HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Protected Health Information	
Policy #: 1-01	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164	

Policy:

Performance Physical Therapy will not use or disclose protected health information without the consent or authorization of its patients for purposes other than treatment, billing or operations related to treatment and billing. All personnel will understand and be able to identify the elements of protected health information.

Procedure:

1. Protected health information is any individually identifiable information contained in the patient's medical record or files. This includes the patient's name, address, diagnosis, chart notes, lab results, treatment plan, insurance or financial information.

2. Every chart should contain a signed consent form from the patient that authorizes or prohibits the practice from using or disclosing protected health information. The consent from must have been signed within one year of the current date.

3. Personnel may use and disclose protected health information for treatment, billing or operations related to treatment and billing without patient consent. Any other use of protected health information must be authorized by the patient and documented in the chart.

4. It is expected that personnel who release protected health information for any reason will release only the minimum amount of information necessary based on the purpose of the request. For example, if an insurance company requests chart notes for the purpose of reviewing a claim, only the notes specific to that date of service and procedure under review should be released.

5. If protected health information is used or disclosed for any other purpose than treatment, billing or operations related to treatment and billing, the information must be "de-identified" by removing any and all information that would distinguish the individual's record from a group.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Release of Information where Authorization Not Required	
Policy #: 1-09	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.	

Policy:

From time to time, Performance Physical Therapy will release patients' health information without patient consent or authorization. Performance Physical Therapy will release the minimum amount of information necessary to the extent that such release complies with the law and satisfies the request.

Procedure:

1. A patient's written authorization is not required for the following: judicial request; health oversight; law enforcement; public health activities; coroners and medical examiners and specialized government functions. Specialized government functions include veterans affairs, military activities, national security and intelligence activities; protective services for the President and others; determination of medical stability; correctional institutions; for disclosure about victims of abuse, neglect or domestic violence and to organ procurement organizations.

2. When information is requested by any of the above mentioned entities or for any of the reasons indicated above, the Compliance Officer/Practice Administrator will verify that the request is coming from an appropriately empowered entity and verify that the individual to whom the information is released is acting on behalf of that entity.

3. Information will be released within two days of the request or after the Compliance Officer or Practice Administrator has sufficient evidence to verify that information is being released appropriately.

4. In order to verify the identity of individuals requesting information for the purposes mentioned above, the Practice Administrator or Compliance Officer will ask for at least two of the following:

    - A written request on company letterhead indicating the purpose for which information will be used and the specific information requested
    - Identification including badge or employee ID presented in person along with a driver's license or other valid form of picture ID
    - Contact information for the immediate supervisor or human resources department for telephone verification of employment

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Patient Information Consent Form	
Policy #: 1-03	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.506	

Policy:

Performancet Physical Therapy will require all patients to sign a consent form indicating that they have read and agree to the use and disclosure of protected health information for purposes outlined in the practice's Notice of Information Practices.

Procedure:

1. A copy of the Notice of Information Practices will be provided to all new patients.

2. Patients will be asked to review a copy of the Notice of Information practices and sign the Patient Information Consent Form prior to beginning treatment.

3. A copy of the signed, dated consent form will be kept with the patient chart.

4. Consent forms will be effective for one year from the date of signature. If a consent form in the chart is over one year old, the patient should be asked to sign an updated form.

5. Patients who do not sign the consent form or who wish to have the use of their protected health information restricted in any way will be asked to notify the practice in writing.

6. Requests for restrictions on the use of protected health information will be considered by the Practice Administrator or Compliance Officer on a case by case basis using the following criteria:

    - Is the restriction request reasonable
    - Will the restriction negatively affect the practice's business cycle – i.e. will it change the timeline for payment
    - Will the restriction interfere with the practice's ability to treat a patient
    -

7. The Practice Administrator or Compliance Officer will notify the patient in writing of Performance Physical Therapy decision to accept or not accept the patient's requested restriction within fifteen days of receipt of the request.

HIPAA Compliance Policies and Procedures

Disciplinary Standards and Corrective Action Initiatives

Policy Name: Investigation of Issues, Complaints, and Problems	
Policy #: 3-04	Origination Date:
Review Date: March 15, 2003	Approval:
Reference:	

Policy:
The Compliance Officer will be responsible for implementation of investigations of reports or reasonable indications of suspected non-compliance within thirty days of notification. Investigations revealing criminal or civil violations will be discussed with legal counsel and reported to the applicable authorities with 10 days of Investigation completion.

Procedure:

1. The Compliance Officer may receive reports or indications of non-compliance through the following channels:
    - Compliance Committee activities such as audits and report reviews;
    - Direct reports from employees;
    - Anonymous report.
2. The Compliance Officer will initiate a Compliance Investigation Report within 30 days of report or indications.
3. The Compliance Officer will investigate the allegations through any of the following methods:
    - Review of reports;
    - Review of claims;
    - Review of medical records and documentation;
    - Review of contracts or arrangements;
    - Interview with employees;
    - Onsite monitoring.
4. After completion of the investigation, if possible criminal or civil violations have been identified, the outcomes will be discussed with legal counsel. Any matter that could indicate violation of Federal or State law should be referred to counsel and reported to the applicable authority within 10 days of Investigation completion. The Compliance Officer and Compliance Committee should review all other matters.

The Compliance Officer and Compliance Committee will work to formulate any disciplinary actions, corrective action plans, return of overpayments or process modification as indicated by the investigation outcomes.

HIPAA Compliance Policies and Procedures

Staff Training and Termination

Policy Name: Training Requirements	
Policy #: 4-01	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142, 164	

Policy:

Performance Physical Therapy will require all new and current employees and partners to attend initial security and privacy training.

Procedure:

1. All current employees and providers will be required to attend compliance training offered by April 11,2003 by Compliance Officer . To signify completion of training, all participants must complete a post-test and sign the attestation of attendance and compliance agreement.

2. All new employees and providers will be required to complete the compliance training module within thirty (30) days of employment. To signify completion of training, all participants must complete the post-test and sign the attestation of completion and compliance agreement.

3. Failure for new or current employees and physicians to complete the required any training may be grounds for dismissal.

4. Compliance training will be ongoing and continued participation is required. Training may occur in staff meetings, via newsletters, faxes or bulletin boards.

HIPAA Compliance Policies and Procedures

Policy Name: Monitoring and Auditing	
Policy #: 3-01	Origination Date:
Review Date: March 15, 2003	Approval:
Reference:	

Policy:

_Performance Physical Therapy will establish methodologies for monitoring activities related to the privacy and security of protected health information. The practice will audit activities related to the privacy and security of protected health information at regular intervals throughout the year.

Procedure:

1. The practice will monitor the following:
    - ❑ Use, disclosure and release of protected health information
    - ❑ Complaints
    - ❑ Access to system and medical records
    - ❑ System maintenance activities
    - ❑ Document storage and disposal activities
    - ❑ Hardware and software
2. It is the responsibility of the Compliance Officer or designee to determine how the practice will monitor the above mentioned activities. It is expected that the monitoring will constitute at least the following:
    - ❑ Maintenance of an information release/disclosure log with patient file
    - ❑ Maintenance of a complaint register
    - ❑ Records of each time information is accessed
    - ❑ Records of system maintenance activities
    - ❑ Records of document storage
    - ❑ Hardware and software inventories
3. It is the responsibility of the Compliance Officer or designee to audit records for potential problems or violations of practice privacy and security policies. Audits will be scheduled at least every six months and more frequent auditing could occur if a problem is found.
4. When problems are discovered, the Compliance Officer and the Privacy/Security committee members will determine the best course of action. This can include further training directed at solving the problem or disciplinary actions for non-compliant staff or partners.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Notice of Information Practices	
Policy #: 1-02	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.506	

Policy:

Performance Physical Therapy will notify all patients of how it intends to use or disclose their protected health care information through a Notice of Information Practices. Performance Physical Therapy will not use health information in any way beyond that which is stated in its Notice of Information Practices.

Procedure:

1. Performance Physical Therapy will develop and post a Notice of Information practices in a visible spot in its waiting area or lobby and in its exam rooms or treatment areas.

2. A copy of the Notice of Information Practices will be provided to all new patients before they sign the practice consent form.

3. A copy of the Notice of Information Practices will be provided to any patient who requests it at any time.

4. If the Notice of Information Practices is updated, new copies will be posted and all patients who have received treatment within the past five years will be informed of the changes.

5. All staff will be familiar with how the practice uses and discloses protected health information and be able to answer patients' questions about the Notice of Information Practices

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Data Authentication	
Policy #: 2-08	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will take steps to ensure the security of data that is transmitted over a communications network to the extent that those steps are necessary.

Procedure:

1. Performance Physical Therapy will instigate integrity controls and message authentication. Internal networking can be considered secure if the practice instigates a user based security system where all users have a specific identification and access code.

2. If Performance Physical Therapy uses the Internet to transmit data, some form of encryption device will be employed. This can most often be handled through the purchase of commercial software that provides protection against unauthorized access to data.

3. Value added networks, private wires and dial up connections are not subject to the encryption requirement.

4. If the vendor's software offers integrity controls and message authentication the practice will take advantage of those.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Physical Safeguards	
Policy #: 2-07	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will make every effort to ensure that there are physical safeguards in place to protect practice data from inadvertent or illegal access.

Procedure:

1. Receipt of any diskettes, tapes or other forms of media that contain protected health information will be noted in the practice information management inventory. Information will be transferred to the practice system in a timely fashion (within 10 days) and materials used for transmission of information will be destroyed.

2. Removal from Performance Physical Therapy site of hardware and software that might contain protected health information is prohibited.

3. Performance Physical Therapy will keep a log of system maintenance procedures and verify the identification of any maintenance personnel not known to the practice.

4. Workstations will be placed in secure areas where monitors are not easily viewed by patients or unauthorized personnel.

5. All employees are required to log off of terminals before leaving them unattended for any length of time. At no time is an employee allowed to log on using another employee's password.

6. No patients, family members or their representatives will be allowed to view data in the system or gain access to the system using employee passwords.

7. All visitors to the practice for reasons other than treatment will be asked to sign in and verify their identity before being allowed to enter secure areas.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Security Configuration Management and Incident Procedures	
Policy #: 2-06	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will manage system integrity by periodically checking for viruses, detecting and containing inadvertent or illegal access, developing an inventory of all hardware and software and correction of any weaknesses in the system.

Procedure:

1. The Compliance Officer or System Administrator will work with vendors to ensure that proper mechanisms are in place to prevent, detect, contain and correct any security breaches.

2. These mechanisms will include regular system virus checks, security testing and maintenance review of hardware and software for security breaches as prescribed by the vendor.

3. All mechanisms used to manage the security configuration of the system will be documented by the vendor or the Compliance Officer at regular intervals.

4. Any breaches of security detected by the System Administrator or Compliance Officer will be solved by the Compliance Officer or discussed with the vendor. Partners of the practice will be informed about security breaches and allowed to comment on solutions designed to respond to them.

5. Periodically, security processes will be reviewed and updated by the Compliance Officer or System Administrator along with the vendor. The Compliance Officer will conduct an annual risk analysis and devise a plan to manage risk.

6. Any employee suspected of intentional involvement in security breaches will be terminated. Any employee that is inadvertently involved in a security breach will be offered training and education on system procedures.

7. Periodically, the Compliance Officer and / or the System Administrator will conduct training sessions for employees to alert them to specific security risks.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Information Access Control	
Policy #: 2-05	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Access to health information at Performance Physical Therapy will be restricted to those employees who have a business need to use it.

Procedure:

1. The Compliance Officer and Practice Administrator will have emergency access to the system. All other types of access to the system will be restricted based on the contextual use of the information (e.g.: insurance department will have access to all data necessary to process and mail out claims); the role of the user (e.g.: therapists will have access to chart notes and medical records but not necessarily insurance information) and/or the type of user (e.g.: some users will be able to view and change data in certain areas of the system while others will only be able to view it or may not be able to see it at all).

2. All employees must be given clearance by the Compliance Officer prior to accessing the system. In order to gain security clearance, the employee must be legally employable and have an active position that requires system access. Employees that do not require system access (Janitors etc) will not be given passwords or access to the system.

3. Once access is defined, the Compliance Officer or System Administrator will assign all employees individually identifiable passwords. All employees will be required to log in to the system using their unique password and the system will log employees off after a specified period of time in which there has been no input from the user.

4. The Compliance Officer or System Administrator will be responsible for maintaining and managing levels of access and user passwords. Passwords will be chosen using a random generation of numbers and letters to reduce the likelihood of password discovery. Employees will be required to maintain the confidentiality of their passwords.

5. Monthly or at least quarterly, the System Administrator or Compliance Officer will run reports to audit system access. Other mechanisms may be put in place to monitor system access from entry points other than user entry.

6. Security incidents will be noted and logged. The System Administrator or Compliance Officer and vendors or security specialists will address any security breaches.

7. Routine changes to system hardware and software will be validated against the security system to avoid creating inadvertent security weaknesses.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Processing Records Received by the Organization	
Policy #: 2-04	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

From time to time, patients will ask that Performance Physical Therapy receive transfers of their protected health information electronically from other providers or payers. Performancet Physical Therapy will make every effort to ensure that the electronic transfer occurs in a secure fashion and that records are maintained securely.

Procedure:

1. Routine and non-routine transfers of patient information will be treated with the same standards as current electronic medical records are treated.

2. Performance Physical Therapy will develop a methodology along with its vendor for the receipt, transmission and dissemination electronic health information.

3. All information received by Performance Physical Therapy will be stored in its patient accounting system for up to seven years past the date of service or in accordance with (State) standards for medical record storage. After seven years from the last active date of service, medical records will be purged from the system and/or archived in the practices' medical records archive (if available).

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Contingency Plan for Responding to System Emergencies	
Policy #: 2-03	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will develop and follow a contingency plan for back up and storage of data to allow for recovery of patient information in the event that the system or network is compromised.

Procedure:

1. All software applications and data will be analyzed and prioritized based on the criticality of the data contained therein.

2. The patient accounts system and all other systems that contain protected health information will be backed up daily or weekly in accordance with the back up plan designated by the software vendor. The most recent back up tapes or devices will be stored off site to protect them from damage by fire or other unforeseen disaster. This can easily be accomplished by requiring the Compliance Officer to take the tape/disc home or to take the tape/disc to a safe deposit box or by purchasing a fire proof lock box for the practice.

3. All original software will be stored in a fire proof lock box within the practice. Other proprietary systems will be insured against loss or damage.

4. If the system is compromised, Performance Physical Therapy will recover data using available system software and the most recent available system back up.

5. The Compliance Officer for Performance Physical Therapy will test the back up system quarterly to ensure that it is operating properly.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Chain of Trust Agreements with Partners	
Policy #: 2-09	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

All data transactions that occur through third parties (e.g.: claims clearinghouses or billing agencies) will be subject to the signature of a chain of trust agreement with those parties before data can be transacted or disclosed.

Procedure:

1. Practice attorneys will develop a "chain of trust" contract for the practice and its third party contractors. This is a contract in which the parties agree to electronically transmit data and protect the transmitted data in ways compliant with HIPAA security standards.

2. All third party contractors to whom protected health information is transmitted electronically will be required to sign chain of trust agreements. This agreement does not include referring physicians or hospitals who use data for the treatment or billing for treatment of the patient.

3. Contracts will be kept on file in the insurance department of Performance Physical Therapye. Contracts will be reviewed every three years along with other administrative safeguards.

4. Once a year, in order to monitor compliance with the agreement, the Compliance Officer of the practice will contact all chain of trust partners of the practice and ask them to confirm that data being transmitted is secure and that their data practices are HIPAA compliant. Confirmation could include obtaining copies of certification of security practices of the chain of trust partner but it will be left to the discretion of the practice Compliance officer to determine sufficient compliance with the chain of trust agreement.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Certification of Security System	
Policy #: 2-02	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will evaluate all computer systems and network designs to certify that an appropriate level of security has been implemented.

Procedure:

1. The security system for electronic data will be evaluated every three years for any risk areas with regards to the integrity, confidentiality and availability of protected health information.

2. This evaluation may be carried out by the practice in conjunction with Performance Physical Therapy's software/system vendors or an external third party accrediting agency.

3. Measures will be taken to make improvements in the security system should they be deemed necessary by Performance Physical Therapy.

HIPAA Compliance Policies and Procedures

Security Standards:

Policy Name: Selection and Execution of Security Measures	
Policy #: 2-01	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 142	

Policy:

Performance Physical Therapy will use HIPAA approved security systems and measures recommended to it by its patient accounting system and other software vendors to protect the integrity, confidentiality and availability of electronic data. Performance Physical Therapy will document its selection of security measures and update its documentation periodically.

Procedure:

1. Performance Physical Therapy will inventory all software programs and systems that could contain protected health information.

2. Vendors for those software programs will be contacted and asked to provide a diagram and documentation of the security measures and access levels available in the software.

3. The Compliance Officer for Performance Physical Therapy will select an appropriate level of security that includes at least the following: individual authentication of users, access controls, audit trails, physical security, disaster recovery, protection of remote access points, protection of external electronic communications and periodic system assessment recommendations.

4. Documentation of the selection process and the choice of security system will be kept by the Compliance Officer. Documentation of system security levels will be made available to individuals responsible for implementation.

5. The documentation of the security system and security measures will be updated every three years to ensure that a HIPAA approved level of security is maintained.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Release of Protected Health Information to Business Associates	
Policy #: 1-12	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 160.103, 164.502(e), 164.514(e)	

Policy:

Performance Physical Therapy will ensure via contract that all business associates to whom protected health information is released will use the information only for the purposes for which is was disclosed, safeguard the information from misuse and will cooperate with Performance Physical Therapy in situations where patients need access to their information.

Procedure:

1. A Business Associate is any person or entity who provides services to Performance Physical Therapy that require the use or disclosure of protected health information. Examples of business associates include insurance companies, billing companies, information technology vendors, marketing firms and consultants.

2. Business Associate requirements do not apply to information exchanges with referring physicians, hospitals, PT practices or other entities for the purpose of treatment.

3. Performance Physical Therapy will develop a list of all business associates and ask them to enter into a contract with respect to the use and disclosure of protected health information.

4. Periodically, a representative from Performance Physical Therapy will visit or call the business associate to verify that protected health information is being used in accordance with the contract.

5. The term of the contract will be in effect for as long as the Business Associate maintains files containing protected health information.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Complaints and Zero Tolerance for Retaliation	
Policy #: 1-11	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.	

Policy:

Performancet Physical Therapy will not tolerate any retaliatory acts against employees or patients who file a complaint with the HHS secretary, participate or testify in an investigation or verbally oppose any actions taken by the practice that are unlawful under HIPAA Administrative Simplification.

Procedure:

1. Employees and patients will be encouraged to report any activities deemed unlawful under HIPAA Administrative Simplification in writing to the Compliance Officer of Performance Physical Therapy.

2. The Compliance Officer will review all complaints and respond to them in writing within three days of receipt of the complaint. Responses will include an explanation of any actions that will be taken to rectify situations where the Compliance Officer considers that the complaint is justifiable.

3. If violations of the privacy laws are discovered through the complaints process or in other ways, the Compliance Officer will be responsible for re-designing work processes to comply with the legislation and re-training all staff and providers.

4. The address of The Department Health and Human Services will be kept on file for employees or patients who request it from the Compliance Officer.

5. Performance Physical Therapy will cooperate fully with requests for information from government investigators and/or patients who are sending complaints to DHHS.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Minimum Necessary Information Standards	
Policy #: 1-04	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.502(b)	

Policy:

Performance Physical Therapy will take reasonable steps to limit the use or disclosure of protected health information.

Procedure:

1. This policy does not apply to disclosure requests from referring physicians or health care providers who are treating the patient, the individual who is the subject of the information, standard HIPAA transactions, DHHS and law enforcement officials and other uses or disclosures required by law.

2. Access to protected health information and the type of information available will be limited to the employees who need the information to conduct their work duties. The security plan contains a list of employee job descriptions and levels of access to information.

3. For routine or recurring requests from payers (for example: requests for chart notes or prepayment reviews) the information released will be restricted to the service in question.

4. For non-routine requests, the Compliance Officer will use the following criteria to determine the amount of information that needs to be released:

    - Is the information required to support a claim or receive payment?
    - If information is not released, will it delay quick, effective treatment?
    - Is releasing the information consistent with professional standards protecting the unnecessary sharing of patient information?

5. In certain circumstances, the judgement of the party requesting the information may be relied upon to determine the minimum amount of information necessary for its purpose. If the request for information is made by a public official or agency, another provider or representative from a payer or a medical researcher with appropriate documentation from an Institutional Review Board, then the exact information they request can be released to them.

6. Any information released in this manner will be subject to verification of the identity of the person requesting the information. Identity can be verified by asking for written requests on company letterhead or request in person with appropriate corporate identification.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: De-Identified Health Information	
Policy #: 1-05	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.502(d)	

Policy:

Periodically Performance Physical Therapy will want to use health information contained in its records without getting the patients' prior authorization to analyze its business activities, evaluate the quality of services provided, develop marketing materials or for other operational purposes. If protected health information is to be used for any purpose other than treatment, billing or operations related to treatment and billing, the information will be "de-identified" by removing all information that could distinguish the individual's record from a group of records.

Procedure:

1. The patient's name, address, diagnosis, chart notes, lab results, treatment plan, insurance or financial information are all considered protected health information. All of these elements appearing together could be used to identify a patient.

2. It is the responsibility of the employee to determine the information on a report that could reasonably be used to identify an individual.

3. Any information that could uniquely identify the patient will be removed from data printouts or reports. For example: a report to analyze treatment patterns by market could contain zip codes and diagnoses but not patient address or names.

4. Patient address information can be used for newsletters and for contacting the patient prior to an appointment but will not be used for targeted marketing activities. For example: Performance Physical Therapy could send out quarterly newsletters to its entire patient base but PPT could not develop and send marketing materials to patients who have had a specific treatment plan for a hip injury unless PPT patients indicate that they would like to receive such targeted materials on their consent forms.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Rights of Individuals	
Policy #: 1-06	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.522-528	

Policy:

Performance Physical Therapy will honor the rights of individuals with respect to their health information.

Procedure:

1. All employees will be educated about the rights of individuals with respect to their health information.

2. Individuals will be allowed to request access to and copy their individual medical records at any time provided they show verifiable identification. Verifiable identification is a driver's license or some other form of identification with a picture. Performance Physical Therapy may charge individuals $20.00 per chart or $.10 per page to cover copying costs.

3. Employees will be trained to inform individuals of their right to restrict the use of their information. Employees will also be trained to inform individuals of Performance Physical Therapye's policies on authorization for release of medical information.

4. Individuals must submit requests for restriction of the use of their information in writing. When a request is accepted by PPT, it will be placed in the patient's file and noted on the outside of the chart where it is easily visible to the employee.

5. Any time information is released for purposes not related to treatment or billing, it will be noted on a log placed in the patient's chart. If an individual requests a copy of the chart log, then the individual will be provided a copy at no charge. The log should be current and indicate all instances of release of information within the lessor of six years from April 14,2003 or six years from date of the request.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Information Release Authorization	
Policy #: 1-07	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.	

Policy:

From time to time, patients will need to release their health information to others for various reasons (for example – applying for life or disability insurance or seeking certain job assignments). Performance Physical Therapy requires patients to complete and sign a written authorization form prior to releasing the information.

Procedure:

1. The authorization form completed by the patient will include the following information: Name and address of the entity to which the information is released; purpose for releasing the information; description of what information is to be released; expiration date; signature or other authentication and date of signature.

2. Individuals will be asked to read and initial a section of the form that notifies them that they can revoke their authorization at any time and that the information that will be disclosed is subject to re-disclosure and no longer protected by the Privacy regulations (45 CFR 164).

3. When a patient requests release of health information, employees will provide the patient with PPT's Information Release Authorization form and ask patients to complete it.

4. Information will be released within two days of receiving completed form.

5. The form will be kept with the patient's chart and any information releases will be logged.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: **Performance Physical Therapy** Authorization	
Policy #: 1-08	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.	

Policy:

From time to time, Performance Physical Therapy will be asked to release patients' health information to others for various reasons (for example – developing marketing materials for PPT or working with research organizations). Performance Physical Therapy will ask patients to authorize the release of protected health information for marketing and other purposes by checking a box on the Patient Information Consent form.

Procedure:

1. All patients will be asked to sign a consent form that allows the use protected health information for treatment, billing and operations related to treatment and billing (See Policy 1-03).

2. The patient will be given an option on the same form to check a box that authorizes Performance Physical Therapy to use protected health information in the following ways: targeted marketing, fund raising and solicitation of participation in research studies (where applicable).

3. The patient has the right to copy or inspect information that will be used for those purposes and the individual can choose not to check the authorization box without affecting his consent to use protected health information for treatment, billing or operations related to treatment and billing.

HIPAA Compliance Policies and Procedures

Privacy Standards:

Policy Name: Release of Information to Designated Individuals	
Policy #: 1-10	Origination Date:
Review Date: March 15, 2003	Approval:
Reference: 45 CFR 164.	

Policy:

Patients may designate individuals to whom their information can be released.

Procedure:

1. Patients will be provided the opportunity to fill out a form that authorizes the release of their information to designated individuals. The form will be kept with the patient's chart.

2. Designated individuals can include relatives, family members, decedents, friends and personal representatives.

3. When a designated individual requests the release of protected health information, employees will check the form in the chart and verify the identification of the person requesting the information before releasing it.

4. The person requesting information must present a valid picture ID in order to verify his/her identity. In the case of decedents, the person must present a copy of the death certificate along with a valid picture ID.

5. Employees will take a copy of the ID, verify it against the information in the chart before releasing the information.

HIPAA Compliance Policies and Procedures

Disciplinary Standards and Corrective Action Initiatives

Policy Name: Disciplinary Actions for HIPAA Non-Compliance	
Policy #: 3-02	Origination Date:
Review Date: March 15, 2003	Approval:
Reference:	

Policy:
Performance Physical Therapy will establish and enforce specific actions against employees that do not follow the specific policies and procedures outlined in the HIPAA Compliance Program.

Procedure:

1. The goals of disciplinary actions are:

- Assist the employee in understanding the commitment of the practice to its HIPAA Compliance Program;
- Assist the employee in understanding his/her role in the Compliance Program;
- Ensure participation in designated educational programs to enhance understanding of employee's responsibilities;
- Decrease, through stringent monitoring, the potential liability of non-compliance by employees;
- Provide a structured format to discharge from employment those employees that are unwilling or unable to meet the requirements of the HIPAA Compliance Program

2. It is the responsibility of the Compliance Officer or designee to determine the application of disciplinary standards based on the type, intent and severity of the violation, problem or incident. Some incidents may require immediate termination such as embezzlement of funds from any source, acceptance of remuneration for referrals, or intentional fraudulent billings for services or supplies.

3. If disciplinary action is to be initiated, the following format will be followed for minimal severity violations:

- **Step One**: Oral warning by Compliance Officer or designee. The officer or designee will meet with the individual involved in the violation and discuss the problem identified, plans to prevent further violations including the educational plan, and plans to monitor the individual's work at least monthly until no further violation is identified. The Compliance Officer or designee will assign the audit to the appropriate Compliance Committee member. Re-evaluation will occur at no more than 8 weeks from the original warning.
- **Step Two:** Written reprimand by the Compliance Officer or designee to the employee file. The Compliance Officer will meet with the individual to review the written reprimand, the plan to prevent further violations including the educational plan, and the plan to perform spot and weekly audits. The Compliance Officer or designee will assign the audit to the appropriate Compliance Committee member. Re-evaluation will occur at no more than 4 weeks from the original reprimand.

- **Step Three:** Entering into a corrective action agreement. The Compliance Officer or designee will draft a corrective action agreement that states specifically what actions the individual must do within the following two weeks to avoid further disciplinary action. The Compliance Officer will meet with the individual to go over the corrective action agreement and the plan to audit 100% of work and plan for preventing further violations and the intensive educational plan. This time intensive process will require coordination between the Compliance Officer and Compliance Committee members to perform audits before any further billings are submitted.

- **Step Four:** Suspension without pay for two weeks. The Compliance Officer, with Board of Director approval, will suspend the individual without pay for a two-week time-period. During the suspension period, the individual will be offered further educational opportunities to pursue during the time off.

- **Step Five:** If, after return from the two-week suspension, the individual continues with previous behaviors causing continued violations, the individual with be discharged from employment with Board of Directors approval.

HIPAA Compliance Policies and Procedures

Disciplinary Standards and Corrective Action Initiatives

Policy Name: Corrective Action Plans for HIPAA Non-Compliance	
Policy #: 3-03	Origination Date:
Review Date: March 15, 2003	Approval:
Reference:	

Policy:
Performance Physical Therapy will utilize corrective action plans to assist employees in understanding their responsibilities in the HIPAA Compliance Program.

Procedure:

1. The Compliance Officer is responsible for formulation of the corrective action plan in the third step of disciplinary standards or earlier if indicated at the discretion of the Compliance Officer.

2. The corrective action plan will contain the following items:

   - Statement of the current violation types observed;
   - Statement of actions to date, including audit results;
   - Description of mandatory educational program that must be completed;
   - Description of the activity that must occur or activities that must cease to obtain compliance;
   - Outline of time frame for completion of education and activity changes;
   - Statement that failure to meet the requirements of the corrective action plan will result in a two-week suspension without pay.

3. The corrective action plan must be signed and dated by both the individual and the Compliance Officer. A copy will be placed in the employment file.