Document Category	Policy		
Policy Name	Confidentiality of Medical Information (HIPAA)		
Affected Program(s)	Vista Autism Services		
Effective Date	07/31/2024	Next Review Date	07/31/2025
Revision Date	12/13/2024	Version Number	1
Responsible Owner	Sabrina Delong (Director of Quality and Compliance)		
Oversight Approval	Trevor Motley (Chief Operating Officer)		

Purpose:

The purpose of the policies and procedures promulgated in this PHI Plan is to treat all information regarding the health care of clients as confidential information, recognizing that such information is the property of such clients, and that Vista receives this information solely and to serve its purposes as a provider of health care services and to protect clients and Vista from unlawful dissemination of information regarding the provision of, and payment for, treatment of clients. This document provides specific guidelines for how Vista will use and disclose PHI, outlines the rights and obligations of Vista and individuals in handling PHI, and provides forms, where needed, for documenting the use and disclosure of PHI. This policy recognizes the scalable nature of HIPAA and its regulations and is drafted to reflect the remote possibility that Vista would ever have access to PHI. These policies also undertake the protection and the security of any PHI that Vista receives or stores in electronic formats ("ePHI") and provide the groundwork for changes to ePHI security policies as the need develops.

PHI, for the purposes of the policies and procedures promulgated herein, shall have the meaning set forth in 45 C.F.R. 160.103. PHI includes any information relating to the past, present, or future physical or mental health or condition of a client; the provision of health care to a client; or the past, present, or future payment for the provision of health care to a client, where such information either identifies the client or where there is a reasonable basis to believe that the information could be used to identify the client. For the sake of clarity, individually identifiable health information of The Vista School clients collected pursuant to the implementation of their individualized education programs (including information collected through the provision of Educationally Integrated Behavioral Services) is not treated as PHI but as education records or treatment records subject to The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g ("FERPA"). In addition, if at any time The Vista School maintains solely education records or treatment records of its clients (as those terms are defined under FERPA) while conducting "covered transactions" under HIPAA, the Vista School will comply with FERPA with respect to the privacy and security of any individually identifiable health information of its students and with the "HIPAA Administrative Simplification Rules" with respect to individually identifiable health information maintained, used or disclosed in connection with said covered transactions.

Policy Statement:

It shall be the policy of The Vista Foundation and its affiliates, The Vista School and Vista Adult Services Organization, to safeguard protected health information of its clients (collectively, "protected health information" or "PHI") pursuant to the protected health information plan ("PHI Plan") reflected in the policies and procedures promulgated in this document.

This PHI Plan serves as an integral part of Vista's compliance program and is subject to the requirements of Privacy and Security Standards and other applicable requirements for protected health information promulgated by the U.S. Department of Health and Human Services ("HHS"), in accordance with the requirements of the Health Insurance Portability and Accountability Act, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, "HIPAA"), and any other related federal or state laws, regulations and standards applicable to Vista's handling of PHI.

Notwithstanding the foregoing, PHI relating to (i) substance abuse records, (ii) HIV/AIDS-related information, and (iii) psychotherapy notes is treated differently from other types of PHI and will in all instances be disclosed to third parties only pursuant to a signed authorization, unless the disclosure is for treatment purposes, or related to the payment for treatment services.

The Board of Directors of The Vista Foundation shall have ultimate authority and oversight responsibility for Vista's compliance with this PHI Plan. As set forth in more detail below, the Compliance Officer shall have day-to-day oversight responsibility for implementing and monitoring this PHI Plan (unless such duties are otherwise delegated as further provided herein).

The Director of Quality and Compliance shall be responsible for reporting PHI compliance and activities to the Board of Directors on an ongoing basis, and not less than annually. Such reports may address specific issues or concerns, or a summary thereof as may be appropriate. In addition, the Director of Quality and Compliance shall be responsible for receiving, handling, and responding to complaints made with respect to the PHI Plan, except as otherwise delegated (as provided herein) to a designated Contact Person or other appropriate designee with Vista's approval.

Vista's senior management shall have responsibility for managing the Director of Quality and Compliance duties and activities (or the delegation of such duties and activities within the organizations). Vista's senior management acting by and through the Compliance Officer, shall have responsibility to support and monitor the implementation of the PHI Plan, and the enforcement of all PHI requirements in accordance with this Plan.

Privacy Officer

Vista has designated the Director of Quality and Compliance to serve as its Privacy Officer to oversee the implementation and compliance of Vista's PHI Plan, unless such duties are otherwise delegated within the organization with Vista's approval. The Privacy Officer shall monitor and make recommendations with respect to PHI Plan compliance. The Privacy Officer shall also evaluate and make recommendations concerning any PHI complaints, incidents, issues or other specific concerns.

Security Officer

Vista has designated its Director of Infrastructure as its Security Officer to oversee the implementation and compliance of the PHI Plan with respect to ePHI. The Director of Infrastructure (as the "Security Official")

shall be responsible for overseeing the security and integrity of Vista's information technology systems and services, and for the implementation and monitoring of policies, procedures and programs that will ensure that ePHI is protected and maintained in accordance with all HIPAA requirements.

Protection of PHI

Only the following representatives of Vista are entitled to have access to PHI:

- All clinical personnel
- All personnel involved in claims and billing procedures, and
- All individuals who otherwise handle customer/resident records as part of their job.

Collectively, the personnel described above shall be referred to as the "Authorized Personnel." PHI shall only be used or disclosed by such individuals in accordance with these policies and procedures. Specifically, but without in any way limiting the applicability of Section IV(B) below, the Authorized Personnel shall use or disclose PHI as necessary to provide or coordinate "treatment" (as defined below) to/for clients. In addition, the Authorized Personnel may use and disclose PHI as needed to conduct "payment" (as defined below) and to perform certain "health care operations" (as defined below) necessary for the proper functioning of Vista operations

Authorized Personnel shall not share PHI with other staff of Vista or with third parties who are not authorized in writing to access PHI. PHI shall be kept secure and not be left lying in areas where unauthorized persons may view or otherwise access it. When PHI is not in use, it shall be kept in locked filing cabinets that are not accessible by the general public.

Authorized Personnel shall sign a confidentiality agreement providing that he/she will take all reasonable efforts to protect the confidentiality of PHI.

In no event shall Vista or any of its Authorized Personnel sell PHI in exchange for any form of remuneration of any kind.

Uses and Disclosures for which No Authorization Required

Treatment, Payment, and Health Care Operations (TPO)

It is policy of Vista to use and disclose an individual's PHI for the purposes of conducting TPO, without first obtaining the individual's authorization, in the following circumstances:

- For the purposes of Vista's TPO;
- For the treatment activities of any Vista health care provider;
- For the payment activities of another health care provider or a health plan, as long as the recipient of PHI is that provider or health plan; or
- For the purposes of assisting another health care provider or a health plan with (i) fraud and abuse detection or compliance, or (ii) quality assessment and improvement activities relating to improving health or reducing health care costs; provided that Vista and the recipient entity both have a relationship with the client who is the subject of the PHI.

Definitions:

- "Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers.
- "Payment" means activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and the provision of benefits, as well as activities undertaken by Vista or health plan to obtain or provide reimbursement for the provision of health care.

- "Health Care Operations" means certain operational and administrative tasks undertaken by Vista or health plan, including such things as (1) quality assessment and quality improvement; (2) reviewing and evaluating the competence or qualifications of health care professionals; (3) contract placement, including underwriting, premium rating and other activities relating to the creation, renewal or replacement of a health insurance or health benefits contract; (4) arranging for certain professional services such as legal or audit review services; (5) business planning and development; (6) resolution of internal grievances; (7) accreditation, certification, licensing, or credentialing activities; and (8) business management and general administrative activities of Vista.
- Any ambiguities that arise regarding whether certain activities fit into the definitions in this Section shall be resolved by contacting legal counsel.

Other Uses & Disclosures Not Requiring Authorization

Vista is permitted by law to disclose PHI, without first obtaining a client's written authorization, for the following purposes:

- Public health purposes
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Disclosures to personal representatives
- Disclosures to family members involved in an individual's care
- To avoid serious threats to health and safety
- For workers' compensation functions
- To protect victims of abuse, neglect or domestic violence; and
- To effect certain other government functions.

Limitation: Each of the above disclosures is subject to a number of legally mandated conditions, limitations and exceptions. All questions relating to the appropriate use and disclosure of PHI for the above purposes shall be resolved by contacting the Privacy Officer.

Verification of Individuals or Entities Requesting Access to PHI

Vista shall take all steps necessary to verify and document the identity and legal authority of persons and entities requesting access to a client's PHI. Such verification may include checking forms of identification, such as driver's license, birth certificate, agency badge (if requestor represents a government entity), letterhead, or other forms of verifying the veracity of the requestor's identity and authority to access PHI. Verification of the requestor's identity and authority will be documented on the Authority/Identity Verification form.

Minimum Necessary Policy

For third party disclosures that do not require the execution of an authorization, Vista will follow proper procedures to ensure that only the minimum amount of PHI necessary to accomplish the specific purpose of a use or disclosure is used or disclosed.

Authorized Personnel shall utilize only the minimum amount of PHI necessary to accomplish the specific purposes for which they are using the PHI.

This Minimum Necessary policy does not apply to the following uses or disclosures of PHI:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the client who is the subject of the PHI;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Health and Human Services;

- Uses or disclosures required by law; and
- Uses or disclosures required in order for Vista to comply with applicable laws and regulations.

Individual Rights

Notice of Privacy Practices

Vista will provide a formal notice to clients describing the ways in which Vista uses and discloses protected health information, and all rights that clients have with regard to their protected health information maintained by Vista.

Vista shall attempt, in good faith, to obtain written acknowledgment that the client has received the notice at the earliest possible opportunity. Specifically, Vista shall furnish the notice to individuals with whom Vista has a direct treatment relationship as follows:

- No later than the date of the first service delivery;
- Upon request; and
- On or after the effective date of a revision to the notice.

Except in an emergency treatment situation, Vista will attempt to obtain acknowledgment of a client's receipt of the notice on the first date of service following the implementation of these policies and procedures. Vista will ask the client to sign an "Acknowledgement of Receipt of Notice" form, verifying that he or she has received the notice. If the client refuses to sign this form, Vista will document Vista's efforts to obtain written acknowledgment and the reasons why the acknowledgment was not obtained.

In the event of an emergency treatment situation, Vista will furnish the client with the notice as soon as reasonably practicable and will attempt to obtain written acknowledgment of receipt at that time.

Vista will make sure that the notice is available for individuals visiting Vista for services, in the event that they ask for a copy.

Vista will post the notice in a clear and prominent location within Vista's offices, where it is reasonable to expect clients seeking health care services to be able to read the notice.

Vista will prominently post the notice on any website(s) maintained by Vista.

Requested Restrictions on Uses and Disclosures

Clients have the right to request that Vista limit its uses and disclosures of PHI in relation to treatment, payment and health care operations, or to request that Vista not use or disclose PHI for these reasons at all. Such requests shall be made to Vista in writing, using Vista's Request for Restrictions form.

Vista is not required to agree to a restriction requested by a client. However, if Vista does agree to a requested restriction, Vista may not violate this restriction.

Vista may terminate an agreed-to restriction by agreement with the client, or by notifying the client that the restriction will be terminated; provided that such termination is only effective with respect to PHI created or received after Vista has so informed the client, and that such termination is documented.

Requests for Confidential Communications of PHI

Vista will take necessary steps to accommodate reasonable requests by clients to receive communications of their PHI in an alternative, more confidential manner. Such requests shall be made in writing, using Vista's Request for Confidential Communications form.

Vista will agree to confidential communications by alternative means or at alternative locations when presented with reasonable requests to do so.

Access to PHI

Clients have the right to inspect and copy their PHI that Vista or its business associates maintain in their "designated record set." Information regarding the status or location of the client (e.g. photographic or video surveillance used for security purposes) and pictures or video taken of clients with written permission, for publicity/marketing or training purposes, are not part of Vista's designated record set.

Pursuant to federal law, clients may not have access to the following: psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and PHI that is subject to federal or state law that prohibits access to that information. Denials based on these factors are not reviewable.

Access may also be denied to part or all of a client's PHI if a licensed health care professional determines that such access is reasonably likely to endanger or harm the client or another person. Such denials *are* reviewable by an independent and licensed health care professional. Requests for access shall be made in writing using Vista's Request for Access form. Vista will communicate all access denials in writing using Vista's Denial of Access form.

Requests to Amend PHI

Vista shall provide clients the right to request an amendment to their PHI that is created and maintained by Vista or its business associates. Such requests shall be made in writing using Vista's Request to Amend form.

Vista may deny an individual's request for amendment if it determines that the requested PHI:

- Was not created by the Vista, unless the client provides a reasonable basis to believe that the originator of PHI is no longer available to act on the amendment;
- Is not maintained by Vista;
- Would not be available for inspection under Vista's Policy on Access to PHI; or
- Is accurate and complete.

If a requested amendment is *denied*:

- Vista will notify the client in writing using Vista's Denial of Amendment form.
- If the client submits a statement of disagreement, Vista may prepare a written rebuttal to the Statement of Disagreement. Vista will provide the client with a copy of any such rebuttal.
- Vista will append or otherwise link the following to our records that is the subject of the disputed amendment:
    - The client's request for an amendment;
    - The denial of the request;
    - The client's statement of disagreement, if any; and Vista's rebuttal, if any.

Accounting for Disclosures

Vista shall, upon written request using Vista's Request for Accounting form, provide a client with an accounting of disclosures of the client's PHI, except for disclosures:

- That relate to treatment, payment or operations;
- To the client;
- Made pursuant to a valid authorization;
- Incidental to a permissible disclosure;
- Provided for national security or intelligence purposes;
- Made before April 14, 2003; or
- Made more than six years prior to the request for accounting.

All disclosures that are required to be accounted for will be documented in Vista's Minimum Necessary/Disclosure Log. This Log, if properly completed, contains all information required for an adequate accounting. Therefore, the Privacy Officer shall respond to a request for an accounting of disclosures by providing the client with copies of all Minimum Necessary/Disclosure logs for the time period requested by the individual, not to exceed six years, and not to cover dates earlier than April 14, 2003.

Vista shall provide the first accounting in any 12-month period for free, but may charge the client a reasonable, cost-based fee for further disclosures during that same 12-month period, provided that the client has advance notice of the fee and has an opportunity to withdraw or modify the request to avoid or reduce the fee.

Authorizations

For all uses and disclosures of PHI that are not described in Section III of this document, Vista will obtain a signed authorization from the client before making such disclosures.

Vista shall not condition the provision of treatment on a client's provision of an authorization unless, if deemed necessary within professional judgment, the provision of health care is solely for the purpose of creating PHI to a third party, in which case the treatment can be conditioned on obtaining an authorization for disclosure to such third party. This exception shall not apply with regard to PHI about psychotherapy notes, HIV/AIDS or treatment of alcohol and/or substance abuse or dependency.

Business Associates

Vista shall not share PHI with a business associate without first obtaining adequate assurances that the business associate will appropriately safeguard the information. Adequate assurances of safeguarding may only be obtained by executing a written business associate agreement with the business associate. The business associate agreement shall ensure that the business associate follows Vista's privacy and security practices and otherwise complies with HIPAA in the course of any duties that involve use of PHI on behalf of Vista.

A business associate is any person or entity that performs a service for or on behalf of Vista, where this service involves the use or disclosure of PHI.

If Vista becomes aware that a business associate is in violation of the business associate agreement, Vista will terminate the contract, or if termination is not feasible, Vista will report the problem to the Secretary of Health and Human Services.

Complaint Process

Vista designates its Compliance Officer as the Privacy Officer who will be responsible for oversight of the policies and procedures regarding the privacy of PHI, as well as for being the contact person who will receive complaints from clients and answer their questions about Vista's privacy policies and procedures.

Complaint Process

Vista shall implement a process that allows clients who believe that Vista has not complied with these privacy policies to file a complaint with the Privacy Official.

Procedures:

- A client who wishes to log a complaint with Vista, alleging that Vista has not complied with these privacy policies, shall follow the Grievance Policy and Procedure and file such complaint in writing to the Privacy Officer.
- The Privacy Officer shall investigate the complaint but is under no obligation to report the results of this investigation to the individual, although the Privacy Officer is encouraged to do so, since the

client is permitted to file such complaints with the Secretary of the Department of Health and Human Services at any time.

- The complaint and any documentation relating to the investigation or resolution of the complaint shall be maintained by Vista for a period of not less than six years.

Workforce Training and Sanctions

Workforce Training

Vista will train all staff members who come into contact with PHI in the course of performing their duties on proper uses and disclosures of PHI, client rights with regard to PHI, and all other policies that are relevant to their particular duties.

Staff members shall include the Authorized Personnel.

Sanctions

Vista will apply appropriate sanctions against staff members who fail to comply with these policies and procedures.

The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of PHI, and similar factors.

This policy and its procedures do not apply specifically when members of Vista's workforce exercise their right to:

- File a complaint with the Department of Health and Human Services;
- Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing relating to compliance with the HIPAA Privacy Standards;
- Oppose any act made unlawful by the HIPAA Privacy Standards; provided that the individual or person 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 HIPAA Privacy Standards; or
- 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.

Mitigating Violations and Breach Notification

Vista, shall detect possible breaches of PHI and upon discovering that a use or disclosure of PHI by a staff member or business associate that is a violation of these policies and procedures, or of the HIPAA Privacy Standards, has had a harmful effect, shall mitigate, to the extent practicable and provide any required notifications consistent with the requirements set forth in the HIPAA regulations, and any other related federal or state laws.

Definition:

Breach: Acquisition, access, use or disclosure or unsecured, unencrypted PHI in a manner not permitted which compromises the security or privacy of the PHI. The term "breach" does not include:

- Any unintentional acquisition, access or use of PHI by a staff member or person acting under the authority of a covered entity or business associate if:
    - Acquisition, access or use was made in good faith and within the course and scope of responsibility;
    - Such information is not further used or disclosed in an impermissible manner; or

- Any inadvertent disclosure by a person who is authorized to access PHI or a Business Associate to another person authorized to access PHI or the Business Associate
- Unauthorized disclosure in which Vista or the Business Associate has a good faith belief that the person to whom the disclosure was made would not reasonably have been able to retain such information.

Procedures:

Discovery and Reporting of Possible Breaches. A staff or client who has knowledge of a potential breach from any source shall immediately notify the Privacy Officer. The Privacy Officer shall accept notice of the potential breach from any person, including staff, individuals, residents, business associates, etc. The Privacy Officer shall take immediate steps to verify the validity of the report and take any appropriate action to mitigate the potential harm from the breach.

Investigation of Possible Breaches. The Privacy Officer will lead an investigation of the facts and circumstances of the potential breach. The Privacy Officer will first determine if any of the exceptions to the definition of "breach" applies. If so, the incident is not considered a breach, and no further action is required.

If an exception does not apply, any acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless it is determined through a risk assessment that there is a low probability that the PHI has been compromised. The following factors should be considered when conducting a risk assessment:

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

The Privacy Officer shall review with legal counsel the findings of the investigation and risk assessment before a final determination is made.

If the risk assessment fails to demonstrate there is a low probability that any PHI has been compromised, breach notification is required.

Breach Notice to Individuals. The Privacy Officer will provide written notification of the breach to the affected client(s) as soon as possible after the investigation is completed, but no later than 60 days after discovery of the breach.

If there is reason to believe the affected client's information is in immediate danger of being misused, the Privacy Officer shall also contact the client by phone in addition to the written notice.

Breach Notice to the Media. When a single breach event affects more than 500 clients of the same state, notice shall be provided to prominent media outlets, in addition to the notice to clients. The notice to the media shall be sent no later than 60 days after the discovery of the breach and must include a toll-free number for the client to call and inquire.

Breach Notice to Secretary of Health and Human Services. When a breach involves 500 or more clients, notice shall be provided to the Secretary of Health and Human Services in the manner specified on the website.

Information: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Notification link: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

When a breach involves fewer than 500 clients, the Privacy Officer shall maintain a log of such breaches and provide notice to the Secretary no later than 60 days after the end of the calendar year, in the manner specified on the website.

Breach Notice – Business Associates. Vista's Business Associates are required to notify Vista of a possible breach under the terms of the Business Associate Agreement. Business Associates are required to provide Vista with the information necessary to conduct a risk assessment and to provide any notice required under this policy.

Non-Retaliation and Non-Waiver

Non-Retaliation. Vista shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against

Any client who exercises his or her right to:

- Request access to their PHI;
- Request amendments to their PHI;
- Request an accounting of disclosures of their PHI;
- Request confidential communications of PHI;
- Request restrictions on the use or disclosure of their PHI;
- File a complaint, either to Vista or to the Secretary of Health and Human Services for alleged violations of the HIPAA Privacy Standards; or

Any client or entity for:

- Filing a complaint with the Secretary of Health and Human Services;
- Testifying, assisting, or participating in an investigation, compliance review or hearing under the HIPAA Privacy Standards; or
- Opposing any act or practice made unlawful by the HIPAA Privacy Standards, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Standards or these policies and procedures.

Non-Waiver. Vista will not require a client to waive their rights to file a complaint to the Secretary of Health and Human Services for perceived violations of the HIPAA Privacy Standards as a condition of payment for healthcare services, enrollment in Vista, or eligibility for benefits.

Documentation

Vista has implemented these written policies and procedures with respect to PHI, and these policies and procedures are designed to comply with the HIPAA Privacy Standards.

Vista will maintain documentation, in written or electronic form, these policies and procedures, as well as all communications and other administrative documents required by these policies and procedures for a period of at least six years from the date of creation or the date when last in effect, whichever is later. This documentation shall include, but is not limited to, all authorization forms, business associate agreements, Privacy Notices and amendments thereto, and any correspondence sent to or received from clients relating to the use and disclosure of their PHI under these policies and procedures.

Vista will incorporate into these policies, procedures and other administrative documents and changes in law, and shall properly document and implement any changes to policies and procedures as necessary, pursuant to changes in law.

HIPAA Security Policies

This policy addresses compliance with the HIPAA Security Rule. The Security Rule defines ePHI as protected health information in electronic form. Protected health information, in turn, means information that relates to the past, present or future physical or mental health of a client (including genetic information); the provision of health care to a client; or the past, present or future payment for the provision of health care to a client that

identifies the client or with respect to which there is a reasonable basis to believe the information can be used to identify the client.

By implementing this policy Vista intends to:

- Ensure the confidentiality, integrity, and availability of all ePHI Vista creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the HIPAA privacy rules; and
- Ensure compliance by Vista's staff.

The policy takes into account Vista's:

- Size, complexity, and capabilities;
- Technical infrastructure, hardware, and software security capabilities;
- Costs of security measures; and
- Probability and criticality of potential risks to electronic protected health information

While Vista is not responsible for the security of electronic transmissions it receives, Vista is responsible for the security and availability to authorized persons of ePHI after receipt, either while the data is at rest or during transmission.

Administrative Safeguards

Vista will prevent, detect, contain, and correct ePHI security violations.

Assigned Security Responsibility

Vista has designated its Director of Infrastructure to serve as Vista's Security Officer. Security Officer responsibilities include the management and supervision of:

- The development and implementation of security measures to protect ePHI, and the conduct of personnel in using and protecting ePHI.
- Conducting an annual risk assessment. This assessment reviews risks associated with a number of key factors. These factors include, but are not limited to:
    - Security processes (security administration, security monitoring, incident response, and virus detection);
    - Physical access to the data center and other critical operations areas;
    - Contingency planning;
    - Operating system and/or platform configurations;
    - Network configurations;
    - Data repositories;
    - Portal/web architecture; and
    - Risk analysis including threat assessment

Risk Assessment Analysis

Vista has conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI received and/or maintained by Vista. The analysis was carried out by Vista's Security Officer and other IT personnel, as needed (collectively, the "Security Team").

The Security Team has determined that the data items determined to qualify as ePHI, and therefore impacted by this HIPAA Security Policy, include (i) electronic messages or other electronic transmissions containing client

names and other identifiers that are sent and received via Outlook; (ii) Word, Excel and PDF documents saved to Vista's document management system that contain client names and other identifiers; (iii) the service billing and invoice management program currently known as Accumedic and MyEvolv; (iv) cloud storage for all Vista programs and document management systems; (v) local storage; and (vi) remote devices, such as laptops and smart phones. These items are typically received and stored to Vista's network by staff and/or their assistants in providing services to clients.

Vista then ranks the level of risk remaining after considering existing risk management factors. From this assessment, Vista identifies the key areas it will audit in the coming year.

Risk Management. Vista has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, and has documented identified risks, corrective actions taken, and risks considered acceptable as more fully described throughout this HIPAA Security Policy.

Sanction Policy. Appropriate sanctions will be taken against staff members who fail to comply with Vista's Security Policy and procedures regarding ePHI, and all staff, vendors, and contractors will be made aware of ramifications of violating this Security Policy. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of ePHI, and similar factors. Sanctions may include restriction or loss of network privileges and other appropriate actions including termination of employment. The Security Officer and supporting staff are authorized to immediately revoke network access or take any other appropriate action to ensure that Vista's IT system remains secure.

Information System Activity Review. Vista will routinely monitor its IT systems relative to the use and dissemination of PHI and ePHI in accordance with its security practices.

Assigned Workforce Security. Vista ensures that staff members have appropriate access to ePHI, but that those who should not have access are restricted from such access. More specifically, access to Vista's IT system, on which ePHI is stored, requires user-based authentication. This authentication system limits system access only to specified, authenticated individuals. Application level access is controlled by specific system user accounts, and they are password protected. All transactions involving access to systems containing ePHI are cloud-based, and security regarding electronic trespass, hacking or unauthorized attempts to access the cloud-based systems is managed by the vendors of those systems. With these measures in place, the risk of unauthorized access to ePHI is extremely low. Data on the IT system has never been compromised as of the date of this HIPAA Security Policy.

Remote devices (laptops, smart phones, etc.) with access to Vista systems are password protected. All staff who access Vista systems from personal remote devices agree in writing to ensure appropriate access to such systems remotely, to install recommended antivirus applications, and to ensure that such devices are not accessed by third parties unaffiliated with Vista. In the event that such devices are lost or stolen, staff are required to immediately notify Vista IT personnel so that appropriate measures may be taken to protect Vista information accessible through such devices.

Appropriate measures will be taken upon a staff member's termination, or if access otherwise needs to be removed, including removal of all access to ePHI; account removal/disablement; lock access to personal files; and return of physical security items (e.g. cell phones, PDAs, blackberries, keys, laptops).

Accountability for completing terminations and ensuring ePHI access is discontinued is assigned to the Security Team.

Access. Vista controls and reviews access to ePHI. Vista has determined that the staff who access ePHI are as follows:

All staff providing healthcare and related services for or on behalf of Vista's clients, supervisors for purposes of data collection and analysis, the business office for purposes of billing, and information technology for support purposes.

Vista manages all user access to the IT system by ensuring that members of its workforce who need access to ePHI to do their jobs have appropriate access, while at the same time ensuring that those who should not have access to ePHI are restricted from such access. More specifically, access to Vista's IT system, on which ePHI is stored, requires user-based authentication. This authentication system limits system access only to specified, authenticated individuals. Application level access is controlled by specific system user accounts, and they are password protected. All transactions and access are logged locally as well as to a central auditing system. Firewall logs assess activity and monitor for suspicious activity. The various logs are periodically reviewed and analyzed for any evidence of electronic trespass, hacking or unauthorized attempts to access the IT system. With these measures in place, the risk of unauthorized access to ePHI is extremely low. To the knowledge of Vista, ePHI contained or maintained on the IT system has never been compromised as of the date of this HIPAA Security Policy.

Security Awareness. Vista shall provide ongoing security information training and awareness to staff who access ePHI through working with Vista. Training shall be conducted when staff are hired and annually thereafter.

Training will, among other things, educate staff about processes for guarding against, detecting and reporting malicious software; provide processes for monitoring IT system log-in attempts and reporting discrepancies; and discuss the necessity of creating, changing and safeguarding user accounts and passwords.

Security Incident Procedures. Vista will address security incidents, which are the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security incidents will be processed and documented by the Security Officer, which shall work in conjunction with local, state, or federal agencies as needed.

Recovery methods for compromised or affected systems shall include scanning of the machines and restoration of operating system(s) and data to pre-security incident state; provided, however, that if returning such systems and date to a pre-security incident state is not possible, a complete rebuild of the affected system(s) shall be ordered.

Contingency Plan. Vista has established policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems and facilities required to conduct business, including ePHI. In addition, all data is backed-up incrementally on a daily basis, and full back-ups are done each week.

Evaluation. Vista will perform an annual evaluation, based initially upon these standards, and later in response to environmental or operational changes affecting the security of ePHI, including:

- Risk analysis;
- Threat assessment;
- Operating system and network device security configurations;
- Access controls and authorization to ePHI;
- Security awareness;
- Security incident response;
- Physical security;
- Transmission security;
- Security model (i.e., data classification/ownership);

- Security policies/procedures; and
- Security architecture and design.

Subcontractors. Administrative safeguards also apply to Vista's business associate/subcontractor contracts and other arrangements in which ePHI is handled on Vista's behalf. Such agreements will be negotiated into a written contract as more fully set forth in Subsection T and the Privacy Policies.

Facility Access Controls (Physical Safeguard). Vista limits physical access to electronic information systems and the facility in which they are housed and ensures that only properly authorized access is allowed. This includes visitor and workforce authorization procedures appropriate to secure access to these facilities.

The IT system and database servers where ePHI data are processed and stored are physically secured in monitored, climate controlled and locked server rooms (maintained by the applicable cloud-based vendor). Keys to the server room are controlled (by the vendor).

Vista has developed a contingency plan that spells out processes to use during recovery from a disaster. These disaster recovery plans detail the responsibility of Vista's supervisors to identify critical business activities and the required resources for resuming critical business in the event of an interruption such as a disaster or other emergency. This includes hardware, software, and people resources for all areas. Recovery teams are identified and authorized to access data resources only as necessary to resume normal business operations. These disaster recovery plans are executed by staff that already have basic access as required by normal business and technical support duties. In the absence or shortage of these critical recovery staff, only authorized substitutes shall be given minimal access as required by restoration operations.

Vista safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. This includes:

- Periodic testing of the security of the computer rooms and sensitive areas;
- Periodic review of the physical access lists; and
- Environmental controls.

IT personnel have only "need to know" access to the areas and systems/data required by their jobs. Vista maintains records of repairs and modifications to Vista's network systems, and Vista destroys faulty hard drives before they leave Vista's facilities.

Workstation Use and Security (Physical Safeguard). Staff who are permitted to access the IT system that houses ePHI do so at workstations that are either (i) located in locked office areas or (ii) in the physical possession of the staff.

All workstation access to the IT system is via confidential staff account with password protection. System access is audited and recorded. The system requires passwords to be routinely changed. Passwords must meet certain cryptographic standards, and old passwords may not be immediately re-used.

Device and Media Controls (Physical Safeguard). Vista maintains records of repairs and modifications to Vista's network systems, and Vista destroys faulty hard drives before they leave Vista's facilities.

It is the policy of Vista to erase all ePHI from electronic media before re-using or replacing the media.

Vista keeps inventory records of which personnel are given access to portable devices, such as laptops, PDAs, etc.

Technical Safeguards. Vista has purchased and implemented information systems that allow access only to those persons and/or software programs that have been granted access rights.

Vista has assigned a unique identifier for each staff who accesses ePHI, and this allows Vista to track and monitor the use of information systems containing ePHI.

Computer workstations automatically lock after fifteen (15) minutes of non-use, and users must enter their confidential password to re-enter the workstation.

Vista has implemented encryption technology for all e-mails containing PHI that are sent from Vista. Encryption technology is available to all staff who use/disclose ePHI and who need to send ePHI via e-mail to third parties as part of Vista's normal operations.

Vista has enabled an Office365 Security and Compliance Data Loss Prevention policy that alerts Security Officer if anyone accesses or sends a file containing a large amount of PHI that contains social security numbers.

Audit Controls. Vista monitors and audits system access.

Integrity. Vista utilizes secure tunneling technology to promote data integrity. Any email which might contain ePHI or other sensitive information will be transmitted by opening a hole in the network firewall to transport such information to only a particular endpoint and no other.

Person or Entity Authentication. Vista ensures that a person or entity seeking access to ePHI is the one claimed, and that access is only granted to Vista staff who require it for their jobs. All ePHI system users are assigned a user account and are required to develop and periodically update a confidential password to access the system.

Transmission Security. Vista has implemented encryption technology functionality for all staff for e-mails containing PHI that are sent from Vista.

Business Associate Contracts or other Arrangements. The contract or other arrangement between Vista and its clients or between Vista and its subcontractor(s), if any, meet the confidentiality requirements, as applicable. Any awareness of a pattern of an activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the contract or other arrangement will be immediately escalated and will be considered a violation unless the subcontractor takes reasonable steps to cure the breach or end the violation; and if such steps are unsuccessful, the contract or arrangement will be terminated, if feasible.

Contracts between Vista and its subcontractors require the subcontractors to implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on Vista's behalf. These safeguards must, in all instances, be no less protective of PHI and ePHI than the safeguards to which Vista is subject under its business associate agreements or that it is subject to as a Covered Entity.

- Subcontractors must ensure that any agent, including another subcontractor, to whom they provide such information agrees to implement safeguards to protect such information that are no less protective of PHI and ePHI than the safeguards to which such subcontractors are subject pursuant to their business associate agreements with Vista.
- Any security incident or breach of which a subcontractor becomes aware must be reported to Vista.
- Vista will regularly review current contracts to assess the need for amendment or re- contracting to ensure the implementation of HIPAA-compliant security practices with business associates or other subcontractors.

Links to additional content or information

Related Relevant Policy	

Related Standard Operating Procedure(s)	
Related Form(s)	