HIPAA
Privacy and Security Policies and Procedures Manual

A. General Policy Statement

Diversus Health 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 to protected health information (PHI) created, acquired, maintained or disclosed by Diversus Health employees, subcontractors, business associates, vendors, volunteers and interns. All individuals representing Diversus Health will take responsibility for safeguarding protected health information to which they have access.

US Department of Health and Human Services (HHS) 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, healthcare clearinghouses and healthcare providers who conduct the standard healthcare transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004 for small health plans).

HHS 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. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

B. 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 of an individual's health information in the provision of patient care. However, access to PHI by the workforce must be limited based on job scope and the need for the information.

C. 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.

Health Insurance Portability and Accountability Act (HIPAA)
Privacy and Security Rule Procedures

Table of Contents

Policy: HIPAA-8010

TITLE: HIPAA Compliance/Privacy and Security

POLICY

Diversus Health complies with the Federal Health Insurance Portability and Accountability Act of 1996 (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). The confidentiality of Protected Health Information (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 Diversus Health, a healthcare provider, health plan employer or healthcare clearinghouse; and,
- 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 afforded the same rights. Legal guardians and personal representatives may also be afforded 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, Diversus Health will change its privacy and security policies and procedures as necessary and appropriate.

These policies should 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 should control.

IDENTIFICATION OF PRIVACY OFFICER PROCEDURES:

A. Diversus Health has appointed a Privacy Officer who:

1. Oversees the development, implementation, maintenance and revision of policies and procedures to protect confidential health information in accordance with Federal and State regulations. The Privacy Officer notifies Leadership of any policies, procedures or implementation issues that need their review.
2. Performs periodic Privacy Rule focused risk assessments to identify issues that need attention.
3. Implements staff training on HIPAA policies, procedures and practices.
4. Monitors participants to ensure that all staff receives HIPAA training as described in Policy 102.1.
5. Maintains updated Notice of Privacy Practices that is distributed in accordance with these procedures.
6. Addresses any disclosures of information, including the preparation and maintenance of mandatory reporting, that fall outside the normal course of disclosures.
7. Investigates and responds to complaints regarding the confidentiality of information.

8. Assures privacy and security forms are updated and available on the Diversus Health intranet and in the electronic health record (EHR) as appropriate.

IDENTIFICATION OF SECURITY OFFICER PROCEDURES:

A. Diversus Health has designated a Security Officer who:

1. Oversees the development, implementation, maintenance and revision of policies and procedures to protect confidential health information in accordance with Federal and State regulations.
2. Assists with the implementation of staff training on HIPAA policies, procedures and practices.
3. Oversees procedures designed to prevent, detect, contain, and correct any security violations.
4. Maintains written or electronic copies of documentation related to communications, actions, activities, security measures or designations required by these policies and procedures or the Security Rule for a period of six (6) years from the date of its creation or the date when it last was in effect, whichever is later.
5. Develop a risk management plan that contains measures for:
    a. Conducting an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by Diversus Health; this risk analysis should be maintained in either written or electronic form for six (6) years from the date it was created or superseded by a newer analysis, whichever is later;
    b. Reducing the exposure to identified risks, including use of firewalls, anti-virus software, updated or new policies and procedures, or additional or advanced training.
    c. Implement security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level; and,
    d. If appropriate, the risk management plan should be revised and improved based on results of periodic risk assessment.
6. The Security Officer should ensure that system security log information is regularly reviewed by the appropriately trained IT staff in order to identify any irregular network activities, including the possible misuse of PHI.

DISCLAIMER

These privacy and security policies, as they exist or may be amended in the future, are intended to be used by Diversus Health employees, subcontractors, interns, volunteers, providers, board of directors or its agents in meeting their responsibilities to Diversus Health. Violation of a policy can be the basis for discipline up to and including termination of employment or an association with Diversus Health. Because these privacy and security 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 Diversus Health, its staff, interns, volunteers, providers, board of directors or its agents to another person.

REFERENCE:

- 45 CFR §164.308 and 45 CFR §164.316
- 45 CFR §164.501 (1) and 45 CFR §164.530(a)

Policy: HIPAA-8020

TITLE: DEFINITIONS – HIPAA Privacy and Security

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. Employees,

subcontractors, interns, volunteers, providers, or other persons affiliated with Diversus Health should consult with the Privacy or Security Officer if they have any questions.

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. (Security)

Amend/Amendment: An amendment to PHI should 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 person served 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 Diversus Health 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 persons served. 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): A contract between a covered entity and a business associate, or between a business associate and its business associate subcontractor, that should:

- Establish the permitted and required uses and disclosures of PHI by the business associate.
- Provide that the business associate should 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 should abide by the same restrictions and conditions, make PHI available to individuals and make its records available to U.S. Department of Health and Human Services (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 contract.

CMS: Centers for Medicare and Medicaid Services – The agency that regulates and enforces Federal Regulations for Medicare in long term care and other healthcare entities.

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 protected health information except to carry out treatment, payment or healthcare operations. Consent is not required under the privacy rule for these activities.

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 person served.

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 Diversus Health that is:

- The medical records and billing records about individuals maintained by or for Diversus Health; or,
- Used, in whole or in part, by or for Diversus Health 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 Diversus Health.

Disaster Recovery Plan (DRP): 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.

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

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

Electronic Media: Includes 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 (wide-open), extranet or intranet (using Internet technology to link a business with information accessible only to collaborating parties), 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 person served 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 in an effort 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, emotional or mental condition or functional status of an individual or that affects the structure or function of the body; and,
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Healthcare Operations: Any of the following activities of Diversus Health 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 patients 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; and,
- Business management and general administrative activities of Diversus Health, 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 Diversus Health with another covered entity, or an entity that following such activity should become a covered entity and due diligence related to such activity; and,
    - 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 Diversus Health, 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, 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.

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; and
- Relates to the past, present or future physical or mental health or condition of an individual, and
    - Identifies the individual or
    - 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 has 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 the purpose of 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 a particular 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 in the course of 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 person served care services, for reviewing person served 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 Protected Health Information needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of Protected Health Information 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 person served with information about their rights under the Privacy Rule and how Diversus Health generally uses their Protected Health Information.

Office of Civil Rights: 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 nondiscrimination and health information privacy laws including HIPAA. (www.hhs.gov/hipaa)

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

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 Diversus Health.

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

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 Breach: A violation of one's responsibility to follow privacy policy and procedure that results in the PHI of a person served being accessed by unauthorized persons.

Privacy Officer: Diversus Health staff member who has been designated, pursuant to the Privacy Rule, with responsibility for ensuring Diversus Health compliance with the Privacy Rule.

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 Diversus Health that is individually identifiable except: (a) employment records held by Diversus Health in its role as an employer; and, (b) information regarding a person who has been deceased. Protected health information 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 health-care provider, health plan, employer or health-care clearinghouse; and,
- 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; and,
    - That identifies the individual; or
    - There is a reasonable basis to believe the information can be used to identify the individual.

All health information maintained by Diversus Health 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 are not a part of the formal medical record and should be kept separate from the record of the person served.

Qualified Protective Order: A legal command intended to protect a person or thing from an unfair or unjust action.

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

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 person served and should 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 staff and individuals and third-party entities doing business with the organization. Also known as a security assessment.

Risk Management: Management's identification, analyses and, when necessary, response to risks that might adversely affect realization of Diversus Health business objectives in its capacity as a business associate of its clients.

Safeguarding: To make certain safekeeping of Protected Health Information for the person served.

Screen Saver: Any software program designed to, after a certain period of inactivity, display on a workstation monitor a random display of patterns, images, or to simply make the monitor blank so as to prevent an image from being burnt into the monitor.

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 Officer: 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.

Security Rule: The Federal privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that created national standards to protect electronic medical records. (42 U.S.C. § 1320d, 45 C.F.R. parts 160 and 164, as amended)

Subcontractor: A person or entity who acts on behalf of Diversus Health.

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. There are two (2) kinds of subpoenas:

- ***Duces tecum:*** A request for witnesses to appear and bring specified documents and other tangible items. The subpoena duces tecum requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.
- ***General subpoena (a.k.a. ad testificandum):*** A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

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

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

Treatment, Payment and Operations (TPO): The Privacy Rule allows sharing of information for purposes of treatment, payment and healthcare operations. Treatment includes use of person served information for providing continuing services. Payment includes sharing of information to bill for provision of services to the person served. Healthcare operations are certain administrative, financial, legal, and quality improvement activities that are necessary for Diversus Health to run its business and to support the core functions of treatment and payment.

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

User: A person or entity with authorized access.

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

Workforce: Staff, volunteers, trainees and other persons whose conduct, in the performance of work for Diversus Health, is under the direct control of Diversus Health, whether or not they are paid. Members of the workforce are not business associates.

REFERENCE:

- 42 CFR §160.103

Policy: HIPAA-8030

TITLE: HIPAA Privacy and Security Rule Training

POLICY:

Diversus Health provides HIPAA privacy and security training to employees, subcontractors, interns and volunteers who should encounter PHI while performing their job functions.

PROCEDURES FOR HIPAA PRIVACY AND SECURITY RULE TRAINING:

A. The Privacy and Security Officer, in concert with Learning & Development staff, implement privacy and security training course(s).

B. Diversus Health staff, interns, subcontractors and volunteers should be trained or retrained.
1. Within 30 days of employment or contracting with Diversus Health.
2. Within two (2) months after a material change in privacy policies becomes effective, when their job duties are affected by the change.
3. Within 30 days of the Privacy Officer or Security Officer determining they have disregarded privacy laws, policies or procedures.
4. Annually thereafter

C. Learning & Development staff should document each training session and the names of Diversus Health staff that completed the training. Such documentation will be maintained in Diversus Health's Learning Management System maintained by the Learning & Development Department. The supervisors of interns and volunteers should document their HIPAA training when it occurs.

D. Discipline for Non-Compliance: Human Resources (HR) and Learning & Development should implement the same procedures to discipline and hold Diversus Health staff, interns or volunteers accountable for completing HIPAA training, as with other trainings conditional for employment.

E. In the event of a material change in Diversus Health Privacy or Security policies or procedures, or in the HIPAA Privacy or Security Regulations, the Privacy and Security Officer should work with Learning & Development to retrain staff, interns and volunteers who would be affected by those changes. This additional training should occur within 60 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, should apply.

F. Employees, subcontractors, interns and volunteers should be trained to recognize and respond to a breach of unsecured PHI and to understand the consequences of a security breach.
1. If Diversus Health employees, subcontractors, interns or volunteers are involved in a privacy or security incident that was not the result of malicious or willful conduct, the offending individual should receive additional training regarding Diversus Health privacy and security policies and procedures. This training should focus on the areas directly related to the incident and should be designed to prevent a recurrence of the incident.

G. In the event of a privacy or security incident, a training reminder should be issued to employees, subcontractors, interns and volunteers that focus on the privacy/security issue involved in the incident and how to avoid it in the future. If the Privacy or Security Officer becomes aware of recurring security lapses, a reminder should be issued to employees, subcontractors, interns and volunteers regarding the lapse and the appropriate way to handle the issue in light of Diversus Health policies and procedures.

H. In order to safeguard ongoing privacy compliance and information security, the Privacy or Security Officer (or their designees) may provide periodic privacy or security reminders to Diversus Health employees, subcontractors, interns or volunteers. These reminders should be provided on an as needed basis. The reminders should be provided by email or presentation at staff meetings and should focus on practical privacy or security issues, such as handling passwords, dealing with email attachments, releasing information, etc.

I. Diversus Health maintains the documentation of its training of its employees, subcontractors, interns and volunteers for a period of seven (7) years.

REFERENCE:

- 45 CFR §164.308(a)(5)
- 42 CFR §164.530

Policy: HIPAA-8040
TITLE: Notice of Privacy Practices

POLICY:

Diversus Health provides a copy of the Notice of Privacy Practices to persons applying for services, their parent (if a minor), legal guardian and personal representative at the time an application for services is being made. These individuals are also notified when the notice of privacy practices changes. Diversus Health requests that each person receiving a copy of the Notice of Privacy Practices at the time of application acknowledges his/her receipt in writing.

NOTICE OF PRIVACY PRACTICES PROCEDURES:

A. The Notice of Privacy Practices should comply with HIPAA rules and regulations. The Notice of Privacy Practices informs the person applying for or receiving services of:
1. The uses and disclosures of Protected Health Information (PHI) that may be made by Diversus Health;
2. The rights of a person with respect to his/her PHI; and
3. Diversus Health duties in safeguarding such PHI.

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

C. Diversus Health staff should provide the Notice of Privacy Practices to the person applying for services at the time of application.

D. At the time the Notice of Privacy Practices is provided, Diversus Health staff should make a good faith effort to obtain the signature of the person applying for services, the parent of a minor, legal guardian or personal representative on the Notice of Privacy Practices Form. Written acknowledgement should be attached to the person's official record.

E. Diversus Health staff should provide a copy of the written Notice of Privacy Practices to persons served and to other persons upon request.

G. The Privacy Officer should post a copy of the Notice of Privacy Practices in a clear and prominent location such as the entrance lobby at Diversus Health service facilities.

H. I. Whenever the Notice of Privacy Practices is revised, Diversus Health Privacy Officer should make the revised Notice of Privacy Practices available on request on or after the effective date of the revision; and the revised Notice of Privacy Practices should be posted in a clear and prominent location. A copy of each Notice of Privacy Practices issued by Diversus Health should be maintained for at least six years from the date it was last in effect.

J. Any member of the workforce who has knowledge of a violation or potential violation of this procedure should make a report through the Quality Incident Reporting (QIR) system which goes to the Privacy Officer (see the Procedure HIPAA-119 "Breach Notification Requirements")

REFERENCE:

- 42 CFR § 164.520

Policy: HIPAA-8050
TITLE: Designated Record Set

POLICY:

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

DESIGNATED RECORD SET PROCEDURES:

A. If records from other providers are used by Diversus Health to make decisions related to the care and treatment of the person served, then these records are considered part of the designated record set for access by employees, subcontractors, interns and volunteers (if within the scope of their job duties). These records may include, but are not limited to, such documents as history and physical examination forms, discharge summaries and lab results from previous acute care hospitalizations.

B. The designated record set is to be retained according to State and Federal regulations and following Diversus Health retention procedure.

C. Program specific records, which may include active and historical designated records set documentation, are generally maintained by the programs in their administrative locations.

REFERENCE:

- 45 CFR §164.501 (1)

Policy: HIPAA-8060

TITLE: Minimum Necessary Uses and Disclosures of Protected Health
POLICY:

When using or disclosing Protected Health Information (PHI), Diversus Health staff should 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 Diversus Health:

- Diversus Health employees, subcontractors, interns and volunteers should only have access to the amount and type of PHI necessary to carry out their job duties, functions and responsibilities.
- Diversus Health limits access to, and use of, the protected health information of persons served in accordance with its business associate agreements with vendors and providers.
- Diversus Health employees, subcontractors, interns and volunteers should 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 patient.
- When the disclosure is to the person served, their parent (if a minor), legal guardian or legally authorized personal representative.
- When the disclosure is pursuant to a valid authorization requested through the person served or their parent (if a minor), legal guardian or legally authorized personal representative, in which case the disclosure should 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 law requires the disclosure; only PHI required to be disclosed by law should be disclosed.

MINIMUM NECESSARY STANDARD WHEN REQUESTING PHI:

A. When requesting PHI from another entity, Diversus Health should 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, Diversus Health should evaluate the request to determine if the requirements of the Privacy Rule have been satisfied.

REFERENCE:

- 42 CFR § 164.502 (b) (1);
- 42 CFR §164.514 (D)

Policy: HIPAA-8070

TITLE: Safeguarding Verbal and Written Protected Health Information (PHI) and Storing PHI
POLICY:

All employees, subcontractors, business associates, vendors, interns and volunteers are responsible for the privacy and security of PHI of persons receiving services. Diversus Health ensures that uses and disclosure of PHI complies with applicable Federal, State and/or local law or regulation, and these policies.

PROCEDURES FOR SAFEGUARDING VERBAL USE OF PHI:

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

B. During face to face conversations, such measures may include:

1. Conducting meetings in a room with a door that closes, if possible;
2. Keeping voices to a moderate level;
3. Having only staff and others involved in the care of the person served, who have a "need to know" the information, present at the meeting;
4. Limiting the PHI discussed to the minimum amount necessary to accomplish the purpose of the meeting;
5. If in a public area, moving to a private or semi-private area within Diversus Health and lowering the voice to minimize likelihood of inadvertent disclosure.

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

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

PROCEDURES FOR SAFEGUARDING WRITTEN PHI:

A. Documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.

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

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

D. Authorized staff should review the master record at the Records Information Management area workstations unless it is signed out in accordance with Diversus Health procedures.

E. Hardcopy master records should not be left unattended in areas where person served, visitors and unauthorized individuals could easily view the records.

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

PROCEDURES FOR STORING WRITTEN PHI:

A. 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 Medical Records Manager or a designee should monitor storage and security of such hardcopy master records.

B. The Medical Records Manager should identify and document those staff members with keys to the file room and access to stored records. The minimum number of staff necessary to assure that records are secured yet accessible should have keys. Staff members with keys should keep them in a secure place so that they are not accessible to unauthorized individuals.

C. Hardcopy master records should be checked out if removed from the file room. Only authorized persons can check out hardcopy master records.
   1. Use of "shadow" or "working copy" records or files is prohibited.

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

E. If the confidentiality or security of PHI stored in an active or inactive master record has been breached, a QIR should be completed immediately.

REFERENCE:

- 42 CFR §164.530 (C) (1) & (2)

Policy: HIPAA-8080

TITLE: Safeguarding Protected Health Information with Office Equipment and Mobile POLICY:

Diversus Health staff may have access to electronic PHI through web portals or email accounts through office equipment and mobile devices. Care should be taken that the PHI accessed in these instances is safeguarded from unauthorized use, disclosure or access. Staff, interns, subcontractors and volunteers should be familiar with the privacy and security policies and procedures relative to confidentiality of the PHI of persons served and educated about the potential privacy and security risks caused by the theft or loss of computers, tablets, flash drives (thumb drives) or other removable media or memory devices.

PROCEDURES FOR SAFEGUARDING PHI WHEN USING COMPUTERS:

A. Staff, interns, subcontractors and volunteers who need to use computers to accomplish work-related tasks should have access to computer workstations. Access to computer-based PHI should be limited to employees, subcontractors, interns and volunteers who need the information for treatment, payment or healthcare operations.
   1. Staff, interns and volunteers should log off their workstation when leaving the work area.
   2. Staff, interns and volunteers should lock their office doors when they leave their offices for extended periods of time and when they leave at the end of each workday.
   3. Where possible, computer monitors should be positioned so that unauthorized persons cannot easily view information on the screen.
   4. The access privileges of employees, subcontractors, interns and volunteers should be removed promptly following their departure from employment, internship or a contractual relationship.

B. Users of computer equipment should have unique login and passwords.
   1. Passwords should be changed in accordance with Security standards set by the Security Officer.
   2. 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.

C. Only staff that is authorized to access the main server is allowed into the server room/data center. At the end of each business day and during any period where the room is unattended, IT staff should lock the door that provides access to that room. The server should not be left unattended if the room is unlocked.

D. Employees, subcontractors, interns and volunteers should immediately report any violations of this procedure to the Security and/or Privacy Officer, and their Supervisor.

PROCEDURES FOR SAFEGUARDING PHI WHEN USING PRINTERS, COPIERS OR SCANNERS:

A. Diversus Health locates printers, copiers and scanners in areas not easily accessible to unauthorized persons.

B. Authorized employees, subcontractors, interns and volunteers may view documents generated on printers, copiers or scanners. Access to such documents by unauthorized persons is prohibited by Federal law.

C. All printers, copiers, scanners and Fax machines that are expected to process PHI will utilize "secure print" feature that holds the print job until the user releases the job via the console on the printer. This prevents unattended PHI printing as well as documents lying unattended on the device.

D. Documents containing PHI should be printed by the individual and then promptly removed from the printer and or copier/scanners and placed in an appropriate and secure location.

E. Documents containing PHI that should be disposed of due to error in printing should be destroyed by shredding or by placing the document in a secure recycling bin to await shredding.

PRIVACY AND SECURITY PROCEDURES FOR PORTABLE DEVICES AND MEDIA:

A. Employees, subcontractors, interns and volunteers should limit the use of assigned portable computers, smart phones and tablet devices or any Diversus Health provided resource or device that contains or can access client PHI, to Diversus Health staff only.
   1. Diversus Health issued portable devices should have appropriate password, security, and encryption programs installed upon them. Any PHI that is accessed from a mobile device should have adequate full-disk encryption as approved by the Security Officer.
   2. Employees, subcontractors, interns and volunteers should avoid accessing individually identifiable information where it might be seen by persons without a legitimate need to know.
   3. Smart phone users should be sure to close connections to email and other systems/portals that contain PHI immediately when they are finished using the system/portal.
   4. Permanent printed asset tags and device identification number should be installed on all computers (servers, desktops & laptops), tablets and select devices.
   5. If necessary, the Security Officer, or his/her or her designee, provides staff, interns and volunteers with accessories to protect their portable computers and tablets, and requires use of these devices.

B. Employees, subcontractors, interns and volunteers should only log in to systems and portals for which they have authority and properly obtained valid access credentials.

C. Employees, subcontractors, interns and volunteers should not store PHI on flash drives (thumb drives) or other removable media or memory devices unless absolutely necessary and only on devices approved by the Security Officer. When using removable media or memory devices is absolutely necessary, employees, interns or volunteers should:
   1. Ensure that the flash/thumb drive is encrypted.
   2. Keep the flash/thumb 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;
   3. Not leave an external drive or other removable media or memory device attached to a computer. (Many removable drives and media devices are lost because their owners transferred a file to the device for a presentation and then forgot the flash drive at the end of the presentation.)
   4. Not store older documents on removable media; they should be archived to Diversus Health network. Removable media should contain what is needed in the immediate future.

D. The Security Officer (or his/her designee) maintains a current list of Diversus Health issued portable computer and tablet users, assigned equipment serial numbers and software. Diversus Health 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, subcontractors, interns and volunteers should:
   1. Transport portable computers in a car's trunk rather than on a seat, thereby keeping it hidden, and <u>never leave</u> them unattended for any time period, in a vehicle overnight or for an extended period of time;
   2. When traveling by air, do not put any portable computer or tablet in checked baggage. At the TSA checkpoint, place a portable computer or tablet on an airport conveyor belt only when the preceding individual has cleared the metal detector; and
   3. Place unattended portable computers in room safes when leaving a hotel room. Some hotel room safes include an AC adapter so that the computer can be recharged while locked away.

E. Employees, subcontractors, interns and volunteers should secure Diversus Health issued portable computers and tablets when equipment is left unattended in offices and meeting rooms.

F. Privacy and security training should emphasize that flash drives and other removable media and memory devices such as PDAs and 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.
   1. The Security Officer should perform loss investigations on stolen equipment.

REFERENCE:

- 42 CFR §164.530 (C) (1) & (2)

Policy: HIPAA-8090

TITLE: Transmitting Protected Health Information through Email or Fax

POLICY:

While providing services to persons applying for or receiving services, Diversus Health staff, interns, subcontractors and volunteers may communicate PHI via email or facsimile (fax) to persons served, their parent (if a minor), legal guardian, personal representatives or providers of service. Care should be taken that the PHI transmitted in these instances is safeguarded from inappropriate use, disclosure or access.

PROCEDURES FOR TRANSMITTING PHI THROUGH EMAIL:

A. Email users should be set up with a unique identity complete with unique password and file access controls.

B. Email users may not intercept, disclose or assist in intercepting and disclosing email communications.

C. Whether the email is to Diversus Health employees, subcontractors, interns or volunteers, or to persons external to Diversus Health, the amount of PHI disclosed via email correspondence should be limited to the minimum necessary to accurately communicate the needs or situation of the person served.

D. PHI may be sent without additional encryption or protection via email within Diversus Health secured, internal network.

E. When sending PHI outside of the Diversus Health network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information.

1. Diversus Health will employ technology solution(s) to encrypt outgoing emails that contain PHI and/or other sensitive personal information.
2. Diversus Health email that contains PHI that is sent or forwarded to an external email address should be encrypted by pressing the *Encrypt & Send* button in the Outlook. No PHI is to be included on the Subject line that is being sent externally as this is not encrypted.
3. Users should exercise extreme caution when forwarding messages. Sensitive information, including PHI, should not be forwarded to any party outside the agency without using the same security safeguards as specified above.
4. Users should verify the accuracy of the email address before sending any external email containing PHI and, if possible, use email addresses loaded in the system address book.
5. PHI including billing information should always be routed in an encrypted format.
6. Due to the sophistication, availability and ease of use of encryption technology, PHI should never be sent via email in an unencrypted format.

G. Users should periodically purge email messages that are no longer needed for business purposes.

H. Employees, subcontractors, intern and volunteer email access privileges should be removed promptly following their departure from Diversus Health.

I. Unencrypted email messages, regardless of content, at not considered secure and private.

J. Employees, subcontractors, interns and volunteers should immediately report any violation of this guideline to their supervisor.

K. All external email should automatically display a confidentiality statement.

PROCEDURES FOR TRANSMITTING PHI THROUGH FACSIMILE (FAX):

A. Received documents should promptly be removed from the fax machine and, if necessary, forwarded to the appropriate recipient. To promote secure delivery, instructions on the cover page should be followed.

B. Received documents via fax may utilize various technologies including Secure Print and Fax-to-Folder functions. Staff is responsible for understanding the security protections afforded and using appropriately.

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

D. When sending a facsimile document that includes PHI, the PHI disclosed should be the minimum necessary to meet the requestor's needs and/or communicate information about the needs or situation of a person served.

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

1. Pre-programming and testing destination numbers to eliminate errors in transmission due to misdialing.
2. Asking frequent recipients to notify Diversus Health of a fax number change.
3. Confirming the accuracy of the recipient's fax number before pressing the submit function.

F. When transmitting information, a cover page should be attached to any facsimile document that includes PHI. The cover page should include:

1. Destination of the fax, including name, fax number and phone number;
2. Name, fax number and phone number of the sender;
3. Date;
4. Number of pages transmitted; and,
5. Confidentiality Statement (see sample below).

G. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system should be checked to obtain incorrect recipient's fax number. Fax a letter to the receiver and ask that the material be returned or destroyed. A QIR is to be completed regarding this situation.

REFERENCE:

- 42 CFR §164.530

Policy: HIPAA-8100

TITLE: Authorizations to Release Protected Health Information and Disclosure of PHI
POLICY:

When PHI is to be used or disclosed for purposes other than the continuing care of persons receiving services (treatment), payment of services, or the coordination of care and day to day operations or Diversus Health (healthcare operations), Diversus Health should disclose PHI only as appropriately authorized.

EXCEPTIONS TO AUTHORIZATION REQUIREMENTS PROCEDURES:

A. When Diversus Health receives a request for disclosure of PHI, medical records staff should determine whether an authorization is required prior to disclosing the PHI. PHI may be disclosed by medical records staff without an authorization if the disclosure is:

1. For official Diversus Health operations such as for the purpose of:
    a. Treatment; or continuation of services;
    b. Diversus Health payment activities, or the payment activities of the entity receiving the PHI;
2. In limited circumstances, for the healthcare operations of another Covered Entity, if the other Covered Entity has or had a relationship with the person served.
3. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the Privacy Rule.
4. As required by other State or Federal law.
5. An administrative request, subpoena or investigative demand. Diversus Health may disclose the requested PHI if the administrative document itself or a separate written statement recites:
    a. The information sought is relevant to a lawful inquiry;
    b. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry; and,
    c. De-identified information could not be used.
6. A request by a Public Officer, if the officer presents:
    a. 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; or
    b. A request on government letterhead.
    c. 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.
7. If PHI is disclosed to:
    a. Prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or;
    b. Law enforcement authorities to identify or apprehend an individual.

8. PHI should not be used or disclosed in the absence of a valid written authorization if the use or disclosure is:
    a. Of psychotherapy notes as defined by the Privacy Rule; or
    b. For the purpose of marketing; or
    c. For the purpose of fundraising.

PROCEDURES FOR ADMINISTRATIVE AND JUDICIAL REVIW OF INFORMATION RELEASE/WITHHOLDING WHEN REQUESTED:

A. When administrative review is requested, the Clinical Director over the area providing care, in consultation with the Compliance Officer, and Legal Counsel will review the record to understand the decision to withhold or release information.
B. If the Clinical Director is not available or unable to be impartial, a Professional Person will be designated to review the record.
    1. The individual will be interviewed as part of the review process.
C. Documentation of the review of the record/decision will be captured and maintained by the Legal Department.
D. If the individual and/or their attorney object to the decision, they will be provided with the procedures for the administrative review and informed of any decision to withhold or release information before any action is taken to release information. A family member would also be provided information about the procedure for administrative review of a decision to release or withhold information.
E. An individual may file a written request for review by a court of the decision from an administrative review to release information to a family member requested and proposed to be released.
    a. The court shall hear the matter within 10 days after their request.
    b. Unless stated in an order by the court, the individual does not forfeit any legal right or suffer legal disability per 27-65 regulation.
F. Diversus Health will not release information requested until 5 days after the determination upon administrative review of the Director or designee is received by the individual.
G. Once the judicial review is requested, Diversus Health will not release information except by court order.
H. If the individual indicates an intention not to appeal a determination upon administrative review that is adverse to the individual concerning the release of information, the information may be released less than 5 days after the determination upon review is received by the individual.

PROCEDURES FOR DISCLOSURE PURSUANT TO AN AUTHORIZATION:

A. When it is determined that a written authorization is required prior to disclosing PHI, medical records staff should not disclose the PHI until a valid, written authorization is received from the person served, their parent (if a minor), legal guardian, or personal representative.
    1. If the request for disclosure is not accompanied by a written authorization, medical records staff should notify the requestor that Diversus Health is unable to provide the PHI requested. The requestor should be supplied with an Authorization to Use or Disclose PHI form.
    2. Medical records staff should 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, Medical Records staff should 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.
        a. Diversus Health 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 as to the requirements, Diversus Health legal counsel should be contacted.

B. If the request for disclosure is accompanied by a written authorization, Medical Records staff, should review the authorization to assure that it is valid. The authorization form should be fully completed, signed and dated by the person served, their parent (if a minor), legal guardian or personal representative before the PHI is used or disclosed.
    1. The authorization should be written in a language understood by the person signing the authorization. If a person served needs interpretation, they should notify Diversus Health staff for assistance.
    2. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, Medical Records staff, should notify the requestor, in writing, of the deficiencies in the authorization. No PHI should be disclosed unless and until a valid authorization is received.

3. If the authorization is valid, Medical Records staff should disclose the requested PHI to the requester. Only the PHI specified in the authorization should be disclosed.

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

D. Other Diversus Health staff members may not release master records without the approval of the Privacy Officer, except in case of emergency (e.g., person served, or legal guardian is unable at point in time to verify, and the person served faces risk of negative outcome if information is not shared), or as a result 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.

E. In specific program instances whereby, a Multi-Agency Authorization to Release Protected Health Information is utilized, the completed form should not accompany the PHI, as it could identify other agency providers and violate confidentiality.

PROCEDURES FOR RESPONDING TO SPECIFIC TYPES OF DISCLOSURES:

A. Media: No PHI should be released to the news media or commercial organizations without the authorization of the person served or his/her personal representative.

B. Telephone Requests: Staff receiving requests for PHI via the telephone should make reasonable efforts to identify and verify that the requesting party is entitled to receive such information (for example, calling the professional contact information of the person requesting information to verify their official capacity).

PROCEDURES FOR DISCLOSURES TO INDIVIDUALS INVOLVED IN THE CARE OF A PERSON SERVED:

A. Diversus Health may disclose PHI to a family member, other relative, close friend, or any other individual identified by the person served:
1. That is directly relevant to that individual's involvement in the care, or payment for care, of the person served; or,
2. To notify such individual of the location, general condition or death of a person served.

B. If the disclosure is sought by individuals involved in the care of a person served and it is relevant to the requesting party's involvement in the care, Diversus Health may rely on reasonable professional judgment in verifying the identity and authority of the individual seeking disclosure.
1. Diversus Health staff, interns and volunteers should take reasonable steps to confirm the identity of a family member or friend of the person served. Diversus Health is permitted to rely on the circumstances as confirmation of involvement in care. For example, the fact that a person served lives at home with family is sufficient confirmation of the family's involvement on the care of the person served.

C. Prior to a permitted disclosure, if the person served is present for, or otherwise available, then Diversus Health staff, interns and volunteers may use or disclose the PHI if they:
1. Obtain the agreement of the person served;
2. Provides the person served with an opportunity to object to the disclosure, and the person served does not express an objection (this opportunity to object and the response may be done orally); or
3. Based on the exercise of professional judgment, reasonably infer from the circumstances that the person served does not object to the disclosure.

PROCEDURES FOR REVOCATION OF AUTHORIZATION

A. The person served may revoke his/her authorization at any time. The authorization may be revoked verbally or in writing. If the person served, parent of a minor, legal guardian or personal representative informs Diversus Health staff that he/she wants to revoke the authorization, Diversus Health employees, subcontractors, interns or volunteers should obtain a copy of the official authorization (hardcopy or printed electronic) and complete the revocation date and signature at the bottom of the form.

B. Upon receipt of a written revocation, Diversus Health may no longer use or disclose the PHI of the person served, pursuant to the authorization.

C. Each printed or electronic revocation formally completed by employees, subcontractors, interns or volunteers should be filed in the official record of the person served.

D. The Medical Records Supervisor and staff will track and maintain a log of these requests.

REFERENCE:

- 42 CFR § 164.502, 42 CFR § 164.508, 42 CFR §164.514 (H)(1)(I) & (II)

Policy: HIPAA-8110

TITLE: Responding to a Subpoena

POLICY:

From time to time, employees, subcontractors and others associated with Diversus Health may be served with a subpoena or should receive a letter from a lawyer or a less formal request for information, testimony or documents. Similarly, employees, subcontractors and others associated with Diversus Health may receive notification, or field questions or requests for information and documents, from Federal, State, or local authorities regarding an investigation. Diversus Health should 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 persons served and the applicability of any other standards, statutes, court orders or policies.

PROCEDURES FOR RESPONDING TO A SUBPOENA OR INVESTIGATIVE DEMAND:

A. Employees, subcontractors, interns, volunteers and others associated with Diversus Health who are served with a formal or informal request for information, testimony or documents relating to any person served by Diversus Health, or to Diversus Health itself, should promptly advise their supervisor and the legal department.

B. Employees, subcontractors, interns, volunteers and others associated with Diversus Health who receive notification, or field questions, from Federal, State, or local authorities regarding an investigation should promptly alert the legal department, the Privacy Officer, and other senior leadership.

C. Subpoena recipients should seek the advice of the legal department before responding to any subpoenas, court orders or investigatory requests for information.

REFERENCE:

- 42 CFR §164.512(e)

Policy: HIPAA-8120

TITLE: Restrictions to Permitted Uses and Disclosures of Protected Health Information

POLICY:

The person served, their parent (if a minor), legal guardian or personal representative are notified of their right to request restrictions on the use and disclosure of PHI in Diversus Health Notice of Privacy Practices. Specifically, the person served may request restrictions on:

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

PROCEDURES FOR RESTRICTIONS ON USES/DISCLOSURES OF PHI:

A. Persons served, their parent (if a minor), legal guardian or personal representative should make their request in writing. Medical records should provide a Request to Restrict Use and Disclosure of Protected Health Information form to the individual asking to make a restriction.

B. Medical records manages requests for restrictions. A request for restriction should not be reviewed until the Request to Restrict form is completed and signed by the person served. Medical records may assist the person served in completing the form, if necessary.

C. A current version of the form should be maintained on the Diversus Health intranet.

D. Medical records should review the request in consultation with the treating providers and their supervisors to determine the feasibility of the request. Diversus Health should give primary consideration to the need for access to the PHI for service and payment purposes in making its determination.

E. If the treating providers and their supervisors agrees to the requested restriction, Medical records should document the restriction on the Request to Restrict Use and Disclosure of Protected Health Information form, provide the individual making a request with a copy and send the original to the master record of the person served. Medical records should also notify appropriate Diversus Health employees, subcontractors, interns or volunteers of the restriction.

F. Diversus Health employees, subcontractors should abide by the accepted restriction with the following exceptions:

1. Diversus Health may use the restricted PHI or may disclose such information to an authorized provider if the person served is in need of emergency services or treatment. In this case, Diversus Health staff should release the information, but ask the emergency provider not to further use or disclose the PHI of the person served.
2. Diversus Health may disclose the information to the individual who requested the restriction.
3. Diversus Health may use and disclose the restricted PHI when statutorily required to use and disclose the information under the Privacy Rule.

G. If Diversus Health declines the request for restriction, Medical records along with the treating providers and their supervisors should complete the "Facility Response" section of the Request to Restrict Use and Disclosure of Protected Health Information form and provide a copy to the individual making the request.

H. The Request and documentation associated with the request should be placed in the master record of the person served and retained for a period of time no less than six years from receipt.

PROCEDURES FOR TERMINATING THE RESTRICTIONS ON USES/ DISCLOSURES OF PHI:

If the person served, the parent of a minor, legal guardian, or personal representative wishes to terminate the accepted restriction they may do so in writing or verbally. If the person

served, the parent of a minor, legal guardian, or personal representative verbally terminates the restriction, Diversus Health staff should document the verbal agreement in the record of the person served.

A. Medical records should notify the appropriate program and/or case management staff of the termination of the restriction.

B. Medical records should document the termination of the restriction on the Request to Restrict Use and Disclosure of Protected Health Information form, provide the person served with a copy and maintain the documentation in the record of the person served.

C. Termination of a restriction is effective for PHI created or received by Diversus Health.

D. There may be situations that occur in which Diversus Health wishes to terminate the restriction without the agreement of the person served, parent of a minor, legal guardian or personal representative.
   1. Medical records and the treating providers should inform the person served, the parent of a minor, legal guardian, or personal representative that the restriction is being terminated.
      a. If by mail: If the person served, the parent of a minor, legal guardian, or personal representative is informed by mail that Diversus Health is terminating the restriction, the notification should be sent via certified mail, return receipt requested. Diversus Health should maintain a copy of the notification and of the return receipt with the Request to Restrict Use and Disclosure of Protected Health Information form. Diversus Health should not terminate the restriction until it receives confirmation that the person(s) listed above have received the notification.
      b. If in person: If the person served, the parent of a minor, legal guardian, or personal representative is informed in person, it is preferable to have the appropriate individual sign and date a notification of termination of a restriction. However, it should be acceptable to document that the person(s) listed above were notified on the Request to Restrict Use and Disclosure of Protected Health Information form.
      c. If by telephone: If the person served, the parent of a minor, legal guardian, or personal representative is informed by telephone, this action should be documented on the Request to Restrict Use and Disclosure of Protected Health Information form. In addition, an email, or alternately a letter should be sent to the appropriate individual listed above. Letters should be sent via certified mail, return receipt requested. The termination should be effective as of the date the appropriate individual listed above is informed by telephone.
      d. If by email: If the person served, the parent of a minor, legal guardian, or personal representative is informed by email, this action should be documented on the Request to Restrict Use and Disclosure of Protected Health Information form. In addition, a letter should be sent via encrypted email, to a verified email account of the appropriate person listed above. The termination should be effective as of the date of the email.

   E. Such termination is only effective with respect to PHI created or received after Diversus Health has informed the person served, the parent of a minor, legal guardian, or personal representative is informed that it is terminating the restriction. Diversus Health should 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.

REFERENCE:

- 42 CFR §165.522 (a), 42 U.S.C. § 17935

Policy: HIPAA-8130

TITLE: Communication and Access to Protected Health Information by Persons Served

POLICY:

Persons served, their parent (if a minor), legal guardian or personal representative have the right to request communication about their PHI in a variety of ways, such as through phone calls, emails, or in writing. A person served, their parent (if a minor), legal guardian or personal representative also have 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.

REQUESTS FOR ALTERNATE COMMUNICATION METHODS:

A. When a person served notifies Diversus Health staff of their preferred method of communication, or requests that Diversus Health communicate with him or his/her personal representative by some alternate means, Medical records should provide the person served with a copy of a Request for Communications by Alternative Means form. A request should not be evaluated until this request form is completed and signed by the person served or personal representative. Reasonable requests should be honored by Diversus Health staff.

B. If the person served would like to communicate by email, it is recommended that an "Email Communication Consent Form" be utilized.

C. Medical records along with the treating providers and their supervisors should review the completed Request for Communications by Alternative Means form to determine if it is a reasonable request. Diversus Health should not require an explanation for the request. Diversus Health should generally accommodate a request determined to be reasonable.

D. Medical records along with the treating providers and their supervisors should complete the response section of the Request for Communications by Alternative Means form to inform the person served of Diversus Health decision.

E. Medical records should maintain requests and responses in the appropriate location in the official record of the person served.

PROCEDURES FOR ACCESS TO PHI BY PERSONS RECEIVING SERVICES:

A. A person served, parent of a minor, legal guardian or personal representative is notified of their right to access PHI in Diversus Health Notice of Privacy Practices. The Notice of Privacy Practices is given to the person when first requesting services with Diversus Health.

B. A person served, parent of a minor, legal guardian, or personal representative 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. The requester is to complete a Client Access to Protected Health Information form.

1. Medical records along with the treating providers and their supervisors should 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).
    a. Medical records along with the treating providers and their supervisors should verify the identity of the requester before he/she is allowed access to record (e.g, driver's license, identification care, other legal ID).

2. Medical records along with the treating providers and their supervisors should coordinate 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.
    a. If possible, program or case management staff 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.
    b. The person served, or their legal representative should be allowed to review and read the record without intervention from the staff present.

C. When a person served, parent of a minor, legal guardian, or personal representative requests a copy of the PHI in the designated record set, they should be provided with a copy of a Diversus Health Access to Protected Health Information form to sign. Diversus Health prefers to provide this information in an

encrypted electronic format copied to a CD; however, if a paper copy is requested that may be accommodated. Medical records should send electronic or paper copies of the records via direct pick up by the USPS.

1. A free copy of the designated record set should be made available to the person served of his/her legal representative.

D. Requests for access to PHI and release of information should be managed by Medical records.

E. If a former person served, parent of a minor, legal guardian, or personal representative requests to view or requests a copy of the PHI, Diversus Health should respond to the request within 30 days.
   1. If the PHI is stored off-site, or cannot be processed within the allowed 30 days, Diversus Health may have a onetime extension of 30 days to the time frames request if received by Diversus Health, provided that a written statement of the reasons for the delay are provided and the date by which Diversus Health should complete its action on the request is stated.
   2. Medical records should 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 Diversus Health and the person making the request should 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.

PROCEDURES FOR DENYING ACCESS TO PHI BY PERSONS RECEIVING SERVICES:

A. Medical records along with the treating providers and their supervisors should provide a timely, written denial to the person served, parent of a minor, legal guardian, or personal representative, which includes the basis for the denial, and, if applicable, a statement of the individual's review rights. In addition, it should provide a description of how the individual may file a complaint to Diversus Health or to the Secretary of the Office of Civil Rights.

B. Diversus Health may deny the request if the PHI is not contained in its designated record set.

C. Person served, the parent of a minor, legal guardian, or personal representative have the right to request a review of the denial. If a request is received, the following steps should be taken:
   1. Medical records should promptly refer the request to have the denial reviewed to the Clinical or Medical leader over the staff providing the individual's care.

   2. The request may also be reviewed by a qualified individual who was not directly involved in the denial, if necessary.
   3. Medical records along with the treating providers and their supervisors should promptly provide written notice of the results of the review and based on the review, take any necessary steps required.

D. Diversus Health may deny the request for access to the PHI of a person served without a right to review if:
   1. The request is for information compiled in anticipation of a legal proceeding; or
   2. The request is for PHI created or obtained during the course of research which includes treatment for as long as the research continues, provided that the person served has agreed to the denial of access and Diversus Health has informed the person served that this right should be reinstated upon completion of the research; or
   3. The request is for PHI obtained from someone other than a provider under the promise of confidentiality and disclosure would likely reveal the source.

B. Diversus Health may deny the request for access to the PHI of a person served provided that the person served has been given a right to review the denial if:
   1. 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; or

2. 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; or
3. 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.

REFERENCE:

- 42 CFR § 164.524,
- 42 U.S.C. § 17935

Policy: HIPAA-8140

TITLE: Amendment of Protected Health Information

POLICY:

Persons served, their parent (if a minor), legal guardian or personal representative should be notified of the right to amend his or her electronic as well as hard copy PHI in the Notice of Privacy Practices.

PROCEDURES FOR EVALUATING AND RESPONDING TO A REQUEST FOR AMENDMENT OF PHI:

A. The Privacy Officer should be alerted to all requests for amendment of PHI.

B. Upon receiving an inquiry from a person served, the parent of a minor, legal guardian or personal representative regarding the right to amend his/her PHI, medical records should provide the person served, the parent of a minor, legal guardian or personal representative with a copy of an Amendment of Protected Health Information form. A request for amendment should not be evaluated until the request form is completed and signed by the person served, the parent of a minor, legal guardian or personal representative.

C. Medical Records should date stamp or write the date received and initial the Amendment of PHI form.

E. The treating providers and their supervisors should act on the request for amendment no later than 60 days after receipt of the request.

1. If the amendment is accepted, the treating providers and their supervisors should make the amendment and inform the person served, the parent of a minor, legal guardian or personal representative within 60 days of the written request.
2. If the amendment is denied, Medical records along with the treating providers and their supervisors should notify the person served, the parent of a minor, legal guardian or personal representative in writing of the denial within 60 days of the written request.

F. If Diversus Health 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. Medical records along with the treating providers and their supervisors should notify the person served, the parent of a minor, legal guardian or personal representative in writing of the extension, the reason for the extension and the date by which action should be taken.

PROCEDURES FOR ACCEPTING A REQUEST FOR AMENDMENT OF PHI:

A. If the treating providers and their supervisors determines that the request for amendment should be accepted, in whole or in part, they should:

1. Place a copy of the amendment in the records of the person served, or provide a reference to the location of the amendment within the body of the master record.
2. The person served, or the parent of a minor, legal guardian or personal representative may indicate providers or entities with whom the amendment should be shared (as identified on the original Amendment of PHI form.)
3. This notification should occur within a reasonable period of time.

B. If the treating providers and their supervisors should 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 person served. The treating providers and their supervisors should determine whether the person served, the parent of a minor, legal guardian or personal

representative wishes for Diversus Health to notify such other persons or organizations of the amendment.

1. If the person served, the parent of a minor, legal guardian or personal representative wishes for Diversus Health to notify these individuals, the medical records should obtain a signed Authorization to Release PHI form.
2. This notification should occur within a reasonable period of time.

PROCEDURES FOR DENYING A REQUEST FOR AMENDMENT OF PHI:

A. Diversus Health may deny the request for amendment in whole or in part if:

1. The PHI was **not** created by Diversus Health (e.g., a physical examination, dental record, agency assessment). An exception may be granted if the person served, the parent of a minor, legal guardian or personal representative 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 should rarely be the case.)
   a. Every other avenue should be explored before an amendment is made to information that was not created by Diversus Health.
2. 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).
3. The PHI would not be available for inspection under the HIPAA Privacy Rule.
4. The PHI that is subject to the request for amendment is accurate and complete.

B. If the treating providers and their supervisors determines that the request for amendment should be denied in whole or in part, they should provide the person served, the parent of a minor, legal guardian or personal representative with a timely amendment denial letter. The denial should be written in plain language and should contain:

1. The basis for the denial;
2. A statement that the person served, the parent of a minor, legal guardian or personal representative has a right to submit a written statement disagreeing with the denial and an explanation of how to file such a statement;
3. A statement that, if the person served, the parent of a minor, legal guardian or personal representative does not submit a statement of disagreement, they may request that Diversus Health includes the request for amendment and the denial with any future disclosures of the PHI; and
4. A description of how the person served, the parent of a minor, legal guardian or personal representative may file a complaint with Diversus Health or to the Secretary of the U.S. Department of Health and Human Services. The description should include the name or title and telephone number of the contact person for complaints.

C. If the person served, the parent of a minor, legal guardian or personal representative submits a written statement of disagreement, Diversus Health may prepare a written rebuttal to the statement. Diversus Health should provide a copy of the written rebuttal to the person served, the parent of a minor, legal guardian or personal representative who submitted the statement.

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

1. The person served, the parent of a minor, legal guardian or personal representative's Amendment of PHI form;
2. Diversus Health amendment denial letter;
3. The person served, the parent of a minor, legal guardian or personal representative's statement of disagreement, if any; and
4. Diversus Health written rebuttal, if any.

E. If the person served, the parent of a minor, legal guardian or personal representative submitted a statement of disagreement, Diversus Health should disclose information listed in Item D above or an

accurate summary of such information with future disclosures of the PHI to which the disagreement relates.

1. If the person served, the parent of a minor, legal guardian or personal representative did not submit a statement of disagreement, and if the person served, the parent of a minor, legal guardian or personal representative has requested that Diversus Health provide the Amendment of PHI form and the amendment denial letter with any future disclosures, Diversus Health should include these documents (or an accurate summary of that information) with future disclosures of the PHI to which the disagreement relates.

PROCEDURES IF Diversus Health RECEIVES A NOTICE OF AMENDMENT FROM <u>ANOTHER ENTITY OR PROVIDER:</u>

A. If another provider or entity notifies Diversus Health of an amendment to the PHI it maintains, the treating providers and their supervisors along with Medical records should make the amendment to the designated record set.
   1. Amendments to the designated record set should be filed with that portion of the PHI to be amended.
   2. Amendments that cannot be physically placed near the original PHI should be filed in an appropriate location. A reference to the location of the amendment should be added near the original information location.

B. General information regarding requests for amendment, forms relating to amendments and correspondence relating to denial or acceptance of requests to amend should be filed in the master record of the person served.

REFERENCE:

- 42 CFR §164.526

Policy: HIPAA-8150

TITLE: Accounting of Disclosures of Protected Health Information

POLICY:

Persons served, their parent (if a minor), legal guardian or personal representative have the right to receive an accounting of the disclosures of their PHI maintained in their designated record set.

PROCEDURES FOR ACCOUNTING OF DISCLOSURES OF PHI:

A. Upon receiving an inquiry about disclosures of PHI, the Medical records should provide the person served, the parent of a minor, legal guardian or personal representative with a copy of a Request for an Accounting of Disclosures of PHI form.
   1. Requests are not evaluated until the form is completed and signed by the person served, the parent of a minor, legal guardian or personal representative.
   2. A current version of Diversus Health HIPAA related privacy forms and letter templates should be maintained on Diversus Health intranet.

B. Medical records should review and process the request.

C. The written accounting of disclosures is provided to the requestor using a format created and maintained by Medical records.
   1. The accounting should include disclosures during the period specified by the person served, the parent of a minor, legal guardian or personal representative in the request. The specified period may be up to six years prior to the date of the request. Disclosures made on or before April 13, 2003 should not be included in the accounting.
   2. The Medical records should 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.
   3. The Medical records should exclude those disclosures that qualify as an exception.
   4. For each disclosure, the accounting should include:
      a. The date the request for disclosure was received;
      b. The name of provider or entity requesting disclosure and, if known, the address of such person or entity;
      c. A brief description of the PHI that was disclosed; and
      d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
   5. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, the Medical records may provide:
      a. The first disclosure during the accounting period;
      b. The frequency, or number of disclosures made during the accounting period;
      c. The date of the last such disclosure during the accounting period.

D. The Medical records should provide the written accounting of disclosures no later than 60 days after receipt of the request.
   1. If Diversus Health is unable to meet the 60-day time frame, Diversus Health may extend the time once by no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay and the date by which Diversus Health should provide the accounting.

E. Diversus Health provides the first accounting to a person served, the parent of a minor, legal guardian or personal representative within a 12-month period without charge. However, Diversus Health may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided Diversus Health has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.

F. Diversus Health should document and retain for six (6) years from the date of the accounting for paper records, and three (3) years from the date of the accounting for electronic records:
1. The information required to be included in the accounting; and
2. The written accounting provided to the requesting party.

PROCEDURES REGARDING THE EXCEPTIONS TO THE ACCOUNTING OF DISCLOSURES:

A. Accounting of disclosure does not include disclosures:
1. Necessary to carry out treatment, payment, and healthcare operations;
2. To the person served, the parent of a minor, legal guardian or personal representative for whom the PHI was created or obtained;
3. Pursuant to a signed authorization by the person served, the parent of a minor, legal guardian or personal representative;
4. To persons involved in the care of the person served;
5. For national security or intelligence purposes;
6. To a correctional institution;
7. Temporarily suspended by a law enforcement official or health oversight agency (exception applies only during the period of suspension);
8. That are incidental;
9. As part of a Limited Data Set; and
10. That occurred on or prior to April 13, 2003.

REFERENCE:

- 42 CFR §164.528, 42 U.S.C. § 17935

Policy: HIPAA-8160

TITLE: 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; or
- Diversus Health's Notice of Privacy Practices does not reflect current practices accurately.

HIPAA PRIVACY COMPLAINT PROCEDURES:

A. Diversus Health uses the Notice of Privacy Practices form to notify persons receiving services, parent(s) of a minor, legal guardian or their personal representatives of their right to complain to Diversus Health, or the Department of Health and Human Services about privacy issues.

B. All concerns/complaints filed should be directed to the Privacy Officer. The person making the complaint should put their complaint in writing, either through a letter, or email.

C. Once the complaint form and log are completed correctly, the Privacy Officer should work with HR, credentialing, and/or legal as appropriate to determine whether an investigation is warranted.

D. Following completion of the investigative team's review, the Privacy Officer should respond with appropriate HIPAA notification as required.

E. Diversus Health should 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.

F. Employees, subcontractors, interns and volunteers may not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against the person served, the parent of a minor, legal guardian or personal representative or any other person filing a complaint.

REFERENCE:

- 42 CFR §164.530(d)

Policy: HIPAA-8170

TITLE: De-Identification of Protected Health Information

POLICY:

Diversus Health should convert the PHI of a person receiving services into a format that does not identify (de-identifies) the person served when:

- PHI is used or shared for purposes other than treatment, payment or healthcare operations, or authorized exceptions, per Diversus Health policy.
- Information is used or shared without the authorization of the person served, the parent of a minor, legal guardian or personal representative authorization.

PROCEDURES FOR DE-IDENTIFICATION OF PHI:

A. Before staff treats any information as being de-identified, it should be submitted to the Privacy Officer for his/her determination of whether or not health information has been de-identified.

B. The following identifiers of the person served, or of relatives, employers, or household members should be removed by one of the following two (2) methods of de-identification:
   1. Elimination of identifiers:
      a. Names.
      b. 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 should be changed to 000.
      c. Months and dates directly related to a person served, including birth date, admission date, discharge date and date of death. For persons over the age of 89, the month, date and year should be removed, except that such ages may be aggregated into a single category of age 90 or older.
      d. Telephone and fax numbers.
      e. Electronic mail address.
      f. Social security numbers.
      g. Medical record numbers.
      h. Health plan beneficiary numbers.
      i. Account numbers.
      j. Certificate/license numbers.
      k. Vehicle identifiers and serial numbers, including license plate numbers.
      l. Device identifiers and serial numbers.
      m. Web Universal Resource Locators (URLs).
      n. Internet Protocol (IP) addresses numbers.
      o. Biometric identifiers, including finger and voiceprints.
      p. Full face photographic images and any comparable images.
      q. Any other unique identifying number, characteristic, or code.

      Note: In addition to removing the above identifiers, Medical records should verify that the de-identified PHI being shared cannot be used alone or in combination with other information to identify a person served.

   2. 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 should be documented.

PROCEDURES FOR RE-IDENTIFICATION OF PHI:

A. During the process of de-identifying PHI, if statistical de-identification is being performed, a code should be assigned that allows the information to be re-identified by Diversus Health as long as the code is not derived from or related to information about the person served, and is not otherwise capable of being translated so as to identify the person served. Diversus Health should not use or disclose the code or any other means of record identification for any other purpose and should not disclose the mechanism for re-identification.

B. Whether or not information should be coded for re-identification and be re-identified should be determined by the Privacy Officer.

REFERENCE:

- 45 CFR §160.103
- 42 CFR §164.502(d)
- 45 CFR§164.514

Policy: HIPAA-8180

TITLE: Business Associates
POLICY:

A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to Diversus Health (a covered entity) is Business Associate. The term "use" as it relates to PHI is defined in the regulations as the sharing, employment, application, utilization, examination, or analysis of such information with an entity that maintains such information. Disclosure of PHI involves the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. A person or entity that contracts with Diversus Health is 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 BA Agreement.

PROCEDURES FOR BUSINESS ASSOCIATES:

A. Diversus Health should follow established procedures regarding contract review, revision and approval to verify that the contract is in compliance with State and Federal law, to include any HIPAA contract addendums.

B. Diversus Health contracts staff, in collaboration with the Privacy Officer should determine whether a BA Agreement is necessary for specific entities. Common examples of entities needing a BA Agreement are:

1. Providers of services;
2. Diversus Health subcontractors;
3. An attorney who reviews PHI to assist in a case or any other matter that requires the disclosure of PHI to the attorney; and,
4. Consultants or vendors who may see PHI in the course of completing their duties for Diversus Health.

C. If a BA Agreement is necessary and the other party provides its own BA Agreement, the CSO should review the Agreement to assure it meets requirements of the Privacy and Security Rule.

D. If a BA Agreement is necessary, and the other party does not provide the Agreement, Diversus Health contracts staff should submit Diversus Health's BA Agreement for approval by the other party.

E. If the BA refuses to sign the Agreement, the Privacy Rule prohibits Diversus Health from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of Diversus Health, Diversus Health should not contract with the BA.

F. The original signed contract and contract addendum containing BA language should be maintained by Diversus Health.

G. The CSO and contracts staff should amend BA Agreements when changes occur to HIPAA rules, regulations and standards.

PROCEDURES FOR BREACH OF A BA AGREEMENT AND SANCTIONS:

A. If Diversus Health staff learns of a breach or violation of a BA requirement by a BA, such breach or violation should be reported to the Privacy/Security Officer. The Privacy/Security Officer should 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.

B. 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, Diversus Health may:
   1. Terminate the contract or arrangement; or
   2. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.

C. 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 as a result of its contract with Diversus Health.

1. The Privacy Officer and/or the legal department should assist with contacting the BA regarding the BA's obligations to return or destroy PHI that originated from Diversus Health.
2. If return or destruction is not feasible, the BA is obligated to maintain the PHI that originated from Diversus Health in accordance with HIPAA standards, rules and regulations.

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

REFERENCE:

- 42 CFR §160.103
- 42 CFR §164.502 (e)
- 164.504(e)(1); 42 U.S.C. § 17931

Policy: HIPAA-8190

TITLE: Marketing and Fundraising

POLICY:

Diversus Health obtains the written consent of a person served, their parent (if a minor), legal guardian or personal representative prior to using confidential information and/or a photograph of a person served in its marketing or communication materials.

PROCEDURES FOR USING PHI FOR MARKETING:

A. 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:

1. Communications made directly by Diversus Health to describe the services it provides;
2. Communications made for care or treatment of the individual;
3. Communications for case management or care coordination for the person served, the parent of a minor, legal guardian or personal representative;
4. Communications to direct or recommend alternative treatments, therapies, and care providers or settings of care; and,
5. Face to face communications made by Diversus Health representatives to an individual.

B. Marketing staff should obtain a valid, completed Authorization to Use or Disclose Protected Health Information 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 (paragraph A above) and do not qualify for any of the exceptions listed in items 1-5 above.

1. The authorization should conform to procedures outlined in the "Uses and Disclosures" procedure HIPAA-109 of the Diversus Health HIPAA policies and procedures.
2. If direct or indirect remuneration to Diversus Health from a third party is involved, the authorization should state the nature of such third-party remuneration.
3. Diversus Health should make reasonable efforts to verify that individuals who decide to opt out of any use of their Protected Health Information is documented appropriately and honored by Diversus Health staff or its business associates.

C. No authorization is required in the following situations:

1. 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.
2. When PHI is not disclosed in a marketing communication (such as a newspaper advertisement).

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

E. Business associates and other third parties:

1. Diversus Health may engage a marketing firm to conduct permitted marketing activities on Diversus Health's behalf. Should the marketing activities require the use or disclosure of PHO to the marketing firm, then a business associate relationship would exist and a BA agreement would be required. (See Policy and procedure HIPAA-117.)
2. Diversus Health 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 person served, the parent of a minor, legal guardian or personal representative.

PROCEDURES FOR USING PHI FOR FUNDRAISING:

A. When fundraising for its own benefit, Diversus Health may use or disclose without authorization the following PHI to a Business Associate, a foundation or consultant to act on Diversus Health behalf:
B. Demographic information relating to an individual, and
C. Dates of service provided to an individual.
    a. Diversus Health's Notice of Privacy Practices should inform the person served, the parent of a minor, legal guardian or personal representative that PHI may be released to raise funds for Diversus Health and that the person served, the parent of a minor, legal guardian or personal representative may opt out of receiving any fundraising communications.
D. Any fundraising materials Diversus Health or its agent sends to an individual should describe how the individual may opt out of receiving any further fundraising communications.
E. If the fundraising is not for Diversus Health's benefit or includes more than demographic or dates of service information, an authorization from the individual is required.
F. Diversus Health should make reasonable efforts to verify that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

REFERENCE:

- 42 CFR §164.508(a)(3)
- 42 CFR §164.514

Policy: HIPAA-8200

TITLE: Breach Notification Requirements and Investigations

POLICY:

A privacy or security breach occurs when there has been an unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the information. If an actual breach occurred, 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. Diversus Health will comply with HIPAA breach notification rules in the notification of the proper entities.

PROCEDURES FOR BREACH NOTIFICATION:

A. Employees, subcontractors, interns or volunteers who believe that unauthorized access, use or disclosure of PHI has occurred should immediately and simultaneously report the circumstances of the suspected breach to their supervisor and the Privacy Officer.
   1. Diversus Health staff should report any suspected breach of unsecured PHI to the Privacy Officer as soon as possible, within 24 hours after knowledge of the incident.

B. The report of a potential breach should include the following information, to the extent available:
   1. A brief description of what happened, including the date of the potential breach and the date the suspected breach was discovered;
   2. Who used the PHI without appropriate permission or authorization and/or to whom the information was disclosed without permission or authorization;
   3. A description of the types of and amount of unsecured PHI involved in the breach;
   4. Whether the PHI was secured by encryption, destruction, or other means;
   5. Whether any intermediate steps were taken to mitigate an impermissible use or disclosure;
   6. Whether the PHI that was disclosed was returned prior to being accessed for an improper purpose; and
   7. If the PHI was provided to Diversus Health under a Business Associate Agreement.

C. The report should be provided to the Privacy Officer.

D. Diversus Health maintains an open-door policy regarding compliance with HIPAA. Employees, subcontractors, interns and volunteers are encouraged to speak with the Privacy Officer or other appropriate individual regarding any concerns they may have with Diversus Health HIPAA compliance program or initiatives designed to maintain and enhance privacy and security controls. These should be no retaliation against employees, subcontractors, interns or volunteers who, in good faith, report any activities he or she believes is a breach of HIPAA.

   1. Although not guaranteed (depending on the circumstances) anonymity should be maintained whenever possible.

E. Failure to report a suspected breach to the Privacy Officer may result in disciplinary action against Employees, subcontractors, interns or volunteers.

PROCEDURES FOR INVESTIGATION OF A REPORTED BREACH OF CONFIDENTIALITY:

A. The Privacy Officer should respond promptly to any security and/or privacy incident.

B. The Privacy Officer and/or Security Officer should determine if there is a concern regarding a possible violation of HIPAA or Diversus Health policies or procedures related to HIPAA. Diversus Health senior leadership is notified of any egregious violations.

C. Appropriate staff including the Privacy Officer, HR, credentialing, and/or the legal department if needed determine if an investigation is necessary and conduct one as soon as possible.

D. If, at the conclusion of the investigation, it is found that a violation of Diversus Health policy or procedure has occurred;

F. The VP of Human Resources, should determine what disciplinary actions should be taken. The disciplinary action report documenting the violation should be placed in the staff's personnel file.

G. Documentation of findings and final actions from the investigation should be maintained as a part of Diversus Health Privacy records and retained for six (6) years.

E. The Privacy/Security Officer should take or direct appropriate action to address the issues identified through the investigatory process.

F. The investigation team should 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 rule guidelines.

1. HIPAA's breach notification rule requires notification of affected individuals, HHS, and in certain cases, the media, without unreasonable delay and within 60 calendar days following the discovery of a confirmed breach under Federal and or State HIPAA rule guidelines. However, Colorado's 'Privacy Law' requires notification within 30 calendar days. Diversus Health will follow the more stringent law.
2. HIPAA's breach notification rule requires notification of the media for breaches of more than 500 clients. Under Colorado's 'Privacy Law', notification of the Colorado Attorney General is also required in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred.
3. If more than 1,000 Colorado residents are affected by a breach, Colorado's 'Privacy Law' requires the Colorado Covered Entity must also notify all consumer reporting agencies of the anticipated date of the notification to Colorado residents and the approximate number of people who are to be notified. The Colorado Covered Entity is not, however, required to provide the names or other personal information of the persons affected. The Privacy Law requires that notice be made to the reporting agencies in the most expedient time possible and without unreasonable delay.
4. Under Colorado's 'Privacy Law', if a Colorado Covered Entity uses a third-party service provider, that third-party service provider is required to give notice to and cooperate with the Colorado Covered Entity in the event of a security breach that compromises any computerized data containing personal information that the third-party service provider maintains on behalf of the Colorado Covered Entity. The third-party service provider is required to notify the Colorado Covered Entity in the most expedient time possible, and without unreasonable delay, following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.

G. Diversus Health staff should not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against:

1. 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.
2. Any individual who:
   a. Files a complaint with the Secretary of the Department of Health and Human Services as permitted by the privacy or security regulations;
   b. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing conducted by a government enforcement agency; or,
   c. Opposes any act or practice made unlawful by the privacy or security regulations under HIPAA, provided that 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 Protected Health Information in violation of the privacy or security regulations under HIPAA or this policy.

H. Any individual who believes that a form of retaliation or intimidation is occurring or has occurred should report the incident to the HR. HR, in collaboration with the investigation team noted above, should treat such a report as a complaint and investigate it accordingly.

ACCESS, USE OR DISCLOSURES THAT DO NOT CONSTITUTE A HIPAA VIOLATION OR BREACH:

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

A. File a complaint with the Office of Civil Rights, U.S. Department of Health and Human Services pursuant to the HIPAA regulations;

B. 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;

C. 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 with regard to the whistleblower activity provided the individual in good faith believes Diversus Health has acted unlawfully; or

D. 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.

REFERENCE:

- 45 C.F.R. § 164.400-414
- 42 U.S.C. § 17932
- 45 C.F.R. § 164.530(g)

Policy: HIPAA-8210

TITLE: Sanctions for Failure to Comply with HIPAA

POLICY:

Employees, subcontractors, interns or volunteers should report coworkers who violate HIPAA Privacy and Security Rules. Employees, subcontractors, interns or volunteers who violate HIPAA Privacy and Security rules may be subject to disciplinary actions up to, and including, termination of employment or the relationship with Diversus Health.

PROCEDURES FOR DETERMINING SANCTIONS FOR EMPLOYEES, SUBCONTRACTORS, INTERNS AND VOLUNTEERS:

A. 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.

B. The degree of discipline may range from a verbal warning up to and including termination of the employment or the relationship with Diversus Health and/or restitution in accordance with Diversus Health policies. The following three (3) levels of violations should be utilized in recommending the disciplinary action and/or corrective action to apply:
   1. Level 1: An individual inadvertently or mistakenly accesses PHI that he/she had no need to know in order to carry out his/her responsibilities for Diversus Health, 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:
      a. Leaving PHI in a public area;
      b. Mistakenly sending emails or faxes containing PHI to the wrong recipient;
      c. Discussing PHI in public areas where it can be overhead, such as elevators, cafeteria, restaurants, hallways, etc.;
      d. Leaving a computer accessible and unattended with unsecured PHI;
      e. Loss of an unencrypted electronic device containing unsecured PHI;
      f. Improperly disposes of PHI in violation of Diversus Health policy; or
      g. An individual fails to report that his/her password has been potentially compromised (e.g., has responded to email spam and given out their password).
   2. 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:
      a. Intentional, unauthorized access to their own, friends, relatives, coworkers, public personality's or other individual's PHI (including searching for an address or phone number);
      b. Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual a user name and password to access electronic PHI;
      c. Disclosing patient condition, status or other PHI obtained as employees, subcontractors, intern or volunteer to a co-worker who does not have a legitimate need to know;
      d. Obtaining PHI under false pretenses;
      e. Failure to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI;
      f. Failure to promptly report any violation of Diversus Health privacy or security policy or procedure or to the Privacy or Security Officer;
      g. Logging into the Diversus Health network resources (including electronic medical records) and allows another individual to access PHI;
      h. Connects devices to the network and/or uploads software without having received authority from IT; or
      i. Second occurrence of any level 1 violation (it does not have to be the same offense).

3. 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:
    a. Unauthorized intentional disclosure and/or delivery of PHI to anyone;
    b. 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 user name and password to access electronic PHI;
    c. Accessing or using PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute);
    d. Disclosing PHI for financial or other personal gain;
    e. Uses, accesses or discloses PHI that results in personal, financial or reputational harm or embarrassment to the person served; or
    f. Second occurrence of any level 2 violation (it does not have to be the same offense) or multiple occurrences of any level 1 violation.

C. The VP of Human Resources should document the sanctions that are applied, if any. This documentation should be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

PROCEDURES FOR DETERMINING SANCTIONS FOR BUSINESS ASSOCIATES:

A. Any level of breach by the business associate and/or its staff or agents should be addressed by Diversus Health in accordance with the terms of the BA Agreement currently in effect at the time of the breach.

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

C. However, if the business associate is required by law to perform a function or activity on behalf of Diversus Health or to provide a service described in the HIPAA Privacy Rule's definition of a business associate to Diversus Health, Diversus Health may disclose electronic protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements for business associates, provided:
    1. Diversus Health attempts in good faith to obtain satisfactory assurances, as stated above; and,
    2. If that attempt fails, the CFO documents the attempt and the reasons that the assurances cannot be obtained.

REFERENCE:

- 45 C.F.R. §164.308(a)(1)(ii)(C) and 45 CFR §164.316(b)
- 42 CFR §164.530 and 45 CFR §164.502, 164.314(a)(2)

Policy: HIPAA-8220

TITLE: Retention of Protected Health Information

POLICY:

The HIPAA Privacy Rule indicates that PHI, including medical and financial records contained in the master record, should be retained for a minimum of seven (7) years. However, Colorado State law specifies that in the case of hospitals, protected health information (PHI) contained in the records should be retained for at least the age of minority (18 years old) plus 10 years until the individual is 25 years old, after the date last in effect.

Diversus Health will comply with the stricter Colorado State law (6 CCR 1011-1) and maintain specific medical and physiological records that have historical value for persons served for a longer period.

(a) for minors, for the period of minority plus 10 years (i.e., until the patient is age 28) or 10 years after the most recent patient usage, whichever is later.

(b) for adults, for 10 years after the most recent patient care usage of the medical record.

RETENTION OF PHI PROCEDURES:

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

B. In instances whereby, non-PHI (administrative records) is maintained for case management business and operations roles, it should be maintained in accordance with State and Federal laws.

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

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

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

REFERENCE:

- 45 CFR §164.526(f)
- 45 CFR § 164.530(j)(1)(2)
- Colorado: 6 C.C.R. § 1011-1, Ch. IV, § 8.102(2)

Policy: HIPAA-8230

TITLE: Destruction of Protected Health Information

POLICY:

PHI maintained in paper format should 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 should not become part of the master record (e.g., draft or working documents, shadow charts or files, unofficial notes, etc.) should 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, Diversus Health should determine if PHI has been stored in this equipment and delete PHI prior to the disposal of the equipment.

PROCEDURES FOR DESTRUCTION OF PHI IN PAPER DOCUMENTS:

A. Acceptable methods of destruction include shredding, incineration, pulverization and use of a bonded recycling company. Records containing PHI should not be thrown into an insecure trash receptacle.

B. A destruction log should be maintained by Medical Records Supervisor to identify the destroyed records. At a minimum, the destruction log should capture the following information.

1. The date of destruction.
2. The name of the individual responsible for destroying the records.
3. The name of the person who witnessed the destruction.
4. The method used to destroy the records.
5. Information about the person served (full name, social security number, date of admission, date of discharge).

C. Prior to destruction of boxed items, the Medical Records Manager should verify the retention period has expired.

D. If the records are destroyed at a non-Diversus Health location through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.

E. Diversus Health should maintain destruction documents permanently.

PROCEDURES FOR DESTRUCTION OF ELECTRONIC PHI:

A. Workstations, laptops and servers use hard drives to store a wide variety of information. PHI may be stored in a number of areas on a computer hard 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.

1. To make certain that the PHI of persons served has been removed, the Security Officer should have IT staff use a software program/utility that overwrites the entire disk drive with "1"s and "0"s.
2. If the computer is being re-deployed internally to an area that would inappropriately expose PHI or disposed of due to obsolescence, the aforementioned software program/utility should 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.
3. 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 should be removed from the computer and

physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser. This applies to PC workstations, laptops and servers.

C. All non-current physical backup media including tapes, optical disks (CDs & DVDs) and diskettes containing PHI should be appropriately destroyed before disposal.

D. If a service is used for disposal of electronic PHI, the vendor should provide a certificate indicating the following:

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

REFERENCE:

- 42 CFR §164.530

Policy: HIPAA-8240

TITLE: Maintaining Security of Electronic PHI (EPHI)

POLICY:

Diversus Health implements procedures to protect electronic protected health information and for controlling access to electronic protected health information.

Diversus Health should encrypt PHI on the hard drives and mobile devices, whenever possible and feasible, to avoid potential breaches of unsecured PHI.

PROCEDURES FOR MAINTAINING THE SECURITY OF EPHI:

A. When employees, subcontractors, interns, and volunteers begin work at Diversus Health, the immediate supervisor or hiring manager should notify the IT Director or his/her designee about the level of access to EPHI that the employees, subcontractors, intern or volunteer is authorized to access. The immediate supervisor should refer to the job description and information that the staff member, intern or volunteer needs, and verify that access to EPHI is the minimum necessary to perform his/her duties.

B. IT staff should then establish the employees, subcontractors, interns or volunteer's access to EPHI on Diversus Health information systems. Access should be established by instituting the appropriate accounts and account permissions on Diversus Health information systems.

C. Employees, subcontractors, interns and volunteers should receive training on the HIPAA Privacy Rule in accordance with established training schedules.

D. The Hiring Manager should designate staff members who are authorized to access areas in which EPHI may be accessible. These individuals should receive the same training on the requirements of the HIPAA Privacy Rule and be subject to the same requirements as other employees, subcontractors, interns or volunteers who are authorized to access EPHI, including sanctions. These individuals' authorization should be reviewed and modified according to these HIPAA policies.

E. Employees, subcontractors, interns and volunteers who access EPHI without authorization are subject to the sanctions listed in Diversus Health policy and procedure HIPAA-120.

F. When a staff changes positions within Diversus Health or for some other reason his/her or her need for access to EPHI change, the Program Manager or Supervisor should notify the IT Director or his/her designee. The IT Director or his/her designee should then review the staff's needs for EPHI and revise the staff's authorization accordingly.

    1. When a staff, intern or volunteer's employment or position with Diversus Health is terminated for any reason, HR staff should inform the Hiring Manager, IT Director or his/her designee that the staff, intern or volunteer no longer works at Diversus Health and that accounts for that individual should be closed. In addition, the following steps should be taken:

    2. The immediate supervisor should collect from the staff any keys, badges, cell phones and any other equipment that was deployed to the individual. This should be verified by using the staff Termination Checklist.

3. The IT Director or VP or his/her designee should disable or inactivate accounts of the former staff within one hour of the staff leaving the premises. For any accounts to which the staff had publicly known passwords, or passwords that cannot be closed, the IT Director or his/her designee should change the passwords immediately.

PROCEDURES FOR REPORTING UNAUTHORIZED USE OF EPHI:

A. Employees, subcontractors, interns or volunteers who believe that unauthorized access, use or disclosure of EPHI has occurred should immediately and simultaneously report the circumstances of the suspected breach to their supervisor and the Security Officer (or, in the absence of the Security Officer, reports may be made to the Privacy Officer). Staff should also report if they detect evidence that a security incident may be imminent.

1. Diversus Health staff should report any suspected breach of unsecured EPHI to the Security/Privacy Officer as soon as possible, within 48 hours after knowledge of the incident.

B. Upon detection of a security incident, the Security Officer should ask IT staff to immediately begin efforts to determine the nature, scope, and source of the incident. The Security Officer should also endeavor to determine the potential harm from the incident including information at risk and the level of risk presented.

C. The Security Officer should work with department heads to determine parameters for containment. These parameters should be used by the Security Officer to determine when to begin containment procedures. Once the Security Officer has determined the nature and scope of the incident, this information should be used, in conjunction with the containment parameters, to determine an appropriate containment strategy and when that strategy should be implemented.

1. Once the Security Officer determines that containment should begin, the IT Director or VP or his/her designee should immediately take steps to isolate those systems that have been affected or compromised by the incident from the rest of Diversus Health information systems. The affected or compromised systems should remain isolated until the incident is resolved.
2. Upon the identification of a security incident, the IT Director or VP or his/her designee should begin eradication procedures as soon as possible.

D. After the Security Officer is certain that the security incident has been resolved, the Security Officer should investigate whether EPHI was lost or altered during the incident. If the Security Officer determines that EPHI was lost or damaged, the Security Officer should determine the extent of loss or alteration to EPHI and should restore lost or damaged information.

1. In the event the Security Officer determines that EPHI was disclosed during the incident, the Security Officer should verify that the information regarding the disclosure is handled in accordance with Diversus Health HIPAA Breach Notification Rule.
2. The Security Officer should take steps to mitigate the harm from the security incident by following Diversus Health's mitigation procedures.

E. The Security Officer should document, in written or electronic form, any security incidents and their outcomes.

1. This documentation should include:
    a. The date of the incident;
    b. Extent of the incident;
    c. Duration of the incident;
    d. Response to the incident; and,
    e. Any other pertinent information that the Security Officer determines is necessary for future reference or any reporting require.
2. The Security Officer should verify that documentation of any security incident is maintained for six (6) years from the date of the incident.

PROCEDURES FOR BACKUP, RECOVERY AND EMERGENCY PREPAREDNESS:

A. Data Backup Plan: Diversus Health should take reasonable steps to protect the confidentiality, availability, and integrity of PHI and other confidential information during an unexpected emergency or negative event.
   1. Diversus Health's information technology system and network should be backed up daily and copies of back up information should be maintained by the approved business associate providing this service at time of data backup.
   2. The IT HelpDesk Manager, Director or VP should establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. The Network Specialist should also verify that the electronic media containing these exact copies are stored in a secure manner.

B. Because computer equipment/hardware may be damaged during a move, IT staff should copy documents that contain electronic protected health information to a central server either through a file transfer or by emailing the documents to another internal email account.
   1. Upon completion of the move, IT staff should check to verify that any electronic protected health information maintained on the piece of hardware has not been damaged or destroyed. In the event such damage or destruction has occurred, IT staff should restore the information onto the hardware from the location to which the information was transferred.
   2. Once the move is complete and IT staff is satisfied the copied files are no longer necessary, the duplicate files should be deleted according to the procedures for deleting electronic protected health information from reusable media.

C. Disaster Recovery Plan: Diversus Health should establish a disaster recovery plan for its IT systems that contain PHI, to be used when an emergency or other unanticipated event disrupts its IT system's functionality. The disaster recovery plan should establish the criticality of each IT system that contains PHI.
   1. The IT HelpDesk Manager, Director or VP should be responsible for implementing procedures to restore any lost data from the exact copies created and stored pursuant to Diversus Health Data Backup Plan, above.
   2. The disaster recovery plan should be part of Diversus Health Emergency Preparedness/Contingency Plan that should be implemented in the event of an emergency or other unanticipated event that disrupts Diversus Health's IT system functionality.

D. Emergency Preparedness/Contingency Plan: The IT Director or VP should 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 electronic protected health information during and immediately after a crisis.
   1. The Emergency Preparedness/Contingency Plan should be tested and reviewed periodically (or at a minimum, yearly) to confirm that it is current, effective and sufficient to meet the needs of Diversus Health workforce members and operations.

E. The IT Director or VP should periodically perform a security risk analysis. This assessment should be documented in written or electronic form and maintained as required by these policies and the HIPAA Regulation

REFERENCE:

- 45 CFR §164.308(a)(3)(i)

Policy: HIPAA-8250

TITLE: Physical Safeguards to Maintain the Security of EPHI

POLICY:

Diversus Health implements policies and procedures for the use of physical safeguards in protecting electronic protected health information and for controlling access to electronic protected health information.

PHYSICAL SAFEGUARD PROCEDURES:

A. Diversus Health should implement procedures to make certain that 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.

1. Unauthorized employees, subcontractors, interns or volunteers who access EPHI or areas where EPHI may be accessed without being properly authorized pursuant to this procedure should be subject to sanctions under Diversus Health policies and procedures HIPAA-120.
2. The Facilities Manager should implement procedures to control and validate individuals' access to facilities / locations based on their role or function. These procedures should include procedures for visitor control and controlling access to software programs for testing and revision.
3. The Facilities Manager should designate members of his/her staff who are authorized to access areas in which EPHI may be accessible. These individuals should be subject to the same requirements as other staff, interns or volunteers who are authorized to access EPHI, including sanctions. These individuals' authorization should be reviewed and modified according to Diversus Health procedures to review and modify access to EPHI.
4. Whenever a physical component of Diversus Health facilities and locations that is related to the security of facilities and locations, is repaired, replaced, or modified, the person making the repair, replacement, or modification should record the work done on a Maintenance Tracking Form. A copy of this form should then be provided to the Facilities Manager who should be responsible for maintaining the record for six (6) years from the date it was created.

B. Diversus Health should implement physical measures designed to protect its information systems and locations from natural disasters, and environmental hazards.
   1. Diversus Health should establish procedures that in the event of emergency allow employees, subcontractors, interns or volunteers to access its facilities locations in support of restoration of lost data under Diversus Health's disaster recovery and emergency mode operations plans.

COMPUTER HARDWARE ASSET TRACKING PROCEDURES:

A. Diversus Health's IT department, with the assistance of the Finance department, should perform an annual inventory to determine what computer hardware and electronic media is maintained by each of Diversus Health departments. This inventory should be recorded on Diversus Health Fixed Asset accounting software.

B. In addition to the annual inventory, the IT HelpDesk Manager or his/her designee should provide an inventory update whenever new equipment is added, or old equipment is removed. This update should be provided to the Diversus Health Finance department. Finance department staff should then update the master inventory list based upon the information provided in the update.

PROCEDURES FOR REMOVAL OF EPHI FROM COMPUTER HARDWARE/MEDIA:

A. Electronic protected health information should be removed from computer hardware and other electronic media prior to disposal or donation to another entity.

B. Computer hardware should be wiped clean prior to sale, donation or disposal. Prior to reformatting the hard drive, IT staff should make certain that files containing EPHI have been deleted using a program that rewrites information over the used sectors of the disk. In the case of a program that allows the user to choose the number of times the program rewrites over a sector of the disk, IT staff should make certain that NIST 800-88 security specifications are met or exceeded.

C. If the computer is to be donated or sold, after the hard drive is wiped clean, IT staff should reinstall software that came pre-installed on the computer when originally purchased as well as any software programs that are to be donated with the computer. Any software that Diversus Health should continue to use on a replacement computer should not be reinstalled on the computer that is to be donated or discarded.

D. In some situations, Diversus Health stores EPHI on removable magnetic storage media (such as external hard drives, floppy disks, or zip drives) or optical storage (such as CDs and DVDs)). When

Diversus Health determines it is appropriate to dispose of this media, IT staff should verify that the media is rendered physically unusable prior to disposal.

E. In some situations, Diversus Health stores electronic protected health information to flash drive media. When Diversus Health determines that it is appropriate to dispose of these flash drives, IT staff should verify that the drives are erased. This should be done by using the appropriate software to return the flash drive to a pristine state. Simply deleting the table of contents is not sufficient

REFERENCE:

- 45 CFR §164.310

Policy: HIPAA-8260

TITLE: Technical Safeguards to Maintain the Security of EPHI

POLICY:

Diversus Health implements policies and procedures for the use of technical safeguards in protecting electronic protected health information and for controlling access to electronic protected health information.

PROCEDURES FOR ESTABLISHING AUTHORIZED USERS OF Diversus Health NETWORK:

A. HR staff should notify the IT and Facilities Department that a new staff has been hired and he or she needs unique user identification.
   1. The IT Director should create a unique identifying name for each user. The IT Director should also be responsible for creating accounts for authorized users. This may include, but is not limited to, such actions as creating accounts on the appropriate servers, creating an account on the workstation the user has been assigned, and any other action necessary to verify that the user is identified by his/her unique user identification in the Diversus Health information systems.
   2. For new accounts, the Network Operations Manager should provide the staff with appropriate levels of access by following Diversus Health procedures for Authorizing Access to Electronic Protected Health Information.

C. Authentication should be provided by the use of a password. Each staff should be assigned a password at the time they are granted access to Diversus Health information systems.
   1. Users should establish passwords that conform to the requirements of Diversus Health password requirements.
   2. The IT Director or VP, or his/her designee, should establish the length of time a password is valid, the composition of the password, and the assignment of a new password at the expiration of the old password.

SAFEGUARDING EPHI AND Diversus Health NETWORK WHEN USING EMAIL:

A. Staff may send and receive work and personal email from work, whether through use of their workstation or when using a Diversus Health issued laptop or mobile device.
   1. Employees, subcontractors, interns or volunteers should not open email or email attachments that are from unknown senders. The email should be deleted immediately upon receipt, before opening.

B. The IT Director or VP should implement procedures governing the appropriate handling of email and email attachments. These procedures should be designed to prevent staff from inadvertently introducing malicious software into Diversus Health environment and to prevent the propagation of malicious software due to staff failure to follow Diversus Health policies and procedures.

C. Diversus Health should implement email encryption methodology and policies and procedures to protect EPHI from improper access during outgoing email communication.
   1. Diversus Health employees, subcontractors, interns and volunteers should use a method for encryption of outgoing email when EPHI is included. Employees, subcontractors, interns, and volunteers should always follow the procedure defined in HIPAA-8090 section of this document.
   2. The method for employing encryption will be included in initial Security Training, as well as any remedial or follow up HIPAA trainings.

D. Diversus Health should implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

1. Whenever a staff believes that a piece of EPHI has been altered in an unauthorized manner, that staff should immediately compare the EPHI contained on Diversus Health information systems to the information contained in the individual's file.
2. In the event that the staff determines, based upon this comparison, that the EPHI has been altered, he or she should immediately notify the Diversus Health Security Officer that the information has been altered. The Diversus Health Security Officer should then follow Diversus Health computer security incident response procedures. The staff should not amend the electronic protected health information but should allow Diversus Health Security Officer to determine when it is appropriate to correct the information.
3. Furthermore, the staff should resend the information, but should use a different mode of transmission. If the need for the information is time sensitive, the staff should attempt to fax the paper copies of the information using Diversus Health's procedures for faxing protected health information.

SAFEGUARDING EPHI AND Diversus Health NETWORK WHEN USING THE INTERNET:

A. When needed for the purposes of completing their job duties, staff, interns or volunteers may access the Internet. Staff, subcontractors, interns or volunteers may also access the Internet for personal use, but only when on lunch or other breaks.
   1. Regardless of the time or reasons for accessing the Internet, staff, interns or volunteers should not visit websites that violate the law or that could be offensive to other staff, interns or volunteers.

B. Staff, subcontractors, interns or volunteers should not download files or install software from the Internet to their workstations, laptops or tablets.
   1. Staff, interns or volunteers should not install software on their workstations. Furthermore staff, interns or volunteers should not download software or other files from the Internet.
   2. In the event staff believes a piece of software, whether from the Internet or elsewhere, or a file from the Internet is necessary for the staff to do his/her or her job, the staff should obtain the approval of their supervisor and IT staff prior to downloading any files or installing any software. IT staff should review the request and, if appropriate, should download and install the software for the person requesting the software.

C. When a staff member is away from his/her or her workplace and needs to access the Internet with his/her or her laptop, the workforce member may use Diversus Health provided devices such as a hotspot on a smartphone or a personal cellular data device. If a secure wireless network is available, the workforce member can use that network to connect to the Internet.
   1. When a staff member uses his/her or her laptop or tablet to access the internet from another location, the member should comply with each of Diversus Health policies governing personal Internet access. In the event of a concern that these policies have been violated, IT staff or HR staff should review the history of locations visited using the designated Internet access monitoring tool.

D. Staff, subcontractors, interns or volunteers should not create web sites that are either hosted by Diversus Health computers or accessed through Diversus Health network.

E. IT staff should monitor Internet traffic in order to make certain that staff, interns and volunteers comply with these policies

F. The IT Director should implement procedures governing downloading files from the Internet. These procedures should be designed to prevent staff, interns and volunteers from inadvertently introducing malicious software into Diversus Health environment and to prevent the propagation of malicious software due to staff failure to follow Diversus Health policies and procedures.

G. The IT Director or VP should verify that Diversus Health has a firewall program or appliance installed between the Internet and its local area network. This firewall should be configured to allow staff, interns or volunteers to use the Internet in conformance with Diversus Health's policies and procedures on Internet usage but should prevent unauthorized access to Diversus Health network from the Internet. The exact configuration of the firewall should be determined by the Network Operations Manager and documented in IT systems documentation.
    1. IT staff should make certain that each workstation, laptop and tablet has a firewall installed. IT staff should configure the firewall according to the procedures developed by the IT Director or VP governing allowed and denied access. Furthermore, the firewall should be configured to initiate when the workstation, laptop or tablet is started.

SAFEGUARDING EPHI AND Diversus Health NETWORK THROUGH ANTI-VIRUS SOFTWARE:

A. IT staff should verify that Diversus Health workstations, laptops and tablets that can access EPHI has an anti-virus software program installed that is capable of intercepting, detecting and removing malicious software. This software should be configured to automatically scan email attachments, floppy disks, and any other files downloaded onto the workstation or any electronic media connected to the workstation.

B. IT staff should verify that this software is regularly updated, has the most current virus definitions, and has the most current patches installed. IT staff should check for new virus definitions and patches on a daily basis. When IT staff determines there are new definitions or patches, IT staff should verify that they are installed on workstations within 5 days.
    1. IT staff should confirm that each mobile workstation's software for detecting and removing malicious software is configured to check for patches and for updated virus definitions each time the workstation is started.

SAFEGUARDING EPHI AND Diversus Health NETWORK THROUGH SETTINGS ON WORKSTATIONS, LAPTOPS AND TABLETS:

A. IT staff should make certain that each Diversus Health issued workstation, laptop and tablet requires a username and password to gain access. For workstations that are shared by staff, interns or volunteers, each individual user should have a unique username and password.

B. IT staff should configure the workstation, laptop or tablet so that users do not have administrative privileges and are not able to alter the settings on the workstation.

C. Each workstation should be configured to require a username and password to shut down the screensaver. The screensaver should be configured to activate automatically after 15 minutes of inactivity. Additionally, the screensaver should be configured so that when the user leaves the computer unattended the user may start the screensaver immediately.

D. Staff, interns or volunteers should not save files containing EPHI to their workstations. Instead, files should be saved to the Diversus Health network or to an encrypted storage device. Staff, interns or volunteers should make certain that any files that are necessary for them to perform their job are copied to the network before leaving for the day. Staff, interns or volunteers may save files containing EPHI to their portable workstations.

E. IT staff should verify that a workstation that is left unattended either terminates any open session or takes some other step to confirm it cannot become an avenue for unauthorized access to electronic protected health information.

AUDITING AND EMERGENCY ACCESS

A. The Network Specialist should verify that hardware, software, or procedural mechanisms are implemented in order to record and examine activity in Diversus Health information systems that contain or use electronic protected health information.

B. The IT Director will establish and implement procedures for obtaining necessary electronic protected health information during an emergency.

ASSESSMENT OF Diversus Health SOFTWARE NEEDS IN RELATON TO THE SECURITY RULE:

A. Diversus Health makes every effort possible to encrypt EPHI data both at rest and in-transit. All data stores of EPHI must be encrypted either by SQL Transparent Data Encryption (TDE) or other proprietary encryption method. All EPHI must be transmitted in encrypted format such as Secure FTP or other method.

B. After conducting a thorough assessment of relevant factors, including those outlined by HHS in the privacy regulation, Diversus Health has determined that Electronic Authentication Mechanisms are not reasonable in its work environment.
   1. The Records Manager should confirm that non-electronic mechanisms are used to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

REFERENCE:

- 45 CFR §164.310
- 45 CFR §164.312

Policy: HIPAA-8270

TITLE: 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 protected health information (PHI), in any form. All protected health information 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 networks sites and servers only when necessary. Only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure should be transported. All protected health information in paper or electronic form must be transported and stored in a secure manner to safeguard it against improper disclosure or loss.

TRANSPORTATION AND STORAGE OF PHI:

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

1. Employees, subcontractors, interns or volunteers who transport PHI must be aware of the possibility of that motor vehicle accidents can occur which could provide unauthorized access to items within the vehicle. In addition, motor vehicles can be inappropriately accessed for the purpose of theft of the contents of the vehicle. 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.

2. Physical PHI transported in a Motor Vehicle must be maintained during transport in a locked container, briefcase or bag that is approved by the Diversus Health HIPAA Privacy Officer. The locked container should be placed in the trunk or another part of the vehicle that is not visible from outside the vehicle.

3. The employee, subcontractor, intern or volunteer must be physically present in the vehicle at all times while PHI is in the vehicle.

4. Employees, subcontractors, interns or volunteers shall only transport the minimum necessary to perform their job duties.

B. If it is necessary to store physical PHI or e-PHI in a location outside a secure location such as a contractor's home office, the PHI must be placed in a secure, locked file cabinet or other locked container. Every effort should be made to keep PHI secured from access by family members and others.

C. If PHI is lost or stolen, or improperly accessed by others, the employee, subcontractor, intern or volunteer should notify the Privacy Officer and file a police report if the improper access involved theft.

D. Employees, subcontractors, interns or volunteers 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, subcontractor, intern or volunteer's immediate supervisor as soon as possible regardless of whether PHI has been compromised.

REFERENCE:

- 42 CFR §164.530(c)

Related Polices/Resources: NA

Effective Date: 7/10/20 Approved By: Policy Review Council

Last Revision Date: 7/11/25 Owner: Compliance Officer