA contract addendums.

The DRCOG contracts department, in collaboration with the Director of Administration and Finance shall determine whether a BAA is necessary for specific entities. Common examples of entities needing a BAA are:

- Providers of services
- DRCOG subcontractors
- An attorney who reviews PHI to assist in a case or any other matter that requires the disclosure of PHI to the attorney
- Consultants or vendors who may see PHI while completing their duties for DRCOG

If a BAA is necessary and the other party provides its own BAA, the HIPAA Compliance Coordinator shall review the Agreement to ensure it meets requirements of the Privacy and Security Rule.

If a BAA is necessary and the other party does not provide the Agreement, the DRCOG contracts department must submit DRCOG's BAA for approval by the other party.

If the business associate (BA) refuses to sign the Agreement, the Privacy Rule prohibits DRCOG from disclosing any PHI to the BA. If the BA requires access to PHI to perform the function or service on behalf of DRCOG, DRCOG may not contract with the BA.

The original signed contract and contract addendum containing BA language must be maintained by DRCOG.

The HIPAA Compliance Coordinator and contracts department shall amend BAAs when changes occur to HIPAA rules, regulations, and standards.

21.2 Breach of a BAA and Sanctions - Procedure

If a DRCOG employee learns of a breach or violation of a BA requirement by a BA, such breach or violation must be reported to the Director of Administration and Finance or the HIPAA Compliance Coordinator. The HIPAA Compliance Coordinator, along with the Director of Administration and Finance and legal counsel, shall determine whether reasonable steps can be taken to cure the breach. The BA is required to take whatever reasonable steps can be taken to cure the breach and prevent further breaches of PHI in the future.

If reasonable steps to cure the BA's violations are unsuccessful or if the BA refuses to take necessary steps to cure the breach or prevent further breaches of PHI, DRCOG may:

- Terminate the contract or arrangement
- If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services

When a contract with a BA is being terminated, the BA is obligated to return or destroy any PHI that was shared with the BA because of its contract with DRCOG.

- The HIPAA Compliance Coordinator shall assist with contacting the BA regarding the BA's obligations to return or destroy PHI that originated from DRCOG
- If return or destruction is not feasible, the BA is obligated to maintain the PHI that originated from DRCOG in accordance with HIPAA standards, rules, and regulations

The contract and contract addendum must be retained for no less than six years after the contract was last in effect.

22.0 Marketing and Fundraising - Policy

DRCOG obtains the written consent of a client prior to using confidential information and/or a photograph of a client in its marketing or communication materials.

22.1 Using PHI for Marketing - Procedure

The Privacy Rule defines marketing as a communication and/or disclosure of PHI that encourages an individual to use or purchase a product or service, except under the following conditions:

- Communications made directly by DRCOG to describe the services it provides
- Communications made for care or treatment of the individual
- Communications for case management or care coordination for the client
- Communications to direct or recommend alternative treatments, therapies, and care providers or settings of care
- Face to face communications made by DRCOG representatives to an individual

Marketing employees shall obtain a valid, completed *Authorization to Use or Disclose PHI* form or other approved forms designed to confirm consent of use, prior to using or disclosing PHI for purposes that meet the HIPAA definition of marketing (above) and do not qualify for any of the exceptions listed in the five items above.

- The authorization must conform to procedures outlined in the "Authorization to Release and Disclosure of PHI" section of this document
- If direct or indirect remuneration to DRCOG from a third party is involved, the authorization must state the nature of such third-party remuneration

- DRCOG shall make reasonable efforts to verify that individuals who decide to opt out of any use of their PHI is documented appropriately and honored by DRCOG employees or its business associates

No authorization is required in the following situations:

- When communications are directed at an entire population (not to a targeted individual) that promote health or services in a general manner and do not endorse a specific product or service
- When PHI is not disclosed in a marketing communication (such as a newspaper advertisement)

In the event a planned marketing activity involves payment to DRCOG (e.g., cash, referral, gifts, etc.), anti-kickback, inducement, self-referral and general fraud and abuse statutes and regulations may apply. These must be considered prior to implementation of the marketing activity.

Business associates and other third parties:

- DRCOG may engage a marketing firm to conduct permitted marketing activities on DRCOG's behalf. If the marketing activities require the use or disclosure of PHI to the marketing firm, then a business associate relationship would exist, and a BAA is required
- DRCOG may not sell or disclose PHI to a third party to help the third-party market its own products or services without a signed authorization from the client

22.2 Using PHI for Fundraising - Procedure

When fundraising for its own benefit, DRCOG may use or disclose without authorization the following PHI to a Business Associate, a foundation, or consultant to act on DRCOG's behalf:

- Demographic information relating to an individual
- Dates of service provided to an individual
- DRCOG's Notice of Privacy Practices shall inform the client that PHI may be released to raise funds for DRCOG and that the client may opt out of receiving any fundraising communications

Any fundraising materials DRCOG or its agent sends to an individual shall describe how the individual may opt out of receiving any further fundraising communications.

If the fundraising is not for DRCOG's benefit or includes more than demographic or dates of service information, an authorization from the individual is required.

DRCOG must make reasonable efforts to verify that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

23.0 Breach Notification Requirements and Investigations - Policy

A privacy or security breach occurs when there has been an acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the information. Depending on the circumstances, a breach may trigger notifications to the persons whose information was breached, the news media, and the Federal government and, in the case of a breach by a business associate, the Covered Entity that is the other party to the Business Associate Agreement. DRCOG will comply with HIPAA breach notification rules in the notification of the proper entities.

23.1 Breach Notification - Procedure

Employees who believe that unauthorized access, use, or disclosure of PHI has occurred must immediately and simultaneously report the circumstances of the suspected breach to their

supervisor, division director, and the HIPAA Compliance Coordinator (or, in the absence of the HIPAA Compliance Coordinator, reports may be made to the Director of Administration and Finance).

- DRCOG employees must report any suspected breach of unsecured PHI to the HIPAA Compliance Coordinator as soon as possible, within 24 hours after knowledge of the incident.

The report of a potential breach must include the following information, to the extent available:

- A brief description of what happened, including the date of the potential breach and the date the suspected breach was discovered
- Who used the PHI without appropriate permission or authorization and/or to whom the information was disclosed without permission or authorization
- A description of the types of and amount of unsecured PHI involved in the breach
- Whether the PHI was secured by encryption, destruction, or other means
- Whether any intermediate steps were taken to mitigate an impermissible use or disclosure
- Whether the PHI that was disclosed was returned prior to being accessed for an improper purpose
- If the PHI was provided to DRCOG under a Business Associate Agreement

The report shall be provided to the HIPAA Compliance Coordinator.

DRCOG maintains an open-door policy regarding compliance with HIPAA. Employees are encouraged to speak with the HIPAA Compliance Coordinator or other appropriate individual regarding any concerns they may have with DRCOG's HIPAA compliance program or initiatives designed to maintain and enhance privacy and security controls. There shall be no retaliation against employees who, in good faith, report any activities he or she believes is a breach of HIPAA.

- Although not guaranteed (depending on the circumstances) anonymity must be maintained whenever possible

Periodic HIPAA training shall be provided so that employees understand their responsibilities in relation to HIPAA policies and procedures. Training opportunities may occur at employee meetings, e-mails, via online training, or informally posting important updates on the office bulletin board.

Failure to report a suspected breach to the HIPAA Compliance Coordinator may result in disciplinary action up to and including termination.

23.2 Investigation of a Reported Breach of Confidentiality - Procedure

The HIPAA Compliance Coordinator shall respond promptly to any security and/or privacy incident.

The HIPAA Compliance Coordinator shall determine if there is a concern regarding a possible violation of HIPAA or DRCOG's policies or procedures related to HIPAA. If the HIPAA Compliance Coordinator determines there is a concern, he/she must notify the Director of Administration and Finance.

If the Director of Administration and Finance determines an investigation is needed, it must begin promptly. The Director of Administration and Finance shall determine who will conduct the investigation.

If, after the investigation, it is found a violation of DRCOG's policy or procedure has occurred, employees conducting the investigation must notify the Director of Administration and Finance.

- The Director of Administration and Finance, in consultation with Human Resources, shall determine what disciplinary actions must be taken. The disciplinary action report documenting the violation must be placed in the employee's personnel file.
- Documentation of findings and final actions from the investigation shall be maintained as a part of DRCOG's Privacy records and retained for six years

The HIPAA Compliance Coordinator shall take or direct appropriate action to address the issues identified through the investigatory process.

The Director of Administration and Finance shall determine whether any external notifications are required and, if so, the specifics of the required notification pursuant to this procedure and Federal and or State HIPAA rules, as well as C.R.S. § 24-73-103.

- HIPAA's breach notification rule requires notification of affected individuals, HHS, and in certain cases, the media, without unreasonable delay following the discovery of a confirmed breach. The default timeline of 60 days as the maximum to provide breach notification was shortened to 30 days by HB18-1128 (codified at C.R.S. §§ 24-73-101 to 103), which requires notification and within 30 calendar days following the determination of a confirmed breach of PI (including medical information), consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of any computerized data system.

Per C.R.S. § 24-73-103, notification of a breach must be made within 30 days following the determination of a breach and may be accomplished by providing written notice to the individual's postal address, by telephone, or by electronic notice (if the primary means of communication is by electronic means), and potentially substitute notice by publication. These procedures are the same as for notification under HIPAA.

The notification must include:

- The date or estimated date or range of the security breach
- Contact information for DRCOG to allow affected persons to inquire about the security breach
- Toll-free numbers, addresses, and websites for consumer reporting agencies and Federal Trade Commission ("FTC") (not relevant for PHI, but still required by statute)
- A statement that the client can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes (again, not exactly relevant for PHI, but likely still required by statute); and
- If a computerized data system's security is involved in the breach and has been restored, the notice must also include directions on how to change passwords, logins, security, and other online account information

DRCOG employees may not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against:

- Any individual for exercising a right or participating in a process provided for in this policy or in the privacy or security regulations under HIPAA
- Any client who:
    - Files a complaint with the Secretary of the Department of Health and Human Services as permitted by the privacy or security regulations
    - Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing conducted by a government enforcement agency
    - Opposes any act or practice made unlawful by the privacy or security regulations under HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the privacy or security regulations under HIPAA or this policy

Any individual who believes that a form of retaliation or intimidation is occurring or has occurred must report the incident to the HIPAA Compliance Coordinator. The HIPAA Compliance Coordinator shall treat such a report as a complaint and investigate it accordingly.

23.3 Access, Use, or Disclosures that do not Constitute a HIPAA Violation or Breach - Procedure

The policy and procedures outlined in this section do not apply when an individual exercises his/her right to:

- File a complaint with the Office of Civil Rights, U.S. Department of Health and Human Services pursuant to the HIPAA regulations or to the Colorado Attorney General's Office, pursuant to PHI data protection
- Oppose any act made unlawful by the Privacy or Security rules; provided the individual has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy and Security rules
- Disclose PHI as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options regarding the whistleblower activity provided the individual in good faith believes DRCOG has acted unlawfully
- The individual is the victim of a crime and discloses PHI to a law enforcement Officer, provided that the PHI is about a suspected perpetrator of the criminal act; and is limited to the information allowed under Federal law

24.0 Sanctions for Failure to Comply with HIPAA - Policy

Employees must report coworkers who violate HIPAA Privacy and Security Rules. Employees who violate HIPAA Privacy and Security rules may be subject to disciplinary actions up to, and including, termination of employment or the relationship with DRCOG.

24.1 Determining Sanctions for Employees - Procedure

The sanctions imposed depends on a variety of factors, including, but not limited to, the severity of the violation, whether it was intentional or unintentional, and whether the violation indicates a pattern of improper use, disclosure, or release of PHI, and/or misuse of computing resources.

The degree of discipline may range from a verbal warning up to and including termination of the employment or the relationship with DRCOG and/or restitution in accordance with DRCOG policies. The following three levels of violations shall be utilized in recommending the disciplinary action and/or corrective action to apply:

- *Level 1*: An individual inadvertently or mistakenly accesses PHI that he/she had no need to know to carry out his/her responsibilities for DRCOG, or carelessly accesses or discloses information to which he/she has authorized access. Examples of level 1 HIPAA violations include, but are not limited to, the following:
    - Leaving PHI in a public area
    - Mistakenly sending e-mails or faxes containing PHI to the wrong recipient
    - Discussing PHI in public areas where it can be overhead, such as elevators, cafeteria, restaurants, hallways, etc.
    - Leaving a computer accessible and unattended with unsecured PHI
    - Loss of an unencrypted electronic device containing unsecured PHI
    - Improperly disposes of PHI in violation of DRCOG policy

    - An individual fails to report that his/her password has been potentially compromised (e.g., has responded to e-mail spam and given out their password)
- *Level 2*: An individual intentionally accesses, uses and/or discloses PHI without appropriate authorization. Examples of level 2 HIPAA violations include, but are not limited to, the following:
    - Intentional, unauthorized access to their own, friends, relatives, coworkers, public personalities, or other individual's PHI (including searching for an address or phone number)
    - Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual a username and password to access ePHI.
    - Disclosing client condition, status, or other PHI obtained as an employee to a co-worker who does not have a legitimate need to know
    - Obtaining PHI under false pretenses
    - Failure to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access, or use of PHI
    - Failure to promptly report any violation of DRCOG's privacy or security policy or procedure or to the HIPAA Compliance Coordinator
    - Logging into the DRCOG network resources and allow another individual to access PHI
    - Second occurrence of any level 1 violation (it does not have to be the same offense)
- *Level 3*: An individual intentionally uses, accesses, and/or discloses PHI without any authorization for personal or financial gain; causes physical or emotional harm to another person; or causes reputational or financial harm to the institution. Examples of level 3 HIPAA violations include, but are not limited to, the following:
    - Unauthorized intentional disclosure and/or delivery of PHI to anyone
    - Intentionally assisting another individual to gain unauthorized access to PHI to cause harm. This includes, but is not limited to, giving another individual your unique username and password to access ePHI.
    - Accessing or using PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute)
    - Disclosing PHI for financial or other personal gain
    - Uses, accesses or discloses PHI that results in personal, financial or reputational harm or embarrassment to the client
    - Second occurrence of any level 2 violation (it does not have to be the same offense) or multiple occurrences of any level 1 violation

Human Resources must document the sanctions that are applied, if any. This documentation must be kept in written or electronic form for six years after the date of its creation or the date when it is last in effect, whichever is later.

24.2 Determining Sanctions for Business Associates - Procedure

Any level of breach by the business associate and/or its employees or agents shall be addressed by DRCOG in accordance with the terms of the BAA currently in effect at the time of the breach.

Prior to DRCOG disclosing any ePHI to a business associate or allowing a business associate to create or receive ePHI on its behalf, DRCOG obtains assurances from the business associate that the business associate will appropriately safeguard the ePHI disclosed to it or that it creates or receives on DRCOG's behalf. The satisfactory assurance shall be through a written contract with the business associate that contains at least the provisions required by the Privacy and Security Rules.

However, if the business associate is required by law to perform a function or activity on behalf of DRCOG or to provide a service described in the HIPAA Privacy Rule's definition of a business associate

to DRCOG, DRCOG may disclose ePHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements for business associates, provided:

- DRCOG attempts in good faith to obtain satisfactory assurances, as stated above
- If that attempt fails, the Director of Administration and Finance documents the attempt and the reasons the assurances cannot be obtained

25.0 Retention of PHI - Policy

The HIPAA Privacy Rule indicates that PHI, including medical and financial records contained in the master record, must be retained for a minimum of six years from the end of the contract.

25.1 Retention of PHI Procedures - Procedure

If Colorado State laws and regulations require a greater retention time, the greater should be followed. DRCOG must review State laws and regulations to determine master record retention period and "legal age."

In instances whereby, non-PHI (administrative records) is maintained for case management business and operations roles, it must be maintained in accordance with State and Federal laws, as well as DRCOG's record retention schedule.

DRCOG must store the records until the retention period has expired. Records must be stored in a secure manner. The records must be protected from unauthorized access and accidental/wrong destruction.

At the expiration of the retention period, the master records must be destroyed. Records must be destroyed annually in accordance with the retention time frames.

Master records on which there may be pending litigation may be exempt from scheduled destruction at the discretion of DRCOG.

26.0 Destruction of PHI - Policy

PHI maintained in paper format must be destroyed at the end of the retention period utilizing an acceptable method of destruction. Documentation that is not part of the master record and must not become part of the master record (e.g., draft or working documents, shadow charts or files, unofficial notes, etc.) must be destroyed when it is no longer needed by shredding or by placing the information in a secure recycling bin to await shredding.

Prior to the disposal of any computer equipment, including donation, sale, or destruction, DRCOG IT staff must securely wipe the computer's storage device (HDD, SSD, etc.).

26.1 Destruction of PHI in Paper Documents - Procedure

Proper destruction of PHI paper documents shall follow the procedures outlined in the *DRCOG Records Retention Schedule* document.

26.2 Destruction of ePHI – Procedure

Workstations and servers use hard drives and solid-state drives to store a wide variety of information. PHI may be stored in many areas on a computer drive. For example, health information may be stored in "folders" specifically designated for storage of this type of information, in temporary storage areas, and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data.

- To make certain that the PHI of clients has been removed, the HIPAA Compliance Coordinator must ensure IT uses a software program/utility that securely overwrites the entire disk drive.
- If the computer is being re-deployed internally or disposed of, the software program/utility must be run against the computer's hard drive, after which the hard drive may be reformatted, and a standard software image loaded on the reformatted drive.
- If the computer is being disposed of due to damage and it is not possible to run the software program/utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser.
- CDs and diskettes containing PHI must be cut into pieces or pulverized before disposal.
- The process to securely delete ePHI is found in the *Data Destruction Procedure* document.

If a service is used for disposal of ePHI, the vendor must provide a certificate indicating the following:

- Computers and media that were decommissioned have been disposed of in accordance with environmental regulations.
- Data stored on the decommissioned computer and/or media was erased or destroyed per the previously stated method(s) prior to disposal.

27.0 Maintaining Security of ePHI - Policy

DRCOG implements procedures to protect ePHI and for controlling access to ePHI.

DRCOG implements a formal, detailed, approved policy to establish encryption and decryption procedures.

DRCOG implements a mechanism to encrypt and decrypt ePHI wherever it is stored.

27.1 Maintaining the Security of ePHI - Procedure

HR must perform a background check on each employee, intern, and volunteer prior to being hired. The background check must include a check of references and a criminal background check.

The process to encrypt and decrypt ePHI is found in the *Encrypt, Decrypt, and Secure Delete Procedure* document.

The process to gain access to ePHI is found in the *User Access Control Procedure* document.

Employees must receive training on the HIPAA Privacy Rule in accordance with established training schedules.

Employees who access or attempt to access ePHI without authorization are subject to the same sanctions listed in the section *Sanctions for Failure to Comply with HIPAA*.

When an employee changes positions within DRCOG or for some other reason the need for access to ePHI changes, the employee's supervisor must follow the process covered in the *User Access Control Procedure* document.

When an employee, intern or volunteer's employment or position with DRCOG is terminated, HR must follow their documented process for termination.

When HR notifies IT of the termination, IT follows the process covered in the *IT Termination Procedure* document.

27.2 Reporting Unauthorized Use of ePHI - Procedure

Employees who believe unauthorized access, use, or disclosure of ePHI has occurred must immediately and simultaneously report the circumstances of the suspected breach to their supervisor

and the HIPAA Compliance Coordinator. Employees must also report if they suspect a security incident may be imminent.

- DRCOG employees must report any suspected breach of unsecured ePHI to the HIPAA Compliance Coordinator as soon as possible, within 48 hours after knowledge of the incident.

Upon detection of a security incident, the HIPAA Compliance Coordinator must ask IT to immediately begin efforts to determine the nature, scope, and source of the incident. The HIPAA Compliance Coordinator must also endeavor to determine the potential harm from the incident including information at risk and the level of risk presented.

The HIPAA Compliance Coordinator must work with division directors to determine parameters for containment. These parameters must be used by the HIPAA Compliance Coordinator to determine when to begin containment procedures. Once the HIPAA Compliance Coordinator has determined the nature and scope of the incident, this information must be used, in conjunction with the containment parameters, to determine an appropriate containment strategy and when that strategy must be implemented.

- Once the HIPAA Compliance Coordinator determines that containment must begin, the IT Manager or designee must immediately take steps to isolate those systems that have been affected or compromised by the incident from the rest of DRCOG's information systems. The affected or compromised systems must remain isolated until the incident is resolved.
- Upon the identification of a security incident, the IT Manager or designee must begin eradication procedures as soon as possible.

After the HIPAA Compliance Coordinator is certain that the security incident has been resolved, the HIPAA Compliance Coordinator must investigate whether ePHI was lost or altered during the incident. If the HIPAA Compliance Coordinator determines ePHI was lost or damaged, the HIPAA Compliance Coordinator must determine the extent of loss or alteration to ePHI and must restore lost or damaged information.

- If the HIPAA Compliance Coordinator determines ePHI was disclosed during the incident, the HIPAA Compliance Coordinator must verify that the information regarding the disclosure is handled in accordance with DRCOG's HIPAA Breach Notification Rule.
- The HIPAA Compliance Coordinator must take steps to mitigate the harm from the security incident by following DRCOG's mitigation procedures.

The HIPAA Compliance Coordinator must document, in written or electronic form, any security incidents and their outcomes.

- This documentation must include:
    - The date of the incident
    - Extent of the incident
    - Duration of the incident
    - Response to the incident
    - Any other pertinent information the HIPAA Compliance Coordinator determines is necessary for future reference or reporting requirement
- The HIPAA Compliance Coordinator must verify that documentation of any security incident is maintained for six years from the date of the incident.

27.3 Emergency Preparedness - Procedure

DRCOG must take reasonable steps to protect the confidentiality, availability, and integrity of ePHI and other confidential information during an emergency or negative event.

DRCOG must create and maintain a business continuity plan for its IT systems that contain ePHI to be used when an emergency or other unanticipated event disrupts its IT system's functionality. The business continuity plan must establish the criticality of each IT system that contains ePHI.

- The IT Manager must be responsible for implementing procedures to restore any lost data from copies created and stored pursuant to DRCOG's Data Backup Plan.

The IT Manager must be responsible for putting into place procedures designed to verify the continuing operation of those business processes that are critical to protecting the security of ePHI during and immediately after a crisis.

28.0 Physical Safeguards to Maintain the Security of ePHI - Policy

DRCOG implements policies and procedures for the use of physical safeguards in protecting ePHI and for controlling access to ePHI.

28.1 Physical Safeguards - Procedure

DRCOG must implement procedures to make certain unauthorized physical access to its electronic information systems and the locations in which they are housed is limited, while ensuring that properly authorized access is allowed.

- Unauthorized employees who access ePHI or areas where ePHI may be accessed without being properly authorized pursuant to this procedure must be subject to sanctions listed in the section *Sanctions for Failure to Comply with HIPAA*.
- The Director of Administration and Finance must implement procedures to control and validate individuals' access to the DRCOG facility based on their role or function. These procedures must also include visitor control.

DRCOG must implement physical measures designed to protect its information systems and locations from natural disasters and environmental hazards.

- DRCOG must establish procedures that in the event of an emergency allow employees to access its facility in support of restoration of lost data under DRCOG's business continuity plan.

28.2 Computer Hardware Asset Tracking - Procedure

DRCOG's IT department must maintain an accurate inventory of computer and computer-related hardware in use at DRCOG. The IT Manager or designee must update the inventory whenever new equipment is added or old equipment is removed.

28.3 Removal of ePHI from Computer Hardware/Media - Procedure

ePHI must be removed from computer hardware and other electronic media prior to disposal or donation to another entity.

Computer storage devices must be securely erased prior to sale, donation, or disposal. The DRCOG document, *Data Destruction Procedure*, must be used to securely erase the device.

In some situations, DRCOG stores ePHI on removable magnetic storage media (such as external hard drives) or optical storage media (such as CDs or DVDs). When DRCOG determines it is appropriate to dispose of this media, IT must verify that the data is either securely erased or is rendered physically unusable prior to disposal per the *Data Destruction Procedure* document.

In some situations, DRCOG stores ePHI on flash drive media. When DRCOG determines that it is appropriate to dispose of these flash drives, IT must verify that the drives are erased using the *Data Destruction Procedure* document.

29.0 Technical Safeguards to Maintain the Security of ePHI - Policy

DRCOG implements policies and procedures for the use of technical safeguards in protecting ePHI and for controlling access to ePHI.

29.1 Establishing Authorized Users of DRCOG's Network - Procedure

HR must notify the IT Department when a new employee has been hired and needs a login account.

Upon request, the IT Department must create a unique user login account per the *User Access Control Procedure* document.

29.2 Safeguarding ePHI and DRCOG's Network when using E-mail - Procedure

When using e-mail, employees must adhere to the guidelines covered in the *Acceptable Computer Use Policy* document.

When using e-mail to send ePHI, employees must adhere to the guidelines covered in the *How to Send Encrypted E-mail in Office 365* user guide.

DRCOG must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

29.3 Safeguarding ePHI and DRCOG's Network when using the Internet - Procedure

When using the Internet, employees must adhere to the guidelines covered in the *Acceptable Computer Use Policy* document.

When an employee is away from the DRCOG office and needs to access the Internet with their laptop, the employee may use a DRCOG provided device such as a hotspot on a smartphone or a personal cellular data device.

The IT Manager ensures the DRCOG network as well as ePHI is secure via the *IT Threat Prevention Procedure* document.

29.4 Safeguarding ePHI and DRCOG's Network through Anti-Virus Software - Procedure

The IT Manager ensures effective anti-virus software is installed on all DRCOG computers via the *IT Threat Prevention Procedure* document.

29.5 Safeguarding ePHI and DRCOG's Network through Settings on Workstations - Procedure

The IT Manager ensures secure and effective access settings on each DRCOG workstation via the *User Access Control Procedure* document.

The workstation must be configured to automatically lock after 15 minutes of inactivity. Additionally, the user must manually lock the workstation when leaving the workstation unattended.

Employees must not store files containing ePHI on their workstations. Instead, files must be saved to a DRCOG-approved HIPAA compliant storage device. Employees may save files containing ePHI to their portable workstations provided the files are encrypted. If necessary, files containing ePHI may also be saved temporarily to an encrypted flash drive. However, such files must be saved to an appropriate storage device when the employee returns to the office.

29.6 Risk Assessment

The HIPAA Compliance Coordinator must schedule regular 3rd party risk assessments. Such assessments must be performed annually, at a minimum.

29.7 Auditing and Emergency Access - Procedure

The IT Manager ensures effective monitoring and auditing of DRCOG information systems containing or using ePHI files via the *WorkDocs Monitoring and Auditing Procedure* document.

The IT Manager ensures an effective process for obtaining necessary ePHI files during an emergency via the *DRCOG Business Continuity Plan* document.

30.0 Transportation and Storage of PHI - 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. All PHI in paper or electronic form must be transported and stored in a secure manner to safeguard it against improper disclosure or loss. PHI will be transported and stored outside secure network sites and servers only when necessary. Only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure must be transported. All PHI in paper or electronic form must be transported and stored in a secure manner to safeguard it against improper disclosure or loss.

30.1 Transportation and Storage of PHI - Procedure

If it is necessary to transport physical PHI or ePHI in a motor vehicle, the following precautions will be applied:

- Employees who transport PHI must be aware motor vehicle accidents can occur which can provide unauthorized access to items within the vehicle.
- In addition, motor vehicles can be broken into. In such circumstances PHI could be accessed by unauthorized individuals. Precautions must be taken to prevent or minimize the possibility that PHI will be compromised.
- Physical PHI transported in a motor vehicle must be maintained during transport in a locked container, briefcase, or bag that is approved by the HIPAA Compliance Coordinator. The locked container must be placed in the trunk or another part of the vehicle that is not visible from outside the vehicle.
- The employee must be physically present in the vehicle while PHI is in the vehicle.
- Employees shall only transport the minimum PHI necessary to perform their job duties.

If it is necessary to store physical PHI or ePHI outside a secure location, the PHI must be placed in a secure, locked file cabinet or other locked container. Every effort must be made to keep PHI secured from access by family members and others.

If PHI is lost or stolen, or improperly accessed by others, the employee must notify the HIPAA Compliance Coordinator and file a police report if the improper access involved theft.

Employees who violate this policy are subject to disciplinary action up to and including termination of employment or contractual relationship. Violations must be reported by the employee's immediate supervisor as soon as possible regardless of whether PHI has been compromised.

31.0 Acknowledgement of Receipt

ACKNOWLEDGMENT OF RECEIPT

I have received a copy of the *DRCOG HIPAA Policy and Procedure Manual* ("HIPAA Policy"). I understand and agree that I am to become familiar with its contents. Further, I understand and agree as follows:

- State and Federal law mandates the non-disclosure and other special treatment of Protected Health Information (PHI) and Personal Information (PI) by covered entities, including DRCOG and its employees, volunteers, vendors, and other partners.
- The policies and information described in the HIPAA Policy are subject to future changes in federal or state law.
- That I have had an opportunity to ask questions related to the HIPAA Policy.
- I understand that I have a duty under State and Federal law, as well as this HIPAA Policy, to maintain the privacy of our clients by keeping their PHI confidential and taking necessary steps to protect the information from disclosure to unauthorized persons.

_____ _____

Print Employee Name Date

_____ _____

Employee Signature Date

32.0 Frequently Asked Questions

What is PHI?

PHI is defined as information that is a subset of health information, including demographic data, that relates to: (1) the individual's past, present or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual, AND that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

If a client sends info unencrypted, is it then okay for staff to also respond unencrypted?

No. If DRCOG's response also includes PHI then the response needs to be encrypted per DRCOG's BAA with the State. The BAA states that DRCOG "*shall not transmit PHI over the internet or any other insecure or open communication channel unless the PHI is encrypted or otherwise safeguarded with a FIPS-compliant encryption algorithm.*"

If DRCOG's response does not include PHI, then the encryption requirement does not apply. Encryption is not mandated by HIPAA although it is considered an addressable implementation specification that should be implemented if, after a risk assessment, the entity has determined the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity, and availability of ePHI. In situations where you are corresponding with an elderly client who is not familiar with encryption software then it seems like encryption may not always be "*reasonable and approximate*."

Does the State take a stand on verbal consent to sharing information?

I do not see anything in DRCOG's BAA with the State that addresses verbal consent. Instead, the BAA refers to the HIPAA rules. HIPAA allows verbal consent in certain circumstances, including disclosures of PHI to family members, close personal friends, or any other persons identified by the individual if the disclosure is directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. However, I agree with the attorney you spoke with that written consent should be obtained if it all possible.

Is it allowable for case managers to share PHI if they need to report abuse, neglect, etc.?

Generally, yes. 45 CFR 164.51(c) states:

> (1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity **may disclose protected health information about an individual whom the covered entity 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:
>
> > (i) To the extent the disclosure is **required by law** and the disclosure complies with and is limited to the relevant requirements of such law;
> >
> > (ii) If the **individual agrees** to the disclosure; or
> >
> > (iii) To the extent the disclosure is **expressly authorized by statute or regulation** and:
> >
> > (A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
> >
> > (B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

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

Can information be shared with another entity we have a BAA with, or do we always need the consent of the client?

So long as the PHI is being shared for the purpose of treatment, payment, or healthcare operations then the patient's written authorization is not required to share PHI with a business associate who has entered into a BAA with DRCOG.

When do we need to give out the notice of privacy to clients?

The notice of privacy practices must be: (1) provided to any person who requests a copy; and (2) prominently posted on the covered entity's website. The notice can be provided via regular mail or by email if the person agrees to electronic notice. 45 CRF § 164.520. There are additional specific notice requirements for health plans and health care providers that have a direct treatment relationship with an individual, but those do not appear to apply to DRCOG.

You asked whether the privacy notice is required when someone calls the Information and Assistance line for referral to a service. Unless the individual specifically requests a copy of DRCOG's privacy practices then I agree you're not required to provide the individual a copy. You also asked about a situation where the employee starts collecting information and forming a "*file*" for the person. Again, I don't believe DRCOG is legally required to provide a copy unless the individual requests a copy.

33.0 Revision History

Date	Revision	Description	Author
04-16-2018	0.01	Initial draft	Tim Feld
11-14-2018	0.02	Updates based on comments from SecurityMetrics	Tim Feld
11-15-2018	0.03	Added referenced documents	Tim Feld
01-10-2019	0.04	Updates based on comments from Kelly law firm	Tim Feld
04-02-2019	0.05	Updates based on comments from Jenny D. and Roxie R.	Tim Feld
03-06-2023	0.06	Added Forms index	Tim Feld
03-17-2023	0.07	Added FAQ section	Tim Feld
04-26-2023	0.08	Edits to section 13	Tim Feld
05-01-2023	1.00	Released	Tim Feld
08-10-2023	1.01	Added annual HIPAA training	Tim Feld