HEALTH DATA VISION, INC.
REALIZING THE POSSIBILITIES

HIPAA Policies and Procedures

Created:
1/1/2017
Health Data Vision Proprietary & Confidential

Publication Note

This guide is published by Health Data Vision, Inc. exclusively for the use of HDV employees, authorized agents, and affiliated companies.

It contains HDV confidential and proprietary information, and under no circumstances should it be delivered or disclosed to any person not employed by HDV, its authorized agents, or affiliated companies, without the expressed written authorization of an officer of HDV.

Trademarks

All trademarks acknowledged

Document History

Version	Date	Updated By	Comments
1.0	**1/1/17**	**Bryan Lee**	**Annual Renewal**
1.1	**9/5/17**	**Jay Ackerman**	**Review & Update**

Introduction

A. General Policy Statement

Health Data Vision, Inc.(HDVI) is committed to protecting the privacy, security, confidentiality, integrity and availability of individually identifiable protected health information 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 HDVI employees, subcontractors, Business Associates, vendors, volunteers and interns. All individuals representing HDVI will take responsibility for safeguarding protected health information to which they have access.

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, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003.

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.

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 Data Vision, Inc.	**Policy & Procedure** **HIPAA Compliance and Security Officers**	**Function** HIPAA
		Number HIPAA-100
		Prior Issue
		Effective Date 01-01-2017

POLICY

Health Data Vision, Inc.(HDVI) 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 HDVI, a healthcare provider, health plan, employee, subcontractor or healthcare clearing house; 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.

As changes occur in the law, including standards, implementation, specifications or other requirements of the HIPAA regulations, HDVI 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.

HIPAA-100.1 – IDENTIFICATION OF COMPLIANCE OFFICER PROCEDURES:

A. HDVI has appointed a Compliance 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 Compliance Officer notifies the Executive Management Team 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. Develops staff training on HIPAA policies, procedures and practices.
   4. Monitors participants to ensure that all staff receive HIPAA training as described in Policy 102.1.
   5. Maintains updated Notice of Privacy Practices that is distributed in accordance with these procedures.

6. Manages any disclosures of information, including the preparation and maintenance of mandatory reporting.
7. Responds to Requests for Amendments of Protected Health Information.
8. Investigates and respond to complaints regarding the confidentiality of information.
9. Updates privacy and security forms and coordinates the placement of these forms on the HDVI intranet.

HIPAA-100.2 – IDENTIFICATION OF SECURITY OFFICER PROCEDURES:

A. HDVI 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. The Security Officer notifies the Executive Management Team of any policies, procedures or implementation issues that need their review;
   2. Assists with the development 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 HDVI; 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 regularly review records of the activity within the information systems of HDVI. As part of the review, the Security Officer should review the list of logs still in process

DISCLAIMER

These privacy and security policies, as they exist or may be amended in the future, are intended to be used by HDVI employees, subcontractors, interns, volunteers, providers, Board of Directors or its agents in meeting their responsibilities to HDVI. Violation of a policy can be the basis for discipline or termination of employment or an association with HDVI. 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 HDVI, 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)

Health Data Vision, Inc.	**Policy & Procedure** **HIPAA Privacy and Security Definition of Terms**	**Function** HIPAA
		Number HIPAA-101
		Prior Issue
		Effective Date 01-01-2017

POLICY

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 HDVI should consult with the Compliance or Security Officer if they have any questions.

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

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 Protected Health Information 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 HDVI that involves the use or disclosure of Protected Health Information. A business associate might also be a person or entity that provides residential or day programs, community participation, therapy, 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 to carry out treatment, payment or healthcare operations. Consent is not required under the privacy rule.

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

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

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

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

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

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 HDVI. The two types of disclosure are:

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

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 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 HDVI 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 HDVI, 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 HDVI 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 HDVI, and marketing for which an individual authorization is not required.

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

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

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 full 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 have not been altered or destroyed in an unauthorized manner.

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

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

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

- Communications by a covered entity for 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 HDVI 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 non-discrimination 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, HDVI 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 HDVI.

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, HDVI 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.

Compliance Officer: HDVI staff member who has been designated, pursuant to the Privacy Rule, with responsibility for ensuring HDVI's 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 full describe the Privacy Rule.*

Protected Health Information (PHI): Any health information maintained by HDVI that is individually identifiable except: (a) employment records held by HDVI in its role as an employer; and, (b) information regarding a person who has been deceased for more than fifty (50) years. 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 HDVI 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 should be kept separate from the rest of the master 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 HDVI's 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 the 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 HDVI.

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 HDVI, including the coordination or management of services by HDVI with a third party; consultation with other providers relating to a person served; or the referral of a person served for services between HDVI 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 in order 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 HDVI 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 HDVI. (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 HDVI, is under the direct control of HDVI, whether or not they are paid. Members of the workforce are not business associates.

REFERENCE:

- 42 CFR §160.103

Health Data Vision, Inc.	**Policy & Procedure** **HIPAA Privacy and Security Rule Training**	**Function** HIPAA
		Number HIPAA-102
		Prior Issue
		Effective Date 01-01-2017

POLICY:
Health Data Vision, Inc. (HDVI) provides HIPAA privacy and security training to employees, subcontractors, interns and volunteers who should come into contact with PHI while performing their job functions.

HIPAA-102.1 – PROCEDURES FOR HIPAA PRIVACY AND SECURITY RULE TRAINING:

A. The Compliance Officer, in concert with Human Resources staff, should establish separate or combined privacy and security training courses.

B. HDVI staff, interns and volunteers should be trained or retrained.
   1. Within 30 days of employment with HDVI.
   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 Compliance Officer determines the individual have disregarded privacy laws, policies or procedures.

C. Human Resources staff should document each training session and the names of HDVI staff that completed the training. Such documentation should be maintained in HDVI's personnel files maintained by Human Resources Department. The supervisors of interns and volunteers should document their HIPAA training when itoccurs.

D. Discipline for Non-Compliance: Human Resources (HR) should implement the same procedures to discipline and hold HDVI 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 HDVI's Privacy or Security policies or procedures, or in the HIPAA Privacy or Security Regulations, the Compliance and Security Officer should work with Human Resources 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 HDVI employees, subcontractors, interns or volunteers are involved in a privacy or security incident that was not the result of malicious or willful conduct, the Compliance Officer (or their designees)

should provide the offending individual with additional training regarding HDVI 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, the Compliance Officer should issue a training reminder to employees, subcontractors, interns and volunteers that focuses on the privacy/security issue involved in the incident and how to avoid it in the future. If the Compliance Officer becomes aware of recurring security lapses, the Compliance Officer should issue a reminder to employees, subcontractors, interns and volunteers regarding the lapse and the appropriate way to handle the issue in light of HDVI's policies and procedures.

H. In order to safeguard ongoing privacy compliance and information security, the Compliance Officer (or their designees) may provide periodic privacy or security reminders to HDVI 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. HDVI maintains the documentation of its training of its employees, subcontractors, interns and volunteers for a period of six (6) years.

REFERENCE:

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

Health Data Vision, Inc.	**Policy & Procedure** **Notice of Privacy Practices**	**Function** HIPAA
		Number HIPAA-103
		Prior Issue
		Effective Date 01-01-2017

POLICY:

Health Data Vision, Inc. (HDVI) 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. HDVI requests that each person receiving a copy of the Notice of Privacy Practices at the time of application acknowledges their receipt in writing.

HIPAA-103.1 – 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 HDVI;
   2. The rights of a person with respect to his/her PHI; and
   3. HDVI 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 HDVI. At a minimum, HDVI should make certain the Notice in Spanish translation is available.

C. HDVI intake 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, HDVI intake 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 - Acknowledgement of Receipt Form. The Notice of Privacy Practices - Acknowledgement of Receipt Form should be attached to the person's official record.

E. If the person applying for services, the parent of a minor, legal guardian or personal representative refuses or is otherwise unable to sign the Notice of Privacy Practices - Acknowledgement of Receipt Form, intake staff should ask them to verbally acknowledge that they have received a copy Notice of Privacy Practices and write "Verbal" on the appropriate signature line of the Acknowledgement of Receipt. Staff should then initial and date next to word "Verbal". This document is then attached to the person's official record.

F. HDVI staff should provide a copy of the written Notice of Privacy Practices to persons served and to other persons upon request.

G. The Compliance Officer should post a copy of the Notice of Privacy Practices in a clear and prominent location such as the entrance lobby at HDVI's various offices and facilities.

H. A current version of the Notice of Privacy Practices should be maintained on the HDVI's website, and intranet.

I. Whenever the Notice of Privacy Practices is revised, HDVI's Compliance Officer should make the revised Notice of Privacy Practices available upon request on or after the effective date of the revision; and

1. The revised Notice of Privacy Practices should be posted in a clear and prominent location.
2. A copy of each Notice of Privacy Practices issued by HDVI 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 directly to the Compliance Officer. (See the Procedure HIPAA-119 "Breach Notification Requirements")

REFERENCE:

- 42 CFR § 164.520

Health Data Vision, Inc.	**Policy & Procedure** **Designated Record Set**	**Function** HIPAA
		Number HIPAA-104
		Prior Issue
		Effective Date 01-01-2017

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

HIPAA-104.1 – DESIGNATED RECORD SET PROCEDURES:

A. If records from other providers are used by the HDVI 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 HDVI's 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. Maintenance of privacy and security of these records is coordinated with the Compliance Officer.

REFERENCE:

- 45 CFR §164.501 (1)

Health Data Vision, Inc.	**Policy & Procedure** **Minimum Necessary Uses and Disclosures of Protected Health Information (PHI)**	**Function** HIPAA **Number** HIPAA-105 **Prior Issue** **Effective Date** 01-01-2017

POLICY:

When using or disclosing Protected Health Information (PHI), Health Data Vision, Inc. (HDVI) 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 HDVI:

- HDVI 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.
- HDVI limits access to, and use of, the protected health information of persons served in accordance with its business associate agreements with vendors and providers.
- HDVI 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.

HIPAA-105.1 – MINIMUM NECESSARY STANDARD WHEN REQUESTING PHI:

A. When requesting PHI from another entity, HDVI 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, HDVI 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)

Health Data Vision, Inc.	**Policy & Procedure** **Safeguarding Verbal and Written Protected Health Information (PHI) and Storing PHI**	**Function** HIPAA
		Number HIPAA-106
		Prior Issue
		Effective Date 01-01-2017

POLICY:
All employees, subcontractors, Business Associates, vendors, interns and volunteers are responsible for the privacy and security of PHI of persons receiving services. Health Data Vision, Inc. (HDVI) Compliance Officer is responsible for periodically monitoring to ensure that uses and disclosure of PHI complies with applicable Federal, State and/or local law or regulation, and these policies.

HIPAA-106.1 – 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 HDVI 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.

HIPAA-106.2 – 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 from an MRCS workstations unless it is signed out in accordance with HDVI 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.

HIPAA-106.3 – 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 Chief Compliance Officer or a designee should monitor storage and security of such hardcopy master records.

B. The Chief Compliance Officer 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 should are not accessible to unauthorized individuals.

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

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. In the event that the confidentiality or security of PHI stored in an active or inactive master record has been breached, the Compliance Officer should be notified immediately.

REFERENCE:

- 42 CFR §164.530 (C) (1) & (2)

Health Data Vision, Inc.	**Policy & Procedure** **Safeguarding Protected Health Information with Office Equipment and Mobile Devices**	**Function** HIPAA **Number** HIPAA-107 **Prior Issue** **Effective Date** 01-01-2017

POLICY:
Health Data Vision, Inc. (HDVI) 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 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.

HIPAA-107.1 – PROCEDURES FOR SAFEGUARDING PHI WHEN USING COMPUTERS:

A. Staff, interns 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. On each workstation chassis, securely closed anti-tamper devices should be installed by the Security Officer or his/her designee.
   5. 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 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 are authorized to access the main server are 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 Compliance Officer, and their Supervisor.

HIPAA-107.2 – PROCEDURES FOR SAFEGUARDING PHI WHEN USING PRINTERS, COPIERS OR SCANNERS:

A. HDVI 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. Documents containing PHI should be promptly removed from the printer and or copier/scanners and placed in an appropriate and secure location.

D. 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.

HIPAA-107.3 – PRIVACY AND SECURITY PROCEDURES FOR PORTABLE DEVICES AND MEDIA:

A. Employees, subcontractors, interns and volunteers should limit the use of assigned portable computers, BlackBerry and tablet devices or any HDVI provided resource or device that contains or can access client PHI, to HDVI staff only.
   1. HDVI 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 Privacy/Security Officers.
   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 with "Property of HDVI" and device identification number should be installed on portable computers, 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 Privacy and or Security Officer. When using removable media or memory devices is absolutely necessary, employees, interns or volunteers should:
   1. Ensure that a departmental policy exists to allow the use of flash drives or obtain approval from a direct supervisor.
   2. Ensure that the flash/thumb drive is encrypted.
   3. 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;
   4. 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.)

5. Not store older documents on removable media; they should be archived to HDVI's 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 HDVI issued portable computer and tablet users, assigned equipment serial numbers and software. HDVI 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 never leave them unattended for any time period, in a vehicle overnight or for an extended period of time;
   2. 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 HDVI 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)

Health Data Vision, Inc.	**Policy & Procedure** **Transmitting Protected Health Information through Email or Fax**	**Function** HIPAA
		Number HIPAA-108
		Prior Issue
		Effective Date 01-01-2017

POLICY:
In the course of providing services to clients, Health Data Vision, Inc. (HDVI) staff, interns and volunteers may communicate PHI via email or facsimile (fax), but under highly restricted circumstances. The preferred method for transmitting PHI is through the MRCS Management Portal. Care should be taken that the PHI transmitted in these instances is safeguarded from inappropriate use, disclosure or access.

HIPAA-108.1 – 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 HDVI employees, subcontractors, interns or volunteers, or to persons external to HDVI, 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 unprotected via email within HDVI's secured, internal network.
   1. Highly sensitive PHI such as information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes should not be sent via email, even within the internal email system.

E. When sending PHI outside of the HDVI network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information.
   1. HDVI email that contains PHI that is sent or forwarded to an external email address should be encrypted by entering *secure* in the email subject line of Microsoft Outlook.
   2. 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.
   3. 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.
   4. PHI including billing information should always be routed in an encrypted format.
   5. PHI including billing information should be routed in a protected format (such as PDF)

F. Non-encrypted email containing PHI should not be transmitted, the use of the MRCS Management Portal is recommended.

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 HDVI.

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

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

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

HIPAA-108.2 – 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. Unless otherwise prohibited by State law, information transmitted via facsimile is acceptable and may be included in the master record of the person served.

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

D. 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 HDVI of a fax number change.
   3. Confirming the accuracy of the recipient's fax number before pressing the submit function.

E. 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).

F. 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. Notify the HDVI Compliance Officer of misdirected fax.

G. Specifically assigned HDVI staff may be provided with RightFax software on their workstation. Staff should refer to RightFax guides for further information on how to use it.

REFERENCE:

- 42 CFR §164.530

Health Data Vision, Inc.	**Policy & Procedure** **Authorizations to Release Protected Health Information and Disclosure of PHI**	**Function** HIPAA **Number** HIPAA-109 **Prior Issue** **Effective Date** 01-01-2017

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, HDVI should disclose PHI only as authorized by the Chief Compliance Officer (CCO) or his/her designee. In some instances, the CCO may need to track information that is disclosed.

HIPAA-109.1 – EXCEPTIONS TO AUTHORIZATION REQUIREMENTS PROCEDURES:

A. When HDVI receives a request for disclosure of PHI, the Compliance Officer, or his/her designated Records staff, should determine whether an authorization is required prior to disclosing the PHI. PHI may be disclosed by the Compliance Officer of his/her designee without an authorization if the disclosure is:
   1. For official HDVI operations such as for the purpose of:
      a. Diagnostic Coding or Quality Measure Abstraction;
      b. Image Quality Assurance and,
      c. Verification of receipt of appropriate documentation.
   2. In limited circumstances, for the healthcare operations of another Business Associate.
   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. HDVI 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.

HIPAA-109.2 –PROCEDURES FOR DISCLOSURE PURSUANT TO AN AUTHORIZATION:

A. When the CCO, or his/her designee, determines that a written authorization is required prior to disclosing PHI, the CCO or his/her designee 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, the Compliance Officer or his/her designated Records staff should notify the requestor that HDVI is unable to provide the PHI requested. The requestor should be supplied with an Authorization to Use or Disclose PHI form.
    2. The Compliance Officer or his /her designated 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, the Compliance Officer or his/her designated 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. HDVI 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, the Compliance Officer should contact HDVI legal counsel.

B. If the request for disclosure is accompanied by a written authorization, the Compliance Officer, or his/her designated 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 HDVI staff for assistance.
    2. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Compliance Officer 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, the Compliance Officer or his/her designated 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 HDVI staff members may not release master records without the approval of the Compliance 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.
    1. 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.
    2. Emergency release of information should be documented in primary information system (CaseTrakker / Dynamo) as to the justification.

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.

HIPAA-109.3 –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).

HIPAA-109.4 – 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 HDVI staff that he/she wants to revoke the authorization, HDVI employees, subcontractors, interns or volunteers should obtain a copy of the official authorization (hardcopy or printed electronic) and complete the shaded area at the bottom of the form:

"NOTE: This Authorization was revoked on (DATE)_____Signature of Staff:_____".

B. Upon receipt of a written revocation, HDVI 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 Compliance Officer 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)

Health Data Vision, Inc.	**Policy & Procedure** **Responding to a Subpoena**	**Function** HIPAA
		Number HIPAA-110
		Prior Issue
		Effective Date 01-01-2017

POLICY:

From time to time, employees, subcontractors and others associated with Health Data Vision, Inc. (HDVI) 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 HDVI may receive notification, or field questions or requests for information and documents, from Federal, State, or local authorities regarding an investigation. HDVI 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.

HIPAA-110.1 – PROCEDURES FOR RESPONDING TO A SUBPOENA OR INVESTIGATIVE DEMAND:

A. Employees, subcontractors, interns, volunteers and others associated with HDVI who are served with a formal or informal request for information, testimony or documents relating to any person served by HDVI, or to HDVI itself, should promptly advise their supervisor and the Chief Compliance Officer (CCO).
   1. The CCO should coordinate responding to the request and provide direction to staff on their response.

B. Employees, subcontractors, interns, volunteers and others associated with HDVI who receive notification, or field questions, from Federal, State, or local authorities regarding an investigation should promptly advise the CFO.
   1. The CCO should coordinate responding to the request and provide direction to staff on their response.

C. The CCO or his/her designee should seek the advice of counsel before responding to any subpoenas, court orders or investigatory requests for information.

REFERENCE:

- 42 CFR §164.512(e)

Health Data Vision, Inc.	**Policy & Procedure** **Accounting of Disclosures of Protected Health Information**	**Function** HIPAA
		Number HIPAA-111
		Prior Issue
		Effective Date 01-01-2017

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.

HIPAA-111.1 – PROCEDURES FOR ACCOUNTING OF DISCLOSURES OF PHI:

A. Upon receiving an inquiry about disclosures of PHI, the Compliance Officer 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 HDVI HIPAA related privacy forms and letter templates should be maintained on HDVI's intranet.

B. The Compliance Officer should review and process the request.

C. The written accounting of disclosures is provided to the requestor using a format created and maintained by Chief Compliance Officer (CCO).
   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 CCO 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 CCO 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 CCO 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 CCO should provide the written accounting of disclosures no later than 60 days after receipt of the request.
   1. If HDVI is unable to meet the 60-day time frame, HDVI 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 HDVI should provide the accounting.

E. HDVI 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, HDVI may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided HDVI has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.

F. HDVI 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.

HIPAA-111.2 – 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

Health Data Vision, Inc.	**Policy & Procedure** **HIPAA Privacy Complaints**	**Function** HIPAA
		Number HIPAA-112
		Prior Issue
		Effective Date 01-01-2017

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
- HDVI's Notice of Privacy Practices does not reflect current practices accurately.

HIPAA-112.1 – HIPAA PRIVACY COMPLAINT PROCEDURES:

A. All concerns/complaints should be directed to the Chief Compliance Officer (CCO), by telephone, fax, mail, email, or in person. The person making the complaint should put their complaint in writing, either through a letter, or email. The CCO should document the complaint in the log of complaints regarding privacy issues.

B. Once the complaint form and log are completed correctly, the Chief Compliance Officer (CCO) will determine whether an investigation is warranted. The CCO should assemble an Investigative Team, as needed, composed of appropriate individuals based upon the circumstances of the complaint.

C. Following completion of the investigative team's review, the Chief Compliance Officer should be notified of the substance of their findings and decision. The Compliance Officer should:
   1. Document the outcome of the complaint.
   2. Complete the log of complaints by entering the resolution and any required follow-up actions.

D. The Chief Compliance Officer 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.

E. Employees, subcontractors, interns and volunteers may not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against the person filing a complaint.

REFERENCE:

- 42 CFR §164.530(d)

Health Data Vision, Inc.	**Policy & Procedure** **De-Identification of Protected Health Information**	**Function** HIPAA
		Number HIPAA-113
		Prior Issue
		Effective Date 01-01-2017

POLICY:

Health Data Vision, Inc. (HDVI) should convert the PHI of client documentation received 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 HDVI policy HIPAA-109.
- Information is used or shared without the authorization of the person served, the parent of a minor, legal guardian or personal representative authorization.

HIPAA-113.1 – PROCEDURES FOR DE-IDENTIFICATION OF PHI:

A. Before staff treats any information as being de-identified, it should be submitted to the Compliance 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, the Compliance Officer 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.

HIPAA-113.2 – PROCEDURES FOR RE-IDENTIFICATION OF PHI:

A. During the process of de-identifying PHI, the Compliance or Security Officer, or consultants performing statistical de- identification, should assign a code that allows the information to be re-identified by HDVI 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. HDVI 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 Compliance Officer. If information is re-identified, the Compliance Officer should oversee the process of doing so.

REFERENCE:

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

Health Data Vision, Inc.	**Policy & Procedure** **Business Associates**	**Function** HIPAA
		Number HIPAA-114
		Prior Issue
		Effective Date 01-01-2017

POLICY:

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

HIPAA-114.1 – PROCEDURES FOR BUSINESS ASSOCIATES:

A. HDVI 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. HDVI contracts staff, in collaboration with the Chief Financial Officer (CFO) 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. HDVI 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 HDVI.

C. If a BA Agreement is necessary and the other party provides its own BA Agreement, the CCO 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, HDVI contracts staff should submit HDVI's BA Agreement for approval by the other party.

E. If the BA refuses to sign the Agreement, the Privacy Rule prohibits HDVI 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 HDVI, HDVI should not contract with the BA.

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

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

HIPAA-114.2 – PROCEDURES FOR BREACH OF A BA AGREEMENT AND SANCTIONS:

A. If HDVI staff learns of a breach or violation of a BA requirement by a BA, such breach or violation should be reported to the (CFO) or 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, HDVI 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.

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

C. 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

Health Data Vision, Inc.	**Policy & Procedure** **Marketing and Fundraising**	**Function** HIPAA
		Number HIPAA-115
		Prior Issue
		Effective Date 01-01-2017

POLICY:

Health Data Vision, Inc. (HDVI) must not use Protected Health Information in its marketing or communication materials.

HIPAA-115.1 – PROCEDURES FOR USING PHI FOR MARKETING:

A. The Privacy Rule defines marketing as communication that encourages an individual to use or purchase a product or service

B. HDVI staff shall not use or disclose any PHI while conducting marketing activities, including, but not limited to, demonstrations or promotions of HDVI services and/or solutions.

C. Business associates and other third parties:
   1. HDVI may engage third parties to conduct permitted marketing activities on HDVI's behalf, however those marketing activities shall not use or disclosure any PHI.
   2. HDVI may not sell or disclose PHI to a third party to help the third party market its own products or services.

HIPAA-115.2 – PROCEDURES FOR USING PHI FOR FUNDRAISING

A. HDVI shall not use or disclose any PHI while conducting fundraising activities.

REFERENCE:

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

Health Data Vision, Inc.	**Policy & Procedure** **Breach Notification Requirements and Investigations**	**Function** HIPAA
		Number HIPAA-116
		Prior Issue
		Effective Date 01-01-2017

POLICY:

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

HIPAA-116.1 – 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 Compliance Officer (or, in the absence of the Compliance Officer, reports may be made to the Security Officer).
   1. HDVI staff should report any suspected breach of unsecured PHI to the Privacy/Security Officer as soon as possible, within 48 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 HDVI under a Business Associate Agreement.

C. The report should be provided to the Compliance Officer and/or Security Officer.

D. HDVI maintains an open-door policy regarding compliance with HIPAA. Employees, subcontractors, interns and volunteers are encouraged to speak with the Privacy/Security Officer or other appropriate individual regarding any concerns they may have with HDVI's 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. Periodic HIPAA training should be provided so that employees, subcontractors, interns and volunteers understand their responsibilities in relation to HIPAA policies and procedures. Training opportunities may occur at staff meetings, emails, via online training or informally posting important updates on the office bulletin board.

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

HIPAA-116.2 – PROCEDURES FOR INVESTIGATION OF A REPORTED BREACH OF CONFIDENTIALITY:

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

B. The Compliance Officer and/or Security Officer should determine if there is a concern regarding a possible violation of HIPAA or HDVI's policies or procedures related to HIPAA. If the Privacy/Security Officer determines there is a concern, he/she should notify the CEO and Management Team.

C. If the CCO determines an investigation is needed, it should begin promptly. The CCO should determine who will conduct the investigation.

D. If, at the conclusion of the investigation, it is found that a violation of HDVI's policy or procedure has occurred, staff conducting the investigation should notify the CCO.
   1. The CCO, in consultation with the Director 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.
   2. Documentation of findings and final actions from the investigation should be maintained as a part of HDVI 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 CCO 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.

G. HDVI 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 Chief Compliance Officer. The Chief Compliance Officer should treat such a report as a complaint and investigate it accordingly.

HIPAA-116.3 –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 HDVI 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)

Health Data Vision, Inc.	**Policy & Procedure** **Sanctions for Failure to Comply with HIPAA**	**Function** HIPAA
		Number HIPAA-117
		Prior Issue
		Effective Date 01-01-2017

POLICY:

Employees, subcontractors, interns or volunteers of Health Data Vision, Inc. (HDVI) 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 HDVI.

HIPAA-117.1 – 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 HDVI and/or restitution in accordance with HDVI policies. The following three (3) levels of violations shouldbe 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 HDVI, 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 HDVI 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 a 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 HDVI's privacy or security policy or procedure or to the Compliance or Security Officer;
g. Logging into the HDVI 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 Chief Compliance Officer (CCO) 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.

HIPAA-117.2 – 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 HDVI in accordance with the terms of the BA Agreement currently in effect at the time of the breach.

B. Prior to HDVI 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, HDVI 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 HDVI'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 HDVI or to provide a service described in the HIPAA Privacy Rule's definition of a business associate to HDVI, HDVI 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. HDVI attempts in good faith to obtain satisfactory assurances, as stated above; and,
2. If that attempt fails, the CCO 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)

Health Data Vision, Inc.	**Policy & Procedure** **Retention of Protected Health Information**	**Function** HIPAA **Number** HIPAA-118 **Prior Issue** **Effective Date** 01-01-2017

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 six (6) years for a Covered Entity. Because HDVI is a Business Associate of the Covered Entity, Retention rules only pertain when the Covered Entity delegates its responsibility. For most clients, HDVI contracts will state that retention is only required during the term of the engagement, after which all PHI is to be destroyed. In cases where the Client has delegated to HDVI retention responsibilities, HDVI will follow these retention procedures:

HIPAA-118.1 – RETENTION OF PHI PROCEDURES:

A. If State laws and regulations require a greater retention time period, the greater should be followed. HDVI should review State laws and regulations to determine master record retention period.

B. HDVI 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.

C. 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.

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

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)

Health Data Vision, Inc.	**Policy & Procedure** **Destruction of Protected Health Information**	**Function** HIPAA
		Number HIPAA-119
		Prior Issue
		Effective Date 01-01-2017

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, HDVI should determine if PHI has been stored in this equipment and delete PHI prior to the disposal of the equipment.

HIPAA-119.1 – 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 the Compliance Officer or his/her designee 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 Compliance Officer should verify the retention period has expired.

D. If the records are destroyed off-site through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.

E. HDVI should maintain destruction documents permanently.

HIPAA-119.2 – 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 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.

B. Backup or data tapes are typically re-used many times but generally only by the Information Technology group within HDVI, which routinely handles the PHI of persons served. However, there may be situations where tapes are sent to external recipients for specific processing.
   1. Tapes used for this purpose should be segregated from the general pool used for backups. These tapes should be degaussed prior to use in creating the files being sent to verify that no prior PHI of persons served remains on that portion of the tape beyond the end of the current file.
   2. Tapes or diskettes that are being decommissioned should be degaussed before disposal. This can be accomplished using a bulk tape eraser. Alternatively, the media may be pulverized or shredded.

C. Compact disks (CDs) and other electronic media: CDs and electronic media containing PHI should be cut into pieces or pulverized 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**

Health Data Vision, Inc.	**Policy & Procedure** **Maintaining Security of Electronic PHI (ePHI)**	**Function** HIPAA
		Number HIPAA-200
		Prior Issue
		Effective Date 01-01-2017

POLICY:

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

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

HIPAA-200.1 – PROCEDURES FOR MAINTAINING THE SECURITY OF ePHI:

A. HR staff should perform a background check on each staff prior to the staff being hired. The background check should include a check of references and a criminal background check.

B. When employees, subcontractors, interns, and volunteers begin work at HDVI, 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.

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

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

E. The Facilities 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.

F. Employees, subcontractors, interns and volunteers who access ePHI without authorization are subject to the sanctions listed in HDVI's policy and procedure HIPAA-120.

G. When a staff changes positions within HDVI 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.

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

1. 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.
2. The IT Director or his/her designee should remove accounts for the former staff within one hour of the staff leaving the premises. For any accounts to which the staff had publicly know passwords, or passwords that cannot be closed, the IT Director or his/her designee should change the passwords immediately.

HIPAA-200.2 – 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 Compliance Officer). Staff should also report if they detect evidence that a security incident may be imminent.
   1. HDVI staff should report any suspected breach of unsecured ePHI to the Security/Compliance 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 his/her designee should immediately take steps to isolate those systems that have been affected or compromised by the incident from the rest of HDVI's 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 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 HDVI's HIPAA Breach Notification Rule.
2. The Security Officer should take steps to mitigate the harm from the security incident by following HDVI'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.

HIPAA-200.3 – PROCEDURES FOR BACKUP, RECOVERY AND EMERGENCY PREPAREDNESS:

A. Data Backup Plan: HDVI 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. HDVI'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 Director 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 re- usable media.

C. Disaster Recovery Plan: HDVI 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 Director should be responsible for implementing procedures to restore any lost data from the exact copies created and stored pursuant to HDVI's Data Backup Plan, above.
2. The disaster recovery plan should be part of HDVI's Emergency Preparedness/Contingency Plan that should be implemented in the event of an emergency or other unanticipated event that disrupts HDVI's IT system functionality.

D. Emergency Preparedness/Contingency Plan: The IT Director 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 HDVI workforce members and operations.

E. The IT Director 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)

Health Data Vision, Inc.	**Policy & Procedure** **Physical Safeguards to Maintain the Security of Electronic PHI**	**Function** HIPAA
		Number HIPAA-201
		Prior Issue
		Effective Date 01-01-2017

POLICY:
HDVI 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.

HIPAA-201.1 – PHYSICAL SAFEGUARD PROCEDURES:

A. HDVI 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 HDVI's 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 HDVI's procedures to review and modify access to ePHI.
   4. Whenever a physical component of HDVI's facilities and locations that is related to the security of facilities and locations, is repaired, re-placed, 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. HDVI should implement physical measures designed to protect its information systems and locations from natural disasters, and environmental hazards.
   1. HDVI 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 HDVI's disaster recovery and emergency mode operations plans.

HIPAA-201.2 – COMPUTER HARDWARE ASSET TRACKING PROCEDURES:

A. HDVI'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 HDVI's departments. This inventory should be recorded on HDVI's Fixed Asset accounting software.

B. In addition to the annual inventory, the IT Director 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 HDVI's Finance department. Finance department staff should then update the master inventory list based upon the information provided in the update.

HIPAA-201.3 – 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 at least 8 rewrites are performed.

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 HDVI 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, HDVI stores ePHI on removable magnetic storage media (such as external hard drives, floppy disks, or zip drives) or non-rewritable optical storage (such as CD-ROMs). When HDVI 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, HDVI stores ePHI on rewritable optical media (such as rewritable CDs). When HDVI determines that it is appropriate to dispose of these rewritable discs, IT staff should verify that the discs are erased. This should be done by using the appropriate software to return the CD-RW to a pristine state. Simply deleting the table of contents is not sufficient.

F. In some situations, HDVI stores electronic protected health information to flash drive media. When HDVI 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

Health Data Vision, Inc.	**Policy & Procedure** **Technical Safeguards to Maintain the Security of Electronic PHI**	**Function** HIPAA
		Number HIPAA-202
		Prior Issue
		Effective Date 01-01-2017

POLICY:
HDVI 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.

HIPAA-202.1 – PROCEDURES FOR ESTABLISHING AUTHORIZED USERS OF HDVI's 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.

B. The Network Operations Manager should create a unique identifying name for each user. The number upon the user unique identifying name should be derived from the first initial of the user's first name and the user's last name.
   1. The Network Operations Manager 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 of HDVI's information systems.
   2. For new accounts, the Network Operations Manager should provide the staff with appropriate levels of access by following HDVI's 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 HDVI's information systems.
   1. Users should establish passwords that conform to the requirements of HDVI's password requirements.
   2. The IT Director, 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.

HIPAA-202.2 – SAFEGUARDING ePHI AND HDVI's 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 an HDVI 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 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 HDVI's environment and to prevent the propagation of malicious software due to staff failure to follow HDVI's policies and procedures.

C. HDVI should implement email encryption methodology and policies and procedures to protect ePHI from improper access during outgoing email communication.
   1. HDVI 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 use the currently recommended encryption software and activate the encryption service by typing *secure* in the SUBJECT line of an email to encrypt the email.

   2. The method for employing encryption will be included in initial Security Training, as well as any remedial or follow up HIPAA trainings.

D. HDVI 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. HDVI has determined, based upon its technical capabilities, size and budget, that a technological authentication solution is not reasonable in its environment. 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 HDVI's 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 HDVI Security Officer that the information has been altered. The HDVI Security Officer should then follow HDVI's computer security incident response procedures. The staff should not amend the electronic protected health information, but should allow HDVI 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 HDVI's procedures for faxing protected health information.

HIPAA-202.3 – SAFEGUARDING ePHI AND HDVI's 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, 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, 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 HDVI's 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 HDVI's 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 generated by the browser. It is a sanctionable offense to alter or delete the web browser history on any of HDVI's workstations.

D. Staff, interns or volunteers should not create web sites that are either hosted by HDVI's computers or accessed through HDVI's 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 HDVI's environment and to prevent the propagation of malicious software due to staff failure to follow HDVI's policies and procedures.

G. The IT Director should verify that HDVI 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 HDVI's policies and procedures on Internet usage, but should prevent unauthorized access to HDVI's 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 governing allowed and denied access. Furthermore, the firewall should be configured to initiate when the workstation, laptop or tablet is started.

HIPAA-202.4 – SAFEGUARDING ePHI AND HDVI's NETWORK THROUGH ANTI-VIRUS SOFTWARE:

A. IT staff should verify that HDVI 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.

HIPAA-202.5 – SAFEGUARDING ePHI AND HDVI's NETWORK THROUGH SETTINGS ON WORKSTATIONS, LAPTOPS AND TABLETS:

A. IT staff should make certain that each HDVI 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 HDVI 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. It is preferred that workforce save files to an encrypted flash drive whenever possible. However, such files should be saved to

the appropriate network share whenever the workforce member returns to the office.

E. Staff, interns or volunteers who are away from HDVI's office with their portable workstation should make duplicate retrievable copies of files and ePHI at the end of each business day while away. Immediately upon returning, a complete back-up should be performed in accordance with HDVI's back-up policies and procedures.

F. 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.
   1. IT staff should confirm that Dynamo Case Management software, which provides access to ePHI, terminates a session after 30 minutes of inactivity.
   2. IT staff should verify that workstations have some form of screen saver software. Additionally, IT staff should confirm that the screen saver is configured to activate after 15 minutes. IT staff should also verify that the screen saver requires a password to deactivate.

HIPAA-202.6 – 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 HDVI's information systems that contain or use electronic protected health information.
B. The Information Systems Manager will establish and implement procedures for obtaining necessary

electronic protected health information during an emergency.

HIPAA-202.7 – ASSESSMENT OF HDVI SOFTWARE NEEDS IN RELATON TO THE SECURITY RULE:

A. After conducting a thorough assessment of relevant factors, including those outlined by HHS in the Security Rule, HDVI has determined that cryptographic software is not reasonable in its work environment.

B. After conducting a thorough assessment of relevant factors, including those outlined by HHS in the privacy regulation, HDVI has determined that teleological 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.

REFERENCES

- 45 CFR §164.310
- 45 CFR §164.312

Health Data Vision, Inc.	**Policy & Procedure** **Transportation and Storage of PHI**	**Function** HIPAA
		Number HIPAA-300
		Prior Issue
		Effective Date 01-01-2017

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.

HIPAA-300.1 – 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 HDVI HIPAA Compliance Officer. The locked container should be placed in the trunk or another part of the vehicle that is not visible from outside thevehicle.

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 Compliance 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.

REFERENCES

42 CFR §164.530(c)