HIPAA COMPLIANCE

POLICY MANUAL

HIPAA Compliance Policy

Northern Arizona Intergovernmental Public Transportation Authority has adopted this HIPAA Compliance Policy to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This HIPAA Compliance Policy is written to familiarize you with the practices required of NAIPTA to remain in full compliance. It is NAIPTA's policy to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy. All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years (See NAIPTA Record Retention Policy) from the date of creation or last revision, whichever is later, in accordance with NAIPTA's Document Retention policy. This HIPAA Compliance Policy applies to all employees unless otherwise specified.

Adopted by NAIPTA Board of Directors,

Updated: April 19, 2017

IMPORTANT - READ CAREFULLY

THIS HIPAA COMPLIANCE POLICY IS DESIGNED TO ACQUAINT EMPLOYEES, OFFICERS, AGENTS, CONTRACTORS, TEMPORARY WORKERS, AND VOLUNTEERS WITH THE NORTHERN ARIZONA INTERGOVERNMENTAL PUBLIC TRANSPORTATION AUTHORITY ("NAIPTA") REQUIREMENTS AS A COVERED ENTITY UNDER THE DEFINITIONS CONTAINED IN THE HIPAA REGULATIONS.

AS A COVERED ENTITY, NAIPTA MUST COMPLY WITH HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 "HIPAA", AS AMENDED BY HITECH ACT OF 2009 (ARRA TITLE XIII). NAIPTA ALSO RECOGNIZES THEIR RESPONSIBILITY TO PROTECT INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION UNDER REGULATIONS IMPLEMENTING HIPAA, OTHER FEDERAL AND STATE LAWS PROTECTING THE CONFIDENTIALITY OF PERSONAL INFORMATION, AND UNDER GENERAL, PROFESSIONAL ETHICS.

COMPLIANCE WITH HIPAA IS MANDATORY AND FAILURE TO COMPLY CAN BRING SEVERE SANCTIONS AND PENALTIES. COMPLIANCE WITH HIPAA WILL STRENGTHEN OUR ABILITY TO MEET OTHER COMPLIANCE OBLIGATIONS, AND IN FACT, WILL SUPPORT AND STRENGTHEN OUR NON-HIPAA COMPLIANCE REQUIREMENTS AND EFFORTS.

UNLESS OTHERWISE SPECIFIED, THIS HIPAA COMPLIANCE POLICY APPLIES TO ALL NAIPTA EMPLOYEES, EXCLUDING APPOINTED OFFICIALS. DEMONSTRATED COMPETENCE IN THE REQUIREMENTS OF THE HIPAA COMPLIANCE POLICY IS AN IMPORTANT PART OF RESPONSIBILITIES OF ALL NAIPTA EMPLOYEES.

THE CEO-GENERAL MANAGER OR HIS DESIGNATE SHALL HAVE AUTHORITY TO MAKE AMENDMENTS. ALL NAIPTA EMPLOYEES MUST READ, UNDERSTAND, AND COMPLY WITH THIS POLICY.

ALL MANAGERS AND SUPERVISORS ARE RESPONSIBLE FOR ENFORCING THIS POLICY. EMPLOYEES WHO VIOLATE THIS POLICY ARE SUBJECT TO DISCIPLINE UP TO AND INCLUDING TERMINATION IN ACCORDANCE WITH NAIPTA'S SANCTION POLICY.

NO HIPAA COMPLIANCE POLICY CAN ANTICIPATE EVERY CIRCUMSTANCE OR QUESTION. AFTER READING THE HIPAA COMPLIANCE POLICY, EMPLOYEES THAT HAVE QUESTIONS SHOULD TALK WITH THEIR IMMEDIATE SUPERVISOR OR HUMAN RESOURCES. IN ADDITION, THE NEED MAY ARISE TO CHANGE THE GUIDELINES DESCRIBED IN THE HIPPA COMPLIANCE POLICY. NAIPTA THEREFORE RESERVES THE RIGHT TO INTERPRET THEM OR TO CHANGE THEM WITH OR WITHOUT PRIOR NOTICE.

Table of Contents

1 POLICY & PROCEDURES 7

2 DOCUMENTATION POLICY 7

2.1 DOCUMENTATION RETENTION POLICY 7

2.2 DOCUMENTATION AVAILABILITY POLICY 7

2.3 DOCUMENTATION UPDATE POLICY 8

3 HHS INVESTIGATIONS POLICY 8

4 BREACH NOTIFICATION POLICY 10

5 HIPAA OFFICER POLICY 10

6 HIPAA STATE LAW PREEMPTION POLICY 12

7 HIPAA TRAINING POLICY 12

8 PHI USES AND DISCLOSURES POLICY 13

9 EMPLOYEE RIGHTS POLICY 15

10 COMPLAINTS POLICY 15

11 RISK MANAGEMENT PROCESS POLICY 17

11.1 RISK ANALYSIS POLICY 17

11.2 RISK MANAGEMENT IMPLEMENTATION POLICY 17

12 SANCTION POLICY 18

12.1 INFORMATION SYSTEMS ACTIVITY REVIEW POLICY 18

12.2 ASSIGNMENT OF SECURITY RESPONSIBILITY POLICY 19

12.3 AUTHORIZATION & SUPERVISION POLICY AND PROCEDURES 20

13 WORKFORCE CLEARANCE POLICY AND PROCEDURES 21

14 ACCESS AUTHORIZATION POLICY 21

14.1 ACCESS ESTABLISHMENT AND MODIFICATION POLICY 21

14.2 ACCESS TERMINATION POLICY AND PROCEDURES 22

14.3 SECURITY REMINDERS POLICY 22

15 MALWARE PROTECTION POLICY 22

16 LOG-IN MONITORING POLICY 23

16.1 PASSWORD MANAGEMENT POLICY 23

17 POLICY ON SECURITY INCIDENT PROCEDURES 24

18 DATA BACKUP PLAN AND STORAGE POLICY 25

19 DISASTER RECOVERY PLAN 26

20 EMERGENCY MODE OPERATIONS PLAN 26

20.1 FOLLOW UP TESTING AND REVISION OF PLANS/PROCEDURES 27

20.2 EMERGENCY ACCESS PROCEDURES 28

21 POLICY ON DATA AND APPLICATIONS CRITICALITY ANALYSES 28

22 BUSINESS ASSOCIATES POLICY 29

23 FACILITY SECURITY PLAN AND POLICY 29

23.1 INFORMATION ACCESS CONTROL AND VALIDATION PROCEDURES 30

23.2 FACILITY SECURITY MAINTENANCE RECORDS POLICY 30

24 WORKSTATION USE AND SECURITY POLICY 31

25 MEDIA DISPOSAL POLICY 31

25.1 MEDIA RE-USE POLICY 31

25.2 HARDWARE AND MEDIA ACCOUNTABILITY POLICY 32

26 UNIQUE USER I.D. POLICY 32

27 AUTOMATIC LOCK POLICY 32

28 ENCRYPTION AND DECRYPTION POLICY 33

29 AUDIT CONTROLS POLICY 33

30 DATA INTEGRITY CONTROLS POLICY 34

30.1 DATA INTEGRITY CONTROLS PROCEDURES 34

31 PERSON OR ENTITY AUTHENTICATION POLICY 34

ACKNOWLEDGEMENT OF RECEIPT 36

1 POLICY & PROCEDURES

NAIPTA is dedicated to the requirements for creation, implementation and use of specific information in accordance with the HIPAA law and implementing HIPAA regulations, at § 164.306, § 160.310, § 164.312, §164.316 and §164.530(a)(i). NAIPTA has developed good business practices and general business ethics for the implementation of the policies and procedures which will provide clear guidance to all employees about our obligations under the law and how we do business.

NAIPTA shall update and amend all policies and procedures as needed or as required by law. Once approval has been granted by the Board of Directors, the policies and procedures shall be made available to the entire workforce. All NAIPTA employees are required to read, understand, comply, and acknowledge the policy and procedures in Paychex within specified timeframe.

Return to Table of Contents

2 DOCUMENTATION POLICY

NAIPTA must comply with HIPAA and the HIPAA implementing regulations concerned with documentation, availability, retention, and updating of HIPAA related documents at §164.310, §164.312(b)(2)(i), §164.316, §164.530 (j)(1)(ii), and §164.530 (j)(1)(iii), among others. This policy governs the creation, use and maintenance of documents related to HIPAA compliance for NAIPTA.

The organization must create or maintain all HIPAA related documentation policies in written form, which may also include electronic forms of documentation. Any action, activity or assessment that is documented will be in accordance with all HIPPAA related policies and procedures. All HIPAA related documentation must be forwarded, used, applied, filed, or stored in accordance with this policy.

Return to Table of Contents

2.1 DOCUMENTATION RETENTION POLICY

The documentation retention policy governs the proper and lawful retention of HIPAA related documents which is a requirement and good business practice. Proper and lawful retention of HIPAA-related documentation is both a requirement under HIPAA and good business practice along with essential to proving our compliance, responding to investigations, and to effectively serving our constituents. It is NAIPTA's policy to retain all HIPAA-related documentation according to the retention policy from the date of its creation or modification, or the date when it was last in effect, whichever is later.

Return to Table of Contents

2.2 DOCUMENTATION AVAILABILITY POLICY

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerned with the availability of HIPAA related documentation, in accordance with the requirements at § 164.310, § 164.316, § 164.530(j), among others.

It is NAIPTA's policy to make all HIPAA-related documentation available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains. All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation. Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation. No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

Return to Table of Contents

2.3 DOCUMENTATION UPDATE POLICY

This policy governs the compliance with HIPAA and the HIPAA implementing regulations concerned with the updating of HIPAA-related documentation, in accordance with the requirements at § 164.310, § 164.316, and § 164.530(j), among others.

Timely updating and maintenance of HIPAA-related documentation is essential to proving compliance with HIPAA regulations, responding to investigations, effectively serving our constituents, and good business practice. It is NAIPTA's policy to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operational changes affecting the privacy or security of individually identifiable health information. Reviews of HIPAA-related documentation shall be made periodically, but at least every 1 year for the purposes of this policy. Reviews and updates of HIPAA-related documentation that occur shall be made by NAIPTA's designated HIPAA Officer per NAIPTA's Documentation Policy.

Return to Table of Contents

3 HHS INVESTIGATIONS POLICY

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerned with HIPAA-related investigations by US Department of Health and Human Services ("HHS)", in accordance with the requirements at § 164.308, § 164.310, and § 164.312, among others.

It is NAIPTA's policy to not impede or obstruct any HIPAA-related investigations conducted by HHS. It is NAIPTA's policy to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS. Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following:

- ☐ When NAIPTA is notified by HHS about an investigation the HIPAA Officer will notify the following people immediately:
  - Attorneys (HIPAA counsel AND local counsel, if different)
  - CEO-General Manager
  - Administrative Director
- ☐ HIPAA Officer, (on-site coordinator), will follow NAIPTA's Standard Operating Procedures when handling HHS Investigations.
  - Cooperate, but do not volunteer information or records that are not requested.

- ☐ Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. (BE SURE that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)
- ☐ Have at least one, if not two witnesses available to testify as to your requests and their responses.
- ☐ Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
- ☐ Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation.
- ☐ Permit the investigators to have access to protected health information ("PHI"), in accordance with our notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- ☐ Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- ☐ Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
- ☐ Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
- ☐ Ask the investigators for documents related to the investigation. For example, request:
    - o copies of any search warrants and/or entry and inspection orders
    - o copies of any complaints
    - o a list of employees they are interested in
    - o a list of documents/items seized
- ☐ Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- ☐ Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- ☐ Don't offer food (coffee, if already prepared, and water, if already available, is ok. Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.

Return to Table of Contents

4 BREACH NOTIFICATION POLICY

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerned with notifications to consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.

It is NAIPTA's policy to provide timely notifications to affected (employees and/or) consumers about breaches of individually identifiable health information.

- ☐ It is the Policy of NAIPTA to timely provide:
  - Notice to employees alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach.
  - Notice to Covered Entities by Business Associates ("BAs") when BAs discover a breach.
  - Notice to the secretary of HHS and prominent media outlets about breaches involving more than 500 employee records.
  - Notice to next of kin about breaches involving employees who are deceased.
  - Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the employee, and the CE's response.
  - Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 employee records.
- ☐ When a security or privacy incident occurs that may be a "breach" under HIPAA regulations, the designated HIPAA Officer will perform a risk assessment to determine whether there is significant risk of harm to the individual(s) whose PHI was inappropriately disclosed or compromised.
- ☐ The risk analysis must accurately address the following questions:
  - Did the breach or compromise involve "unsecured" protected health information?
  - In whose hands did the PHI land?
  - Can the information disclosed cause "significant risk of financial, reputational, or other harm to the individual"?
  - Was mitigation possible? For example, can you obtain forensic proof that a stolen laptop computer's data was not accessed?
- ☐ NAIPTA's Business Associates are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to the designated HIPAA Officer.
- ☐ Business Associate contracts, whether existing or new, are required to have corresponding breach notification requirements included in them.
- ☐ Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, per NAIPTA's Sanction Policy.
- ☐ All breach-related activities and investigations shall be thoroughly and timely documented in accordance with NAIPTA's Documentation Policy.

Return to Table of Contents

5 HIPAA OFFICER POLICY

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerning the designation of a HIPAA Officer, in accordance with the requirements at § 164.530(a).

- ☐ It is the Policy of NAIPTA to designate and maintain at all times an active HIPAA Officer.

- ☐ The HIPAA Officer's general responsibilities are to:
    - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
    - Conduct various risk analyses, as needed, or required.
    - Manage breach notification investigations, determinations, and responses, including breach notifications.
    - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.
- ☐ The HIPAA Officer's potential duties may include:
    - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, Information Technology Manager, administration, and legal counsel as applicable.
    - Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
    - Administer employee requests under HIPAA's Employee Rights.
    - Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
    - Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
    - Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
    - Develop specific policies and procedures mandated by HIPAA.
    - Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
    - Draft and disseminate the Privacy Notice required by the Privacy Rule.
    - Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
    - Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
    - Ensure that all policies, procedures, and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
    - Ensure that future initiatives are structured in such a way as to ensure employee privacy.
    - Conduct periodic privacy audits and take remedial action as necessary.
    - Oversee employee training in the areas of information privacy and security.
    - Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
    - Remain up-to-date and advise on new technologies to protect data privacy.
    - Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.

- Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- Anticipate employee or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
- Evaluate privacy implications of online, web-based applications.
- Monitor data collected by or posted on our website(s) for privacy concerns.
- Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.

Return to Table of Contents

6 HIPAA State Law Preemption Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.

- ☐ It is NAIPTA's policy to comply, whenever possible, with both state law in Arizona where we operate, as well as HIPAA law and regulations.
- ☐ It is the responsibility of the designated HIPAA Officer to analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
- ☐ The designated HIPAA Officer shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
- ☐ If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the designated HIPAA Officer, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to our operations.
- ☐ The designated HIPAA Officer shall conduct ongoing research to monitor legislative changes in Arizona where we operate that could affect HIPAA preemption issues.

Return to Table of Contents

7 HIPAA Training Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations concerning the training of workforce members, in accordance with the requirements at § 164.530(b).

- ☐ It is NAIPTA's policy to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers, and volunteers.
- ☐ HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.

- ☐ HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.
- ☐ HIPAA training shall be conducted periodically for all employees, but no less than once per year.
- ☐ Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training.
- ☐ The designated HIPAA Officer shall be responsible for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.
- ☐ HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.

Return to Table of Contents

8 PHI Uses and Disclosures Policy

This policy governs NAIPTA compliance with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.

- ☐ It is NAIPTA's policy to conduct its operations in accordance with HIPAA's rules governing uses and disclosures of Protected Health Information.
- ☐ NAIPTA will process requests for information from employee records in a timely, consistent manner as set forth in this policy.
- ☐ The following priorities and time frames shall apply to requests for disclosures of PHI:
    - Emergency requests involving immediate emergency care of employee: immediate processing.
    - Priority requests pertaining to current care of employee: within one workday.
    - Employee request for access to own record: within three (3) workdays.
    - Subpoenas and depositions: as required.
    - All other requests: within five (5) workdays
- ☐ Disclosure Monitoring and Logging -- Medical records personnel will maintain a log to track the step-by-step process towards completion of each request for the release of PHI. Health Information Management personnel and/or the Privacy Official will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
    - Date department received the request.
    - Name of employee.
    - Name and status (employee, parent, guardian) of person making request.
    - Information released.
    - Date released.
    - Fee charged.
- ☐ Unless the request specifies release of the complete medical record, the Health Information Management Department shall release only selected portions of the record. The department shall prepare an appropriate cover letter detailing the items included.
- ☐ Retention of Disclosure Requests -- The Health Information Management Department and/or HIPAA Officer will retain the original request, the authorization for release of information, and a copy of the cover letter in the employee(s) medical record for the appropriate record retention period.

- □ Disclosure Quality Control -- The HIPAA Officer shall conduct a routine audit of the release of information at least quarterly, paying particular attention to the following:
    - o Appropriateness of information abstracted in response to the request.
    - o Retention of authorization, request, and transmitting cover letter.
    - o Procedures for telephone, electronic, and in-person requests.
    - o Compliance with designated priorities and time frames.
    - o Proper processing of fees.
    - o Maintenance of confidentiality.
- □ In-service Training on Disclosures -- The HIPAA Officer shall give periodic in-service training to all employees involved in the release of information.
- □ Semi-Annual Policy Review - The HIPAA Officer shall review this policy and associated procedures with risk management and legal counsel at least annually.
- □ Capacity to Authorize -- NAIPTA requires a written, signed, current, valid authorization to release medical information as follows:

Employee Category	**Required Signature**
Adult Employee	The employee or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Employee	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.
Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult employee above.
Psychiatric, drug, alcohol program employees/client's	Same as adult employee above, but check for special requirements.
AIDS/HIV or other sexually transmitted disease employee	Same as adult employee above, but check for special requirements.

- □ Authorization Forms -- The HIPAA Officer shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
- □ Revocation of Authorization -- A employee may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
- □ Refusal to Honor Authorization -- The HIPAA Officer or others authorized to release information will not honor a em ployee authorization when they have a reasonable doubt or question as to the following information:
    - o Identity of the person presenting the authorization.
    - o Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
    - o Legal age or status as an emancipated minor.
    - o Employee capacity to understand the meaning of the authorization.
    - o Authenticity of the employee(s) signature.
    - o Current validity of the authorization.

- In such situations, the employee shall refer the matter to the HIPAA Officer for review and decision.

☐ Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.

Return to Table of Contents

9 Employee Rights Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations, in accordance with the requirements pertaining to the rights of employees at § 164.520, to § 164.528, as amended by the HITECH Act of 2009 (ARRA Title XIII).

☐ It is NAIPTA's policy to provide all the employee rights to our employees that are called for in the HIPAA regulations in a timely and positive manner.

☐ Employee Rights that we provide and support include:
- The Right to receive a copy of our "Notice of Privacy Practices", which details how individually identifiable health information may be used or disclosed by this organization.
- The Right to review or obtain a copy of medical records about that employee, or about the employee's minor children.
- The Right to request restrictions on the use or disclosure of the employee's medical records.
- The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
- The Right to request amendments to medical records, with certain limitations.
- The Right to an accounting of certain disclosures of individually identifiable health information.
- The Right to file a privacy complaint directly with us, or with the federal government.

☐ No retaliation of any kind is permitted against any person, employee, or workforce member for exercising any Right guaranteed by HIPAA.

☐ It is NAIPTA's policy that our Designated Record Set ("DRS"), for purposes of fulfilling HIPAA Employee Rights include the following types or categories of data and items:
- Benefit Enrollment Documents
- HIPPA RIGHTS

☐ The provision of employee rights in a timely and positive manner can enhance the quality of care we provide to employees, by providing certain rights and controls to employees over their individually identifiable health information.

Return to Table of Contents

10 Complaints Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII). In addition, HIPAA regulations, at § 164.530(g), prohibit

intimidating or retaliatory acts against any person or employee who files a privacy complaint or exercises any Right guaranteed under HIPAA.

- ☐ It is NAIPTA's policy to respond in a timely and positive manner to all complaints submitted by any persons or parties, including employees, workforce members, and any other person or party.
- ☐ Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Officer, who shall establish a process and appropriate forms to receive and process complaints.
- ☐ All complaints must be submitted in written form, dated, and signed by the complainant.
- ☐ NAIPTA shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case, shall more than 60 days' elapse between the time a complaint is submitted in writing and the resolution of the complaint.
- ☐ The HIPAA Officer shall investigate each complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
- ☐ The final resolution or disposition of each complaint shall be documented in accordance with NAIPTA 's Documentation Policy, and shall be retained in accordance with NAIPTA 's Documentation Retention Policy.
- ☐ The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
- ☐ In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediation's may include, but are not limited to:
    - o A written apology to the complainant from our organization.
    - o Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
    - o Sanctions against workforce members, as appropriate to the circumstances.
    - o Other unspecified remediation(s), as determined by legal counsel and senior management.
- ☐ For complaints submitted to the federal government, it is NAIPTA's policy to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in this organization's HHS Investigations Policy.
- ☐ No officer, agent, employee, contractor, temporary worker, or volunteer of this organization shall obstruct or impede any investigation in any way, whether internal or federal.

Return to Table of Contents

11 Risk Management Process Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.

- ☐ It is NAIPTA's policy to establish, implement, and maintain an appropriate risk management process.
- ☐ Such a risk management process shall be under the direct control and supervision of the HIPAA Officer and shall involve legal counsel, information technology, records management, senior management, and any other parties or persons deemed to be appropriate to the process.
- ☐ Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- ☐ The results of the risk management process shall be input into management's decision-making processes, to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

Return to Table of Contents

11.1 Risk Analysis Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the requirements at § 164.308(a)(1).

- ☐ It is NAIPTA's policy to conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that we are entrusted at least annually.
- ☐ Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Officer, who shall establish a plan and procedures for conducting such analyses.
- ☐ The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information
- ☐ All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy.

Return to Table of Contents

11.2 Risk Management Implementation Policy

This policy governs NAIPTA compliance with HIPAA and the HIPAA implementing regulations pertaining to risk management implementation, in accordance with the requirements at § 164.308(a)(1).

- ☐ It is NAIPTA's policy to fully and completely implement our risk management process and all related policies.

- ☐ The implementation of our risk management process, analyses, and improvements shall be under the direct supervision of the designated HIPAA Officer.
- ☐ The designated HIPAA Officer shall develop and implement a plan, procedures, and a timetable for the implementation of our risk management process in all its aspects. Such actions shall be consistent with our other risk management policies.

Return to Table of Contents

12 Sanction Policy

The policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).

- ☐ Establishment and implementation of appropriate, fair, and consistent sanctions have a deterrent influence on workforce transgressions such as:
  - o Can help prevent breaches of individually identifiable health information,
  - o Can help prevent or reduce the severity of HIPAA violations.
  - o Fail to follow established policies and procedures,
  - o Or who commit various offenses.
- ☐ Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- ☐ Certain offenses can invoke immediate termination, including, but not limited to:
  - o Theft
  - o Intentional lying or deception
  - o Drug or alcohol use while on the job
  - o Violence against persons or property
- ☐ Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- ☐ It is NAIPTA's policy to fully document all workforce sanctions and their dispositions, according to our Documentation Policy.

Return to Table of Contents

12.1 Information Systems Activity Review Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to information systems activity review, in accordance with the requirements at § 164.308(a)(1).

- ☐ It is NAIPTA's policy to regularly review various indicators and records of information system activity, including, but not limited to: audit logs, access reports, and security incident reports.
- ☐ The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- ☐ This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Return to Table of Contents

12.2 Assignment of Security Responsibility Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).

- ☐ It is NAIPTA's policy to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- ☐ The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be Designated HIPAA Officer, who shall report directly to the Administrative Director.
- ☐ The responsibilities and duties of the designated HIPAA Officer with overall security responsibility shall include, but are not limited to:
    - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
    - Maintain an accurate inventory of (1) all individuals who have access to the NAIPTA's confidential information, including PHI, and (2) all uses and disclosures of the NAIPTA's confidential information by any person or entity.
    - Administer employee requests and processes under HIPAA's employee rights.
    - Administer the process for receiving, documenting, tracking, investigating, and acting on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
    - Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
    - Work with appropriate technical personnel to protect the NAIPTA's confidential information from unauthorized use or disclosure.
    - Develop specific policies and procedures mandated by the Privacy Rule.
    - Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
    - Draft and disseminate the privacy notice required by the Privacy Rule.
    - Determine when NAIPTA might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
    - Ensure that any research efforts conducted or supported by the NAIPTA comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
    - Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that the NAIPTA's confidential data is adequately protected when such access is granted.
    - Ensure that all policies, procedures, and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.

- Ensure that future NAIPTA initiatives are structured in such a way to ensure employee privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Oversee employee training in the area of privacy.
- Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy.
- Remain up-to-date on laws, rules and regulations regarding data privacy and update the NAIPTA's policies and procedures as necessary.
- Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- Anticipate members' concerns and questions about the NAIPTA's use of their confidential information and develop policies and procedures to respond to those concerns and questions.
- Evaluate privacy implications of any future on-line, web-based application procedure.
- Monitor any data collected by or posted on the NAIPTA's Web sites for privacy concerns.
- Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the NAIPTA's privacy practices.

☐ It is NAIPTA's policy to fully document the assignment of overall security responsibility, and all related activities and efforts, per our Documentation Policy.

Return to Table of Contents

12.3 Authorization & Supervision Policy and Procedures

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).

☐ Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.

☐ By creating a well-managed risk management system that includes the components listed below NAIPTA can help reduce the overall risk, and reduce the likelihood of data breaches and HIPAA violations:

- Individuals having proper and appropriate authorization to access individually identifiable health information,
- Properly and appropriately supervise workforce members who have access to individually identifiable health information.
- Workforce members having access only to the individual identifiable health information that they need to perform their work-related duties,
- Fully document the authorization and supervision of all workforce members who have access to individually identifiable health information.

Return to Table of Contents

13 Workforce Clearance Policy and Procedures

This policy governs NAIPTA compliance with HIPAA and the HIPAA implementing regulations pertaining to workforce clearance, in accordance with the requirements at § 164.308(a)(3).

- ☐ It is NAIPTA's policy to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
- ☐ The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members shall be able to perform their job duties without limitations but may not have access to non-essential information.
- ☐ The HIPAA Officer, (or designee) shall develop specific procedures to ensure that the intent of this policy is executed in fact.
- ☐ Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to individually identifiable health information.
- ☐ The HIPAA Officer shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.
- ☐ It is NAIPTA's to fully document all workforce clearance-related activities and efforts.

Return to Table of Contents

14 Access Authorization Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to access authorization, in accordance with the requirements at § 164.308(a)(4).

- ☐ It is NAIPTA's policy to grant workforce members an appropriate level of access to individually identifiable health information that is based on their work-related duties and responsibilities.
- ☐ The level of access to individually identifiable health information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
- ☐ It is NAIPTA policy to fully document all access authorization-related activities and efforts.

Return to Table of Contents

14.1 Access Establishment and Modification Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the establishment and modification of workforce member access to individually identifiable health information, in accordance with the requirements at § 164.308(a)(4).

- ☐ It is NAIPTA's policy to provide a lawful and appropriate level of access to individually identifiable health information for each workforce member.
- ☐ Such access to individually identifiable health information shall be granted based on the nature and duties of the workforce member's job.
- ☐ Higher levels of access shall be provided only to those who need it.

- ☐ Any workforce member's ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- ☐ It is NAIPTA policy to fully document all access establishment and modification-related activities and efforts, according to our Documentation Policy.

Return to Table of Contents

14.2 Access Termination Policy and Procedures

This policy governs NAIPTA must comply with HIPAA and the HIPAA implementing regulations pertaining to the termination of workforce member access to individually identifiable health information, in accordance with the requirements at § 164.308(a)(3).

- ☐ It is NAIPTA's policy to terminate any workforce member's access to individually identifiable health information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
- ☐ Termination of workforce member access to individually identifiable health information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy or HIPAA offense.
- ☐ It is NAIPTA's policy to fully document all access termination-related activities, in accordance with our Documentation Policy.
- ☐ Prompt and appropriate termination of workforce member access to individually identifiable health information can greatly reduce the likelihood of data breaches and HIPAA violations.

Return to Table of Contents

14.3 Security Reminders Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to security reminders, in accordance with the requirements at § 164.308(a)(5).

- ☐ It is NAIPTA's policy to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- ☐ The designated HIPAA Officer shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
- ☐ It is NAIPTA's policy to fully document all information security reminder related activities and efforts, per our Documentation Policy.

Return to Table of Contents

15 Malware Protection Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).

- ☐ It is NAIPTA's policy to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
- ☐ Responsibility for malware protection shall reside with the designated HIPAA Officer, who shall ensure that the most powerful and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from malicious software.
- ☐ It is NAIPTA's policy to fully document all malware protection-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

16 Log-In Monitoring Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to log-in monitoring, in accordance with the requirements at § 164.308(a)(5).

- ☐ It is NAIPTA's policy to establish a program of regular monitoring and review of log-ins and log-in attempts.
- ☐ The HIPAA Officer shall assume responsibility for log-in monitoring and analysis, and for ensuring that such activities are executed on a continuous basis.
- ☐ Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- ☐ It is NAIPTA's policy to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

16.1 Password Management Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to password management, in accordance with the requirements at § 164.308(a)(5).

- ☐ It is NAIPTA's policy to require the use of strong passwords and pass-phrases by all workforce members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information.
- ☐ The responsibility for implementing this policy and any attendant procedures is hereby assigned to the designated HIPAA Officer, who shall develop and implement this policy in coordination with the IT Manager.
- ☐ All passwords used to access HRIS systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of six (8) characters in length, and must include 1 uppercase letter, 1 lowercase letter, 1 number, and 1 symbol in them.
- ☐ Passwords must or should be changed by users or management at least every three (3) to six (6) months.
- ☐ In the event of an information system compromise, as determined by the designated HIPAA Officer or IT Manager, some or all workforce-member passwords and pass-phrases may need to be changed.
- ☐ Under no circumstances shall passwords be written down and kept at or near computers and workstations. If the password is recorded or written down by an employee, it must be afforded

protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.

- ☐ It is NAIPTA's policy that any workforce member who loses, misplaces, forgets, or experiences any compromise of their password shall immediately notify the HIPAA Officer, IT Manager, or designee. Such notification of password compromise must be made immediately to HIPAA Officer, IT Manager or designee, but in no case, shall such notification be delayed more than one hour.
- ☐ Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by this organization.
- ☐ It is NAIPTA's policy to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

17 Policy on Security Incident Procedures

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.

- ☐ It is NAIPTA's policy to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
    - o Determination of the actual risk to individually identifiable health information
    - o Repairing, patching, or otherwise correcting the condition or error that created the security incident.
    - o Retrieving or limiting the dissemination of individually identifiable health information.
    - o Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
    - o Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to:
        - Employees
        - Consumers
        - Regulatory Authorities, including HHS and/or the Federal Trade Commission
        - Law Enforcement
        - The local media, if necessary and required by law
    - o Mitigating any harmful effects of the security incident.
    - o Fully documenting security incidents, along with their causes and our responses.
    - o Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
- ☐ Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- ☐ Responsibility for responding to and managing security incidents shall reside with the designated HIPAA Officer or, designee.
- ☐ The HIPAA Officer shall develop specific forms and procedures that shall be implemented in response to security incidents.
- ☐ It is NAIPTA's policy to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy.

Return to Table of Contents

18 Data Backup Plan and Storage Policy

This plan and policy governs NAIPTA compliance with HIPAA and the HIPAA implementing regulations pertaining to data backups and storage, in accordance with the requirements at § 164.310(d) (1-2) and § 164.308(a)(7).

Data Backup Plan Specifics

- ☐ IT Manager is responsible for performing daily incremental backups on NAIPTA's network Monday through Friday and one full backup per week including shared drives containing application data, employee, or client information, financial data, and crucial system information.
- ☐ NAIPTA will back up all such data automatically, per BackupExec programmed standards, nightly at 2300 hours.
- ☐ The IT Manager, or designee will, no later than 1800 the next day, place the monthly backup tapes offsite at the Downtown Connection Center ("DCC"), while daily and weekly tapes are stored in the server room. Both storage facilities have a fire resistant, media rated vault.
- ☐ The media vault meets fire and disaster standards for media and will be kept locked at all times. The IT Manager and Facilities Manager or their designees have access to the media vault.
- ☐ If the secured onsite media vault is not available or properly functioning, IT Manager and or their designees will remove backup media to a secured offsite location (DCC) until the media vault becomes available.
- ☐ IT Manager, or their designees will visually confirm that BackupExec ran successfully by utilizing the reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
- ☐ Responsible personnel will clean the tape or other backup unit(s) once the tape library provides notification.
- ☐ NAIPTA has a rotation of Monday through Thursday and Week 1-Week 4 weekly tapes. In addition, there are January to December monthly tapes.
- ☐ Currently, the backup tapes and tape drives have a life expectancy of 7 years which is monitored by the IT Manager and replaced accordingly. If there is a backup tape malfunction, this will trigger a replacement immediately.
- ☐ The IT Manager is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least twice monthly and more often if necessary to ensure data integrity, availability, and confidentiality.
- ☐ Successful restore functions are logged into the BackupExec. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- ☐ All personnel who detect or suspect a data backup problem should immediately report the same to the IT Department. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - o Narrative of the data backup problem.
    - o How long the problem has existed.

19 Disaster Recovery Plan

This plan and policy governs compliance with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).

Preventive Measures

- ☐ NAIPTA must ensure that all personnel must take the following preventive measures per Data Backup Plan and Storage Policy 18:
    - o Back up computerized files.
    - o Store backup media tape in the off-site media vault,
    - o Maintain and replace backup tapes
    - o Test integrity of backup system no less than every other week
    - o Store media properly. For example, backup tapes must be stored in climate controlled rooms, and in media-rated fireproof vaults.
    - o Protect by uninterruptible power supplies all servers and other critical equipment from damage in the event of an electrical outage.
    - o Locate file servers and other critical hardware in rooms with water based fire protection systems as change as facilities update. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
    - o In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
    - o In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
    - o Receive training in disaster preparation and recovery and know responsibilities in the event of a disaster.
- ☐ IT Manager, must take the following measures:
    - o Ensure that major hardware is covered under NAIPTA's property and casualty, and or other appropriate insurance policy or policies.
    - o Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

High Priority Tasks During Emergencies and Disaster Recovery Tasks

See Hazardous Situations and Catastrophic Events SOP

Return to Table of Contents

20 Emergency Mode Operations Plan

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).

- ☐ It is NAIPTA's policy to establish this Emergency Mode Operations Plan to implement procedures to enable continuation of critical business processes for the protection of individually identifiable health information while operating in emergency mode.

- ☐ It is NAIPTA's policy to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.
- ☐ This Emergency Mode Operations Plan shall be executed whenever NAIPTA must operate in "emergency mode" in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary.
- ☐ When "Emergency Mode" is in effect, NAIPTA shall follow the Hazardous Situations and Catastrophe Events SOP.

Plan Details

The following personnel are hereby assigned to lead the functions listed below during emergency mode operations.

Department	Department Manager
Communication/Marketing	Marketing Manager
Computing-Software/Hardware	IT Manager
Transportation Operations	Operations Director
Facilities	Facilities Manager
Fleet Operations	Fleet Manager
Media Relations	Jackie Lenners
Fleet Operations	George Gillette

Return to Table of Contents

20.1 Follow up Testing and Revision of Plans/Procedures

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).

- ☐ It is NAIPTA's policy that all individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.
- ☐ NAIPTA utilizes the procedures established in the Emergency Plan.
- ☐ The purpose of such evaluations is to improve the effectiveness of our emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) that we possess or use.

Return to Table of Contents

20.2 Emergency Access Procedures

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to procedures for emergency access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).

- ☐ It is NAIPTA's policy to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
- ☐ These emergency access procedures apply to access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ Responsibility for the development and implementation of our emergency access procedures shall reside with HIPAA Officer, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies.
- ☐ These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
- ☐ It is NAIPTA's policy to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

21 Policy on Data and Applications Criticality Analyses

This policy governs NAIPTA compliance with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).

- ☐ It is NAIPTA's policy to thoroughly assess the relative criticality of all data and applications, so that such data may be properly protected during emergencies and during normal business operations.
- ☐ Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ Criticality analysis shall be the responsibility of Administrative Director, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- ☐ Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that NAIPTA possesses and/or uses to the continuity and success of our operations.
- ☐ The most critical data and applications shall be given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- ☐ It is NAIPTA's policy to fully document all analyses of the relative criticality of both data and applications, in accordance with our Documentation Policy.

Return to Table of Contents

22 Business Associates Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to Business Associates (as defined by HIPAA at § 160.103 and as amended by the HITECH Act), in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.

- ☐ It is NAIPTA's policy to establish and maintain business and working relationships with Business Associates that are in full compliance with all HIPAA requirements.
- ☐ Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the Administrative Director, who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected, and safeguarded by our Business Associates.
- ☐ With regard to Business Associates, the duties, and responsibilities of the Administrative Director, shall include, but are not limited to the following:
    - o Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, and any requirements of State laws in Arizona where we operate.
    - o Ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected, and safeguarded by our Business Associates.
    - o Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), whether in electronic form ("ePHI") or hardcopy form.
    - o Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before entrusting such information to them.
    - o Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy.

Return to Table of Contents

23 Facility Security Plan and Policy

This plan and policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a) (1-2).

- ☐ It is NAIPTA's policy to provide strong facility security, in addition to other technical and administrative safeguards, to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ Primary responsibility for facility security is hereby assigned to NAIPTA's Facilities Manager, who shall analyze the security of our facility and implement devices, tools, and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

- ☐ The analyses of our facility security should include, but are not limited to, the following factors:
    - o Windows and doors
    - o Roofs and the potential for roof access
    - o Locks and keys
    - o Electronic access control systems
    - o Video cameras and video surveillance systems
    - o Electronic alarms and related systems
    - o Employee, partner, vendor, and guest access
    - o Vehicle parking security
    - o Routine and non-routine deliveries
- ☐ It is NAIPTA's policy to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.

Return to Table of Contents

23.1 Information Access Control and Validation Procedures

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to information access control and validation, in accordance with the requirements at § 164.310(a) (1-2).

- ☐ It is the Policy of NAIPTA to implement and support strong information access control and validation procedures, in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for developing, testing, analyzing, and periodically updating information access control and validation procedures shall reside with NAIPTA's IT Manager.
- ☐ It is NAIPTA's policy to fully document information access control and validation procedures, in accordance with our Documentation Policy.

Return to Table of Contents

23.2 Facility Security Maintenance Records Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to the creation and use of facility security-related maintenance records in accordance with the requirements at § 164.310(a) (1-2).

- ☐ It is NAIPTA's policy to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
- ☐ Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.
- ☐ Responsibility for the creation and updating of facility security maintenance records is hereby assigned to NAIPTA Facilities Manager, who shall establish procedures for maintaining such records in appropriate form.
- ☐ It is NAIPTA's policy to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

24 Workstation Use and Security Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to workstation use and security, in accordance with the requirements at § 164.310(b) and § 164.310(c).

- ☐ It is NAIPTA's policy to establish and maintain this workstation use policy in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this workstation use and security policy, and any procedures associated with it, shall reside with IT Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), to restrict access to authorized users only.
- ☐ It is NAIPTA's policy to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

25 Media Disposal Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d) (1-2).

- ☐ It is NAIPTA's policy to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for proper media disposal and disposition shall reside with IT Manager, who shall develop procedures to ensure the proper disposition of all such media.
- ☐ It is NAIPTA's policy to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy.
- ☐ All scheduled files to be destroyed will follow NAIPTA Records Retention Policy

Return to Table of Contents

25.1 Media Re-Use Policy

This policy governs compliance with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d) (1-2).

- ☐ It is NAIPTA's policy to properly erase and or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used.
- ☐ Responsibility for proper media re-use shall reside with IT Manager, who shall develop procedures to ensure the proper disposition of all such media before any re-use.

- ☐ It is NAIPTA's policy to fully document media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

25.2 Hardware and Media Accountability Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to hardware and media accountability, in accordance with the requirements at § 164.310(d) (1-2).

- ☐ It is NAIPTA's policy to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with IT Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ It is NAIPTA's policy to fully document all hardware and media accountability-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

26 Unique User I.D. Policy

This policy governs the compliance with HIPAA and the HIPAA implementing regulations pertaining to the mandatory use of unique user I.D.'s, in accordance with the requirements at § 164.306, and § 164.312(a)(1).

- ☐ It is NAIPTA's policy to exclusively use unique user I.D.'s for all information system access and activities, in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with NAIPTA's IT Manager, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.'s.
- ☐ Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

27 Automatic Lock Policy

This policy governs compliance with HIPAA and the HIPAA implementing regulations pertaining to the use of automatic log-off applications, in accordance with the requirements at § 164.306 and § 164.312(a) (1-2).

- ☐ It is NAIPTA's policy to always use automatic lock applications or systems on all workstations and computers, in full compliance with all the requirements of HIPAA.

- ☐ Responsibility for the development and implementation of this automatic lock policy, and any procedures associated with it, shall reside with IT Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to specify the proper functions and procedures of our automatic lock systems on all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document automatic lock-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

28 Encryption and Decryption Policy

This policy governs compliance with HIPAA and the HIPAA implementing regulations pertaining to the encryption and decryption of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in accordance with the requirements at § 164.312(a) (1-2).

- ☐ It is NAIPTA's policy to establish, implement, and maintain an effective encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with IT Manager, Jon Matthies, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

29 Audit Controls Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).

- ☐ It is NAIPTA's policy to establish and maintain this audit controls policy in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with IT Manager who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all audit controls-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

30 Data Integrity Controls Policy

This policy governs compliance with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c) (1-2).

- ☐ It is NAIPTA's policy to establish and maintain this data integrity controls policy in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with IT Manager, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

30.1 Data Integrity Controls Procedures

These procedures govern NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c) (1-2) and § 164.312(e) (1-2).

- ☐ It is NAIPTA's policy to establish and maintain these data integrity controls procedures in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of these data integrity controls procedures, as with our Data Integrity Controls Policy, shall reside with IT Manager, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- ☐ Specific integrity control procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ☐ It is NAIPTA's policy to fully document all data integrity controls-related procedures, activities, and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

31 Person or Entity Authentication Policy

This policy governs NAIPTA's compliance with HIPAA and the HIPAA implementing regulations pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).

- ☐ It is NAIPTA's policy to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- ☐ Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with IT Manager and HIPAA Officer who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.

- ☐ Specific procedures shall be developed to specify the proper authentication of persons and entities who access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations, and systems.
- ☐ It is NAIPTA's policy to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

Return to Table of Contents

ACKNOWLEDGEMENT OF RECEIPT

I HAVE RECEIVED A COPY OF THE NORTHERN ARIZONA INTERGOVERNMENTAL PUBLIC TRANSIT AUTHORITY ("NAIPTA") HIPAA POLICY DATED _____. I UNDERSTAND THAT I AM TO BECOME FAMILIAR WITH ITS CONTENTS. FURTHER, I UNDERSTAND:

- THE LANGUAGE USED IN THIS HIPAA COMPLIANCE POLICY IS INTENDED TO ASSIST YOU IN LEARNING THE OBLIGATIONS THAT NAIPTA, AS A COVERED ENTITY AND YOU AS AN EMPLOYEE SHOULD COMPLY WITH HIPAA REGULATIONS.

- THE HIPAA COMPLIANCE POLICY IS NOT ALL INCLUSIVE, BUT IS INTENDED TO PROVIDE ME WITH A SUMMARY OF SOME OF THE ORGANIZATION'S GUIDELINES.

- THE NEED MAY ARISE TO CHANGE THE GUIDELINES DESCRIBED IN THE HIPAA COMPLIANCE POLICY. THE ORGANIZATION THEREFORE RESERVES THE RIGHT TO INTERPRET THEM OR TO CHANGE THEM WITHOUT PRIOR NOTICE. UPDATES CAN BE FOUND IN PAYCHEX WITH THE MOST CURRENT REVISION DATE.

_____ _____ _____ _____ _____

Employee Name Date

Return to Table of Contents