



PRIVACY PRACTICES POLICY AND PROCEDURES MANUAL

1. AUTHORIZATIONS FOR USE, DISCLOSURE, RELEASE OR REQUEST OF PHI
2. BUSINESS ASSOCIATE POLICY
3. PRACTICE COMPUTER PRIVACY AND SECURITY POLICY
4. DATA CLASSIFICATION POLICY
5. DESTRUCTION AND/OR DISPOSAL OF PHI AND STORAGE MEDIA
6. DISCLOSURE OF PHI (for Worker's Compensation Proceedings)
7. EMAIL POLICIES
8. EMERGENCY, CATASTROPHY AND RELATED POLICIES
9. EMPLOYEE PRIVACY TRAINING
10. EMPLOYEE BUSINESS ASSOCIATES AND OTHERS; PROCEDURES ON VIOLATION OF POLICY
11. FAX POLICIES
12. INTERNET, EXTRANET AND LAN/WAN POLICIES
13. MINIMUM NECESSARY POLICIES AND PROCEDURES
14. NOTICE OF PRIVACY PRACTICES
15. PATIENT COMPLAINT PROCEDURES
16. PATIENT'S PRIVACY RIGHTS; GENERALLY
17. PATIENT RIGHTS TO REQUEST RESTRICTIONS; ACCESS AND/OR AMENDMENTS TO PHI
18. PATIENT RIGHTS TO REQUEST CONFIDENTIAL COMMUNICATIONS
19. DENIALS AND GRANTS OF PATIENT REQUESTS
20. PRIVACY OFFICER
21. SECURITY STANDARDS
22. SECURITY OFFICER
23. USE AND/OR DISCLOSURE OF PHI FOR MARKETING

24. USE AND/OR DISCLOSURE OF PHI FOR JUDICIAL AND/OR ADMINISTRATIVE PROCEEDINGS
25. PROHIBITIONS AGAINST RETALIATION

AUTHORIZATION FOR USE OR DISCLOSURE OF HEALTH INFORMATION

Policy

Patient authorization is required for most uses or disclosures of protected health information that are not specifically for treatment, payment and health care operations. Use of our existing forms generally satisfies this requirement when appropriately used. For example, a patient authorization is required for:

- Use or disclosure requested by the patient.
- Marketing of services by the covered entity.
- Disclosures to an employer for employment determinations.
- Use by anyone other than the originator of psychotherapy notes.
- Research purposes not related to treatment.

Procedure

An authorization must be written in plain language and contain the following elements:

- A meaningful description of the health information to be used and disclosed.
- A description of each purpose of the requested use or disclosure.
- The name or specific identification of the person(s) or class of persons authorized to make the requested use or disclosure.
- The name or specific identification of the person(s) or class of persons to whom the use or disclosure may be made.
- An expiration date or event.
- A statement of the individual's right to revoke the authorization in writing.
- A description of how the individual may revoke the authorization.
- A statement acknowledging that the information may be subject to re-disclosure and no longer protected by this rule.
- A statement of the entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the individual's signing the authorization. A statement regarding remuneration, either direct or indirect, if the entity is to receive such remuneration for a use or disclosure for marketing purposes.
- Signature of the individual and date.
- If the authorization is signed by a personal representative, a description of the representative's authority to act for this individual.

Duties Regarding the Authorization:

- THE WESTCHESTER HEADACHE CENTER must provide the individual with a signed copy of the authorization.
- THE WESTCHESTER HEADACHE CENTER must document and maintain individual authorizations for a period of at least six years, or in accordance with state law, whichever is longer.
- THE WESTCHESTER HEADACHE CENTER'S use or disclosure of health information must be consistent with the individual's authorization.

An authorization is not valid if any of the following occur:

- The expiration date or event has passed.
- The authorization has not been filled out completely.
- The authorization contains material information that the entity knows to be false.
- The authorization is known by the covered entity to have been revoked.
- The authorization lacks one or more of the required elements previously described. Or
- The authorization is a prohibited type. For example, the authorization is invalid if it improperly conditions treatment, payment, enrollment, or eligibility for benefits on the individual's signing the authorization, or is a prohibited compound authorization (see section immediately below).

An authorization for the use or disclosure of protected health information may not be combined with other documents to create a combined authorization except in the following circumstances:

- An authorization for the use and disclosure of protected health information created for research may be combined with any other type of written permission for the same research study.
- An authorization for use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.
- A non-psychotherapy note authorization may be combined with another non-psychotherapy note authorization, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the plan, or eligibility for benefits on obtaining any of the authorizations.

THE WESTCHESTER HEADACHE CENTER may (but is not required to) use or disclose protected health information without patient authorization in a number of circumstances. These permitted uses and disclosures include:

- THE WESTCHESTER HEADACHE CENTER'S own treatment, payment, or health care operations.
- To another covered entity for treatment, payment, or health care operations.
- To another covered entity for the purpose of health care fraud and abuse detection or compliance, if each entity has had a relationship with the individual whose protected health information is disclosed.
- To another covered entity that participates in the same health care arrangement for the purpose of any health care operations activities of the organized health care arrangement.
- THE WESTCHESTER HEADACHE CENTER may release certain directory information such as name, location in the facility, and general condition. (Clergy may receive religious information.) However, the patient must be given the opportunity to object and these objections must be honored.
- To family members or close personal friends if the information is directly relevant to the person's involvement in the individual's care or payment of health care costs. However, different standards for disclosure apply based upon if the patient is present during the disclosure.
- Disaster relief purposes.
- To certain public health authorities for public health purposes.
- To a government authority if the covered entity reasonably believes the patient is a victim of abuse, neglect or domestic violence, or as otherwise required or permitted by law.
- In response to a court order.
- To law enforcement personnel for suspect, witness and victims of crimes identification and location purposes.
- To coroners and medical examiners to identify the decedent or determine the cause of death or to funeral directors to carry out their duties.
- To appropriate individuals or organization to comply with laws relating to Workers' Compensation or similar programs.

BUSINESS ASSOCIATE POLICY

Policy

It is the policy of The Westchester Headache Center to effect and maintain appropriate written Business Associate Agreements with all third party business associates that The Westchester Headache Center has such relationships with.

Our business associates shall be required to maintain the appropriate levels of protection of all our patient PHI provided to them, including but not limited to:

- Non-disclosure of PHI except as required for treatment, payment or operations of the business associates' business activities.
- As appropriate and/or required, training of the business associates' staff in privacy practices.
- Secure and private uses for Fax and computerized transactions involving our patient's PHI.
- Written Business Associate Agreements with The Westchester Headache Center to insure compliance.
- Proper maintenance and destruction of PHI.
- In the event we discover a business associate is not in compliance with either our written business associate agreement or the generally accepted standards governing PHI, they will either come into compliance, or we shall terminate their business associate relationship with The Westchester Headache Center.

Procedure

We require all business associates:

- To enter into written "business associate agreements" with The Westchester Headache Center.
- To safeguard the privacy of all PHI The Westchester Headache Center provides to them.
- To follow accepted standards for the use, access and/or disclosure of PHI provided to them by us.
- To properly dispose of PHI when the business associate's need for same is ended.
- To provide The Westchester Headache Center with assurance that the business associate is in compliance with the terms and conditions of our written business associate agreement upon our request for same, from time to time.
- Should a business associate be found to not be in compliance with the terms and conditions of our written business associate agreement and we obtain knowledge of same, to become compliant therewith.
- Should a business associate fail to be in compliance with the terms and conditions of our written business associate agreement and remain so after demand by us, we may terminate the business associate relationship as provided in the agreement.

PRACTICE COMPUTER PRIVACY AND SECURITY POLICY

Policy

It is the policy of The Westchester Headache Center to ensure proper privacy and security of our computer system and to maintain the privacy of all PHI accessed by or stored in our computer system.

It is the policy of The Westchester Headache Center to require separate and unique passwords for all personnel authorized to use our computer(s) to access, use or disclose PHI, and to not allow the sharing of passwords between staff, or staff and others.

It is the policy of The Westchester Headache Center to utilize screen savers that come on promptly when a computer monitor or terminal is not used for a period of time, to prevent the observation of PHI on our computer monitors by staff or others without a need to know that information, or who may not be authorized to use or access such information.

It is the policy of The Westchester Headache Center to place and/or position the monitors and terminals of our computers so as to prevent them from being readily observed by staff or others without a need to know that information, or who may not be authorized to use or access such information.

Procedure

To maintain the privacy of our computerized PHI, The Westchester Headache Center does and will:

- Assign to each staff member and other person authorized to use our computers and/or terminals a unique and individual password.
- Provide appropriate discipline or sanctions to staff or others found to be in violation of our password and/or computer privacy policies.
- Position our monitors so as to prevent observation by persons who are not authorized to have access to the PHI contained in our computer system.
- Require non-staff members who may have access to our computer system for maintenance or repair to enter into written agreements to ensure the privacy of PHI on our computers to which their position may allow them access.
- Utilize screen savers or other procedures to prevent the observation of PHI on our computer screens and monitors by those without authorization or “need to know” that information.

DATA CLASSIFICATION POLICY

Policy

The Westchester Headache Center's data classification system has been designed to support the need to know that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, THE WESTCHESTER HEADACHE CENTER unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage. The purpose of this data classification policy is to provide a system for protecting information that is critical to THE WESTCHESTER HEADACHE CENTER. All workers who may come into contact with confidential information are expected to familiarize themselves with this data classification policy and to consistently use it.

Procedure

Applicable Information: This data classification policy is applicable to all information in The Westchester Headache Center's possession. For example, medical records on patients, confidential information from suppliers, business partners and others must be protected with this data classification policy. No distinctions between the word data, information, knowledge, and wisdom are made for purposes of this policy.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, workers will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

Classification Labels

Public: This classification applies to information that is available to the general public and intended for distribution outside The Westchester Headache Center's office. This information may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

For Internal Use Only: This classification applies to all other information that does not clearly fit into the other classifications. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact The Westchester Headache Center's business, patients, employees, or business partners. Examples include the company telephone directory, new employee training materials, and internal policy manuals.

Confidential: This classification applies to information that is intended for use within the The Westchester Headache Center's practice. Unauthorized disclosure could adversely impact The Westchester Headache Center's business, patients, employees and business partners. Information that some people would consider private is included in this classification. Examples include medical information (except that which is restricted confidential), patient medical charts, appointment schedules, patient account records, department financial data, purchasing information, vendor contracts.

Restricted Confidential: This classification applies to the most sensitive medical and business information that are intended strictly for use within The Westchester Headache Center's business. Its unauthorized disclosure could seriously and adversely impact The Westchester Headache Center's business, patients, employees and business partners. For example, statutorily protected medical information such as,

mental health treatment, HIV testing, sexually transmitted diseases, abortion, and alcoholism or substance abuse treatment data.

DESTRUCTION AND DISPOSAL OF PROTECTED HEALTH INFORMATION MEDIA

Policy

It is the policy of THE WESTCHESTER HEADACHE CENTER to ensure the privacy and security of protected patient health information in the maintenance, retention, and eventual destruction/disposal of such media. Destruction/disposal of patient health information shall be carried out in accordance with federal and state law and as may be specified from time to time in our retention policy. The schedule for destruction/disposal shall be suspended for records of active patients or those records which may be involved in any open investigation, audit, or litigation.

Procedures

1. All destruction/disposal of patient health information media will be done in accordance with federal and state law and pursuant to the organization's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
2. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
3. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of patient information is complete.
4. A contract between the organization and a business associate must provide that, upon termination of the contract, the business associate will return or destroy/dispose of all patient health information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal. These requirements also apply to a health plan that discloses patient health information to the plan sponsor.
5. A record of all patient health information media destruction/disposal should be made and retained permanently by the organization. Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:
 - Date of destruction/disposal.
 - Method of destruction/disposal.
 - Description of the destroyed/disposed record series or medium.
 - Inclusive dates covered.
 - A statement that the patient information records were destroyed/disposed of in the normal course of business.
 - The signatures of the individuals supervising and witnessing the destruction/disposal.
6. If destruction/disposal services are contracted, the contract must provide that the organization's business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (*outlined in the Business Associate Agreement*) and include the following elements:

- Specify the method of destruction/disposal.
- Specify the time that will elapse between acquisition and destruction/disposal of data/media.
- Establish safeguards against breaches in confidentiality.
- Indemnify the organization from loss due to unauthorized disclosure.
- Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.
- Provide proof of destruction/disposal.

7. Patient information media should be destroyed/disposed of using a method that ensures the patient information cannot be recovered or reconstructed. Appropriate methods for destroying/disposing of media are outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destroying/disposing of audiotapes include recycling (tape over) or pulverizing.
Computerized Data/ Hard Disk Drives	Methods of destruction/disposal should destroy data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. Total data destruction does not occur until the back-up tapes have been overwritten.
Computer Data/ Magnetic Media	Methods may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the back-up tapes have been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.
Computer Diskettes	Methods for destroying/disposing of diskettes include reformatting, pulverizing, or magnetic degaussing.
Laser Disks	Disks used in “write once-read many” (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/ Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate.
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing.

Medium	Recommendation
Videotapes	Methods for destroying/disposing of videotapes include recycling (tape over) or pulverizing.

8. The methods of destruction/disposal should be reassessed annually, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR WORKERS' COMPENSATION AND RELATED PURPOSES

Policy

It is the policy of THE WESTCHESTER HEADACHE CENTER to disclose protected health information to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. However, the health information disclosed must be limited to the minimum amount necessary to carry out the purpose of the disclosure.

An employee filing a claim for workers' compensation due to an on-the-job injury consents to certain conditions. One of those conditions is, at the employer's request, they will submit to an examination to determine the validity of their claim. This information is then available, with certain restrictions, to the employee, employer, a State Workers' Compensation Tribunal, or the appropriate authorized representative of any of these to assist in resolution of our patient's claim.

Procedures

1. Copies of medical records or verbal communications, reasonably related to a work injury, should be released within a reasonable time, after written request, to the employee, employer, workers compensation insurance carrier for the employer, State Workers' Compensation Tribunal or its authorized representatives.
2. Requests for copies of medical records which extend beyond the scope of the work-related injury need to be accompanied by a written authorization from the patient/employee.
3. We will furnish legible duplicates of written material requested. Certified copies are furnished upon request.

E-MAIL POLICIES

Policy

It is the policy of The Westchester Headache Center to ensure proper privacy and security of our email when PHI is to be sent or received using email.

Our policy is to safeguard the privacy and integrity of email involving our patient's PHI by, whenever possible, utilizing encrypted email and/or assuring the privacy of email sent or received by us in accord with our "computer privacy" policies as set forth in this manual.

Our policy is to safeguard the privacy of PHI either sent or received by us in the form of email communications.

Procedure

To maintain the privacy and security of our email communications involving PHI, The Westchester Headache Center does and will:

- Assign to each staff member and other person authorized to use our computers to send and/or receive email containing PHI a unique and individual password.
- Whenever possible, to utilize email with encryption to prevent the interception or unauthorized observation or reception of our email communications containing PHI.
- Provide appropriate discipline or sanctions to staff or others found to be in violation of our email policies.
- To require business associates who send or receive either to or from us email containing PHI to maintain protection of the privacy of such email to the same standards as our policies.

EMERGENCY, CATASTROPHY AND RELATED POLICIES

Policy

It is the policy of The Westchester Headache Center to ensure that we have in place appropriate emergency procedures and disaster recovery plans for the proper protection of PHI and to ensure that both PHI and our TPO can continue without compromise of privacy or security in the event of an emergency or disaster.

Our policy is to provide for appropriate backup and restoration of PHI and other data in our computer system and to provide for safe and secure storage of information including but not limited to PHI kept by us in non-computerized format.

It is our policy to provide for regular back up of our computerized information, and to provide for restoration of PHI and other computerized data should an emergency or disaster occur, as well as provisions for back ups and similar procedures for our non-computerized data.

Procedure

To maintain the integrity and availability of our PHI and other data required for the continued orderly operations of The Westchester Headache Center, our procedures are to:

- Arrange for regular back-ups of our computerized data, including but not limited to both PHI and other data required for the orderly conduct of The Westchester Headache Center.
- As may be required, to provide as required uninterruptible power supplies as may be necessary for the protection of our computer systems and computerized PHI.
- As regards non-computerized data, to provide for appropriate back ups of same to allow orderly continuation of business in the event of a disaster or emergency which effects our non-computerized data.
- To provide for efficient and orderly restoration of data from our back-ups following a disaster or emergency.

EMPLOYEE PRIVACY TRAINING

Policy

It is the policy of The Westchester Headache Center to provide employee and/or staff training in the proper procedures for compliance with the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) as may be required; and also to provide such privacy training as may be required for persons other than our regular staff for whom such training may also be required. It is also the policy of The Westchester Headache Center to document all privacy training provided.

Procedure

To comply with required mandates, The Westchester Headache Center will provide privacy training for all current staff members, and will provide appropriate privacy training for new and future personnel.

- Appropriate privacy awareness training will be provided for all current staff.
- Appropriate privacy awareness training will be provided for all future personnel.
- Documentation of privacy awareness training will be maintained for all personnel.

EMPLOYEE TRAINING ON HIPAA PRIVACY RULES AND POLICY

Policy

The Westchester Headache Center's HIPAA privacy training is the foundation upon which The Westchester Headache Center's compliance rests. We know HIPAA requires us to comply with detailed regulations designed to protect "Protected Health Information" (Hereafter "PHI") as that information is used in the health care profession. In addition, The Westchester Headache Center acknowledges that the privacy rule required that "a covered entity must train all members of its work force on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the work force to carry out their function within the covered entity."

Procedure-The Westchester Headache Center will train our entire work force

We acknowledge that our first step in meeting the HIPAA regulations is that we understand exactly what is expected of The Westchester Headache Center in terms of work force training. According to section 164.530 (b), each entity must provide training to its work force no later than the compliance date for the covered entity.

While the privacy requirement does not specify how long or how involved the training must be, the requirement does explicitly state that the training must cover policies and procedures with respect to protected health information, therefore we will train our workforce on policies and procedures as is needed and appropriate for our staff members and other personnel involved to carry out their functions within The Westchester Headache Center.

The Westchester Headache Center acknowledges that documentation is required to establish appropriate training of our personnel; therefore our procedure is to appropriately document training of staff. It is our policy to train our staff including, but not limited to the following:

- HIPAA objectives

- HIPAA information source
- Definitions of HIPAA terms
- What the HIPAA privacy regulations cover
- Uses and disclosures of protected health information (PHI)
- The nexus between public responsibility and the HIPAA regulations
- Individual and patient rights under HIPAA
- Accountability of The Westchester Headache Center, staff and business associates under HIPAA
- Administrative safeguards of PHI
- The physical safeguards of PHI
- Technical safeguards of PHI
- How HIPAA relates to state law
- How The Westchester Headache Center will become and remain HIPAA compliant
- Complaint procedures

EMPLOYEE, BUSINESS ASSOCIATE AND OTHERS; PROCEDURES ON VIOLATIONS OF OUR POLICY

Policy

It is the policy of The Westchester Headache Center to require compliance with all provisions of The Health Insurance Portability and Accountability Act (HIPAA) as required.

In accordance therewith, we have adopted discipline and sanction provisions for both staff and business associates for violations thereof.

Staff members who violate provisions of The Health Insurance Portability and Accountability Act (HIPAA) and especially the privacy provisions thereof shall be disciplined; and the level and/or severity of such discipline may depend upon whether any such violations are willful and intentional or of a negligent nature.

Staff discipline for violations may consist of verbal warnings, written warnings or other discipline up to termination depending on the severity of the violation.

As regards business associates, In the event we discover a business associate is not in compliance with either our written business associate agreement or the generally accepted standards governing PHI, they will either come into compliance, or we shall terminate their business associate relationship with The Westchester Headache Center.

Procedure

The Westchester Headache Center will levy appropriate sanctions and/or discipline for staff members and business associates found to be in violation of The Health Insurance Portability and Accountability Act (HIPAA).

As regards staff members, such discipline may include but are not limited to any combination of:

- Verbal warnings
- Written warnings
- Termination of employment.

As regards violations by business associates, sanctions may include but are not limited to any combination of:

- Verbal demands to come into compliance;
- Written demands to come into compliance;
- Termination of the business associate relationship with the non-compliant business associate.

FAX POLICIES

Policy

It is the policy of The Westchester Headache Center to maintain and protect the privacy and security of our faxes containing PHI, both sent and received by The Westchester Headache Center.

As regards faxes containing PHI we send, it is our policy to first notify the recipient that a fax transmission containing PHI is to be sent and the approximate time at which that transmission will be made.

As regards faxes containing PHI we are aware we will receive, it is our policy to request the transmitter first notify us that a fax transmission containing PHI is to be sent to us, and to request they inform us of the approximate time at which that transmission will be made to us.

It is also our policy to use an appropriate Fax Transmittal Cover Sheet to further protect the privacy of fax transmissions we send containing PHI.

It is our policy to further protect the privacy of fax transmissions by placing our fax machine in an area where transmissions received cannot be readily seen by persons without any need to know the PHI contained therein, and to be sure that fax transmissions containing PHI which have been received by us are not left unattended on the fax machine.

Procedure

The Westchester Headache Center will protect and maintain the privacy of fax transmissions containing PHI both sent by received by us.

As regards fax transmissions containing PHI we send:

- We will phone to recipient and advise a fax containing PHI is to be sent, and the approximate time such transmission will be made.
- We will request the recipient to not leave the fax where it can be seen by persons with no need to know the information to be sent by fax.
- We will use a confidential cover sheet to further protect the information to be faxed.

As regards fax transmissions containing PHI we are aware are to be sent to us:

- We will ask the transmitter when we can expect to receive their fax transmission;
- We will not leave faxes containing PHI on our fax machine for any protracted length of time;
- We will place our fax machine in an area where faxes received by us cannot be readily seen by persons not authorized to access or use PHI.

INTERNET, EXTRANET AND LAN/WAN POLICIES

Policy

It is the policy of The Westchester Headache Center to maintain and protect the privacy and security of both our computer system and PHI stored therein, in connection with The Westchester Headache Center uses of the Internet, extranet uses, and in the use of local area networks and wide area network applications.

In connection with Internet, extranet uses, and in the use of local area networks and wide area network applications, our computer privacy policies as set forth shall at all times be maintained.

In addition, when such shall be deemed appropriate and proper, the use of firewalls shall be implemented, and as regards the transmission or anticipated receipt of PHI, encryption shall be utilized as deemed appropriate for the security and privacy of PHI.

The Westchester Headache Center recognizes the potential dangers posed by virus threats and interception or other activities by unauthorized persons including “hackers” and other non-authorized persons attempting to gain access to our computer system.

The Westchester Headache Center will, whenever appropriate, utilize firewalls to prevent outside access to our computerized data, and as is practical utilize anti-virus software and procedures to both prevent and detect the attempted or actual introduction of a virus or other malicious code or software into our computer system, and for the identification and removal thereof.

Procedure

The Westchester Headache Center will protect and maintain the privacy and security of our computer system in connection with uses of the Internet, extranet uses, and in the use of local area networks and wide area network applications:

- Our computer privacy policies shall also extend to Internet, extranet and local/wide area network uses and applications of our computer systems.
- Firewall hardware and/or software shall be used as appropriate to prevent unauthorized access to our computerized data.
- Anti-virus software shall as appropriate be used to prevent or remove malicious code or software and to identify and remove any introduced to our computer system.

Appropriate back up and restoration procedures as set forth in our emergency and disaster policies shall also apply to use of Internet, extranet and local/wide area network uses and applications of our computer systems.

MINIMUM NECESSARY POLICIES AND PROCEDURES

Policy

THE WESTCHESTER HEADACHE CENTER will make every reasonable effort to limit use, disclosure of, and requests for Protected Health Information (PHI) to the minimum necessary to accomplish the intended purpose.

Access to PHI is limited to the persons and/or employee classifications listed below, and then limited to the identified PHI only, consistent with their job responsibilities. Access to an entire medical record will not be allowed except, when provided for in these policies and procedures and the justification for use of the entire medical record is specifically identified and documented.

We are not required to limit to the minimum necessary our disclosures of PHI to our patient who is the subject of the PHI. Disclosures authorized by our patient are exempt from the minimum necessary requirements.

Authorizations received directly from third parties, such as life, disability, or casualty insurers, which direct us to release PHI to them, are not subject to the minimum necessary standards.

Procedures

The following listing of THE WESTCHESTER HEADACHE CENTER'S employees page identifies (A) THE WESTCHESTER HEADACHE CENTER'S employees (or other designated persons) who need access to PHI to carry out their duties, (B) the categories and/or /types of PHI to which such persons need access, and (C) the conditions if any, as appropriate, that would apply to such designated person(s) access to PHI:

<u>EMPLOYEE TITLE/POSITION</u>	<u>PHI TO BE ACCESSED</u>	<u>CONDITIONS OF ACCESS</u>
---------------------------------------	----------------------------------	------------------------------------

PATIENT NOTICE OF PRIVACY PRACTICES AND PATIENT ACKNOWLEDGMENT OF RECEIPT OF SAME

Policy

THE WESTCHESTER HEADACHE CENTER is required to provide all patients with a “Notice of Privacy Practices” at or immediately following their first patient visit to The Westchester Headache Center, and to obtain their acknowledgment of receipt of this “Notice of Privacy Practices”.

Use of our “Notice of Privacy Practices” form on the patient’s first visit will generally accomplish both these requirements.

Procedures

Upon a patient’s first visit to THE WESTCHESTER HEADACHE CENTER, the patient will be provided with our then-current “NOTICE OF PROVIDER PRIVACY PRACTICES” form, and the patient’s signature will be obtained on the copy of that form which will be placed in the patient’s chart. The “NOTICE OF PROVIDER PRIVACY PRACTICES” form will be in substantially the following form, or provide substantially the following information, or as may otherwise be provided in our then-current Privacy Forms Manual:

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT
YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET
ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

THE WESTCHESTER HEADACHE CENTER must maintain the privacy of your personal health information and give you this notice that describes our legal duties and privacy practices concerning your personal health information. In general, when we release your health information, we must release only the information we need to achieve the purpose of the use or disclosure. However, all of your personal health information that you designate will be available for release if you sign an authorization form, if you request the information for yourself, to a provider regarding your treatment, or due to a legal requirement. We must follow the privacy practices described in this notice.

However, we reserve the right to change the privacy practices described in this notice, in accordance with the law. Changes to our privacy practices would apply to all health information we maintain. If we change our privacy practices, you will receive a revised copy.

Without your written authorization, we can use your health information for the following purposes:

1. Treatment: For example, a doctor may use the information in your medical record to determine which treatment option, such as a drug or surgery, best addresses your health needs. The treatment selected will be documented in your medical record, so that other health care professionals can make informed decisions about your care.

2. Payment: In order for an insurance company to pay for your treatment, we must submit a bill that identifies you, your diagnosis, and the treatment provided to you. As a result, we will pass such health information onto an insurer in order to help receive payment for your medical bills.

3. Health Care Operations: We may need your diagnosis, treatment, and outcome information in order to improve the quality or cost of care we deliver. These quality and cost improvement activities may include evaluating the performance of your doctors, nurses and other health care professionals, or examining the effectiveness of the treatment provided to you when compared to patients in similar situations.

In addition, we may want to use your health information for appointment reminders. For example, we may look at your medical record to determine the date and time of your next appointment with us, and then send you a reminder letter to help you remember the appointment. Or, we may look at your medical information and decide that another treatment or a new service we offer may interest you. For example, we may contact a cancer patient to notify them that we have a new cancer research facility that offers new life-saving treatments.

Furthermore, we may want to use information found in your medical record, such as your name, address, phone number and treatment dates, to contact you for our fund-raising purposes. For example, in order to provide more charity care or otherwise improve the health of your community, we may want to raise additional money and therefore may contact you for a donation.

4. As required or permitted by law: Sometimes we must report some of your health information to legal authorities, such as law enforcement officials, court officials, or government agencies. For example, we may have to report abuse, neglect, domestic violence or certain physical injuries, or to respond to a court order.

5. For public health activities: We may be required to report your health information to authorities to help prevent or control disease, injury, or disability. This may include using your medical record to report certain diseases, injuries, birth or death information, information of concern to the Food and Drug Administration, or information related to child abuse or neglect. We may also have to report to your employer certain work-related illnesses and injuries so that your workplace can be monitored for safety.

6. For health oversight activities: We may disclose your health information to authorities so they can monitor, investigate, inspect, discipline or license those who work in the health care system or for government benefit programs.

7. For activities related to death: We may disclose your health information to coroners, medical examiners and funeral directors so they can carry out their duties related to your death, such as identifying the body, determining cause of death, or in the case of funeral directors, to carry out funeral preparation activities.

8. For organ, eye or tissue donation: We may disclose your health information to people involved with obtaining, storing or transplanting organs, eyes or tissue of cadavers for donation purposes.

9. For research: Under certain circumstances, and only after a special approval process, we may use and disclose your health information to help conduct research. Such research might try to find out whether a certain treatment is effective in curing an illness.

10. To avoid a serious threat to health or safety: As required by law and standards of ethical conduct, we may release your health information to the proper authorities if we believe, in good faith, that such release is necessary to prevent or minimize a serious and approaching threat to your or the public's health or safety.

11. For military, national security, or incarceration/law enforcement custody: If you are involved with the military, national security or intelligence activities, or you are in the custody of law enforcement officials or an inmate in a correctional institution, we may release your health information to the proper authorities so they may carry out their duties under the law.

12. For workers' compensation: We may disclose your health information to the appropriate persons in order to comply with the laws related to workers' compensation or other similar programs. These programs may provide benefits for work-related injuries or illness.

13. For The Westchester Headache Center's directory: Unless you object, we may use your health information, such as your name, location in our facility, your general health condition (e.g., "stable," or "unstable"), and your religious affiliation for our directory. It is our duty to give you enough information so you can decide whether or not to object to release of this information for our directory. The information about you contained in our directory will be released to people who ask for you by name. However, the information about your religious affiliation will only be disclosed to clergy. We may allow you to agree or disagree orally regarding the use of your health information for directory purposes.

14. To those involved with your care or payment of your care: If people such as family members, relatives, or close personal friends are helping care for you or helping you pay your medical bills, we may release important health information about you to those people. The information released to these people may include your location within our facility, your general condition, or death. You have the right to object to such disclosure, unless you are unable to function or there is an emergency. In addition, we may release your health information to organizations authorized to handle disaster relief efforts so those who care for you can receive information about your location or health status. We may allow you to

agree or disagree orally to such release, unless there is an emergency. It is our duty to give you enough information so you can decide whether or not to object to release of your health information to others involved with your care.

NOTE: Except for the situations listed above, we must obtain your specific written authorization for any other release of your health information.

If you sign an authorization form, you may withdraw your authorization at any time, as long as your withdrawal is in writing. If you wish to withdraw your authorization, please submit your written withdrawal to OUR PRIVACY OFFICER.

Your Health Information Rights

You have several rights with regard to your health information. If you wish to exercise any of the following rights, please contact OUR PRIVACY OFFICER. Specifically, you have the right to:

1. Inspect and copy your health information: With a few exceptions, you have the right to inspect and obtain a copy of your health information. However, this right does not apply to psychotherapy notes or information gathered for judicial proceedings, for example. In addition, we may charge you a reasonable fee if you want a copy of your health information.

2. Request to correct your health information: If you believe your health information is incorrect, you may ask us to correct the information. You may be asked to make such requests in writing and to give a reason as to why your health information should be changed. However, if we did not create the health information that you believe is incorrect, or if we disagree with you and believe your health information is correct, we may deny your request.

3. Request restrictions on certain uses and disclosures: You have the right ask for restrictions on how your health information is used or to whom your information is disclosed, even if the restriction affects your treatment or our payment or health care operation activities. Or, you may want to limit the health information provided to family or friends involved in your care or payment of medical bills. You may also want to limit the health information provided to authorities involved with disaster relief efforts. However, we are not required to agree in all circumstances to your requested restriction.

If you receive certain medical devices (for example, life-supporting devices used outside our facility), you may refuse to release your name, address, telephone number, social security number or other identifying information for purpose of tracking the medical device.

4. As applicable, receive confidential communication of health information: You have the right to ask that we communicate your health information to you in different ways or places. For example, you may wish to receive information about your health status in a special, private room or through a written letter sent to a private address. We must accommodate reasonable requests.

5. Receive a record of disclosures of your health information: In some limited instances, you have the right to ask for a list of the disclosures of your health information we have made during the previous six years, but the request cannot include dates before April 14, 2003. This list must include the date of each disclosure, who received the disclosed health information, a brief description of the health information disclosed, and why the disclosure was made. We must comply with your request for a list within 60 days, unless you agree to a 30-day extension, and we may not charge you for the list, unless you request such list more than once per year. In addition, we will not include in the list disclosures made to you, or for purposes of treatment, payment, health care operations, our directory, national security, law enforcement/corrections, and certain health oversight activities.

6. Obtain a paper copy of this notice: Upon your request, you may at any time receive a paper copy of this notice, even if you earlier agreed to receive this notice electronically. **[IF PROVIDER MAINTAINS A WEB SITE THAT PROVIDES INFORMATION ABOUT PROVIDER'S CUSTOMER SERVICES OR BENEFITS, PROVIDER MUST POST ITS NOTICE ON THE WEB SITE AND MAKE NOTICE AVAILABLE ELECTRONICALLY THROUGH THE WEB SITE. AS A RESULT, PROVIDER MAY WANT TO INDICATE HERE THE AVAILABILITY OF THE PRIVACY NOTICE ON ITS WEB SITE.]**

7. Complain: If you believe your privacy rights have been violated, you may file a complaint with us and with the federal Department of Health and Human Services. We will not retaliate against you for filing such a complaint. To file a complaint with either entity, please contact OUR PRIVACY OFFICER, who will provide you with the necessary assistance and paperwork.

Again, if you have any questions or concerns regarding your privacy rights or the information in this notice, please contact OUR PRIVACY OFFICER at our office.

This Notice of Medical Information Privacy is Effective_____.

PATIENT COMPLAINT PROCEDURES CONCERNING PRIVACY

Policy

THE WESTCHESTER HEADACHE CENTER shall provide a process for the patient to file a complaint if the patient feels his or her privacy rights have been violated. The patient may also file a complaint concerning THE WESTCHESTER HEADACHE CENTER's privacy policies and procedures, even without alleging a violation of rights.

THE WESTCHESTER HEADACHE CENTER has designated our Privacy Officer as the contact person responsible for receiving complaints and has established a process for receiving, investigating and responding to patient complaints. The patient complaint process is as described in THE WESTCHESTER HEADACHE CENTER's Patient Privacy Rights Notice. THE WESTCHESTER HEADACHE CENTER also recognizes the patient's right to file a complaint with the federal Department of Health and Human Services. THE WESTCHESTER HEADACHE CENTER shall cooperate with a federal investigation of the patient's complaint to the extent provided by law.

THE WESTCHESTER HEADACHE CENTER does not allow any intimidation of or retaliation against patients, families, friends, or other participants in the complaint process, and any such retaliation is prohibited by our policies. Employees who violate this policy are subject to disciplinary action, up to and including termination.

If the patient's rights have been violated, employees who violated those rights are subject to disciplinary action, up to and including termination. THE WESTCHESTER HEADACHE CENTER shall mitigate, to the extent feasible, any known harmful effects of the violation.

Procedures

1. Filing a Complaint

- A patient may call, write, or present in person to the Privacy Officer or designated person the alleged privacy violation or complaint.
- The Privacy Officer or designated person will summarize the complaint on the Patient Complaint Report Form.

2. Investigation of Complaint

- The Privacy Officer or designated person will facilitate the investigation of the complaint.

3. Response to Complaint

- A written response will be provided to the patient within 30 days from the date the complaint was filed.
- A written summary of the complaint and action taken will be filed with the Privacy Officer.

4. Translators, interpreters, and others who may help meet any special communication needs of the patient may be provided during the complaint process.

5. Patients are permitted to have a representative of their choice to represent their interests during the complaint process.
6. Occurrences representing potential liability claims against The Westchester Headache Center will be processed as any other claim against The Westchester Headache Center.
7. Patients who request an outside agency to review their complaint may contact the Secretary of the Federal Department of Health and Human Services at 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.
8. All complaints received must be documented.
9. All complaint dispositions must be documented.

The documentation must be retained for six years.

PATIENT PRIVACY RIGHTS - GENERAL

Policy

It is the policy of THE WESTCHESTER HEADACHE CENTER to implement the following policies and procedures that will ensure patient privacy rights in accordance with the Privacy Regulations promulgated under The Health Insurance Portability and Accountability Act (HIPAA):

- 1. Availability of THE WESTCHESTER HEADACHE CENTER's Privacy Notice.** The patient has the right to receive our privacy notice in a timely manner. Upon request, the patient may at any time receive a paper copy of our privacy notice, even if he or she earlier agreed to receive the notice electronically. We must also post our privacy notice in a prominent location.
- 2. Requesting restrictions on certain uses and disclosures.** The patient has the right to object to, and ask for restrictions on, how his or her health information is used or to whom the information is disclosed, even if the restriction affects the patient's treatment or our payment or health care operation activities. The patient may want to limit the health information that is included in patient directories, or provided to family or friends involved in his or her care or payment of medical bills. The patient may also want to limit the health information provided to authorities involved with disaster relief efforts. However, we are not required to agree in all circumstances to the patient's requested restriction.
- 3. Receiving confidential communication of health information.** The patient has the right to ask that we communicate his or her health information to them in different ways or places. For example, the patient may wish to receive information about their health status in a special, private room or through a written letter sent to a private address. We must accommodate requests that are reasonable in terms of administrative burden. We may not require the patient to give a reason for the request.
- 4. Access, inspection and copying of health information.** With a few exceptions, patients have the right to inspect and obtain a copy of their health information. However, this right does not apply to psychotherapy notes or information gathered for judicial proceedings, for example. In addition, we may charge the patient a reasonable fee for copies of their health information.
- 5. Requesting amendments or corrections to health information.** If the patient believes their health information is incomplete or incorrect, they may ask us to correct the information. The patient may be asked to make such requests in writing and to give a reason as to why his or her health information should be changed. However, if we did not create the health information that the patient believes is incorrect, or if we disagree with the patient and believe his or her health information is correct, we may deny the request. We must act on the request within 60 days after we receive it, unless we inform the patient of our need for a one-time 30-day extension.
- 6. Receiving an accounting of disclosures of health information.** In some limited instances, the patient has the right to ask for a list of the disclosures of their health information that we have made during the previous six years, but the request cannot include dates before April 14, 2003. This list must include the date of each disclosure, who received the disclosed health information, a brief description of the health information disclosed, and why the disclosure was made. We must furnish the patient with a list within 60 days of the request, unless we inform the patient of our need for a one-time 30-day extension, and we may not charge the patient for the list, unless the patient requests such list more than once in a 12 month period. In addition, we will not include in the list disclosures made to the patient, or for purposes of treatment, payment, health care operations, our directory, national security, law enforcement/corrections, and certain health oversight activities.

- 7. Complaints.** Patients have the right to file a complaint with us and with the federal Department of Health and Human Services if they believe their privacy rights have been violated. We will not retaliate against the patient for filing such a complaint. To file a complaint with either entity, the patient should contact POX, the Privacy Officer, who will provide the patient with the necessary assistance and paperwork.

Procedures

- 1.** Should the law regarding patient privacy rights under The Health Insurance Portability and Accountability Act (HIPAA) change, we will update our organization's policies and procedures to reflect such changes if any, if applicable to The Westchester Headache Center.
- 2.** All new staff of THE WESTCHESTER HEADACHE CENTER shall receive a copy of this document at employee orientation and be directed at orientation and/or training as to how to access more detailed privacy policy and procedure documents.
- 3.** All current staff of THE WESTCHESTER HEADACHE CENTER shall receive a copy of this document as part of our Health Insurance Portability and Accountability Act compliance training session, and upon an employee's request.

PATIENT RIGHT TO REQUEST THE WESTCHESTER HEADACHE CENTER TO AMEND PROTECTED HEALTH INFORMATION

Policy

It is the policy of THE WESTCHESTER HEADACHE CENTER to honor a patient's right to request an amendment or correction to their protected health information if they feel that the information is incomplete or inaccurate. The patient has the right to request an amendment of their protected health information for as long as that information is maintained in the designated record set.

Procedures

Patient requests for amendment of protected health information shall be made in writing to OUR PRIVACY OFFICER and clearly identify the information to be amended, as well as the reasons for the amendment. These requirements are as set forth in Our Policies and Procedures and as detailed in our Notice of Privacy Practices.

1. Requests may be denied if the material requested to be amended:
 - Was not created by The Westchester Headache Center, unless the originator is no longer available to act on the request
 - Is not part of the individual's health record
 - Is not accessible to the individual because federal and state law do not permit it
 - Is accurate and complete
2. THE WESTCHESTER HEADACHE CENTER must act on the individual's request for amendment no later than 60 days after receipt of the amendment. The Westchester Headache Center may have a one-time extension of 30 days for processing the amendment if the individual is given a written statement of the reason for the delay, and the date by which the amendment request will be processed.

If An Amendment Request is Granted

If the request to amend is **granted**, after review and approval by the individual responsible for the entry to be amended, THE WESTCHESTER HEADACHE CENTER must:

1. Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.
2. Inform the individual that the amendment is accepted.
3. Obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with whom the amendment needs to be shared.

4. Within a reasonable time period, make reasonable efforts to provide the amendment to persons identified by the individual, and persons including our business associates, that The Westchester Headache Center knows have the protected health information that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the patient or other individual concerned.

If An Amendment Request is Denied

If the request is **denied**, The Westchester Headache Center must provide the individual with timely, written denial in plain language that contains:

- The basis for the denial.
 - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.
 - A statement that if the individual does not submit a statement of disagreement, the individual may request that THE WESTCHESTER HEADACHE CENTER provide the individual's request for amendment and the denial with any future disclosures of the protected health information that was the subject of the request.
 - A description of how the individual may complain to The Westchester Headache Center or the Secretary of Health and Human Services.
 - The name or title, and the telephone number of our Privacy Officer who is our designated contact person who handles complaints for The Westchester Headache Center.
1. THE WESTCHESTER HEADACHE CENTER must permit the individual to submit to us (or other involved covered entity) a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such agreement. THE WESTCHESTER HEADACHE CENTER may reasonably limit the length of such a statement of disagreement.
 2. THE WESTCHESTER HEADACHE CENTER may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, The Westchester Headache Center must provide a copy to the individual who submitted the statement of disagreement.
 3. THE WESTCHESTER HEADACHE CENTER must, as appropriate, identify the record of protected health information that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, our denial of the request, the individual's statement of disagreement, if any, and our rebuttal, if any.
 4. If the statement of disagreement has been submitted by the individual, THE WESTCHESTER HEADACHE CENTER must include the material appended or an accurate summary of such information with any subsequent disclosure of the protected health information to which the disagreement relates.

5. If the individual has not submitted a written statement of disagreement, THE WESTCHESTER HEADACHE CENTER must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of protected health information only if the individual has requested such action.
6. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, THE WESTCHESTER HEADACHE CENTER must separately transmit the material required.
7. When THE WESTCHESTER HEADACHE CENTER is informed by another covered entity of an amendment to an individual's protected health information, we must amend the protected health information in written or electronic form.
8. THE WESTCHESTER HEADACHE CENTER must document the titles of the persons or offices responsible for receiving and processing requests for amendments. In The Westchester Headache Center, that person is our Privacy Officer.

Additional Considerations of Amendments from Other Covered Entities

When THE WESTCHESTER HEADACHE CENTER receives notification from another health care provider or health plan that a patient's protected health information has been amended, THE WESTCHESTER HEADACHE CENTER:

1. Must insure that the amendment is appended to the patient's health record.
2. Will inform its business associates that may use or rely on the patient's protected health information of the amendment (as agreed to in the business associate contract) so that they may make the necessary revisions based on the amendment.

PATIENT RIGHT TO REQUEST RESTRICTION ON PHI COMMUNICATIONS

Policy

Our Patients (as used hereafter, “patient” includes our patients and their authorized representatives or other legally qualified and authorized individuals) have the right to request restrictions on how and where their Protected Health Information (PHI) is communicated. To comply with the HIPAA Privacy Rule, THE WESTCHESTER HEADACHE CENTER must permit patients/individuals to request to receive communications of Protected Health Information by alternative means or at alternative locations.

Procedures

1. THE WESTCHESTER HEADACHE CENTER may require that patient requests to receive communications of PHI by alternative means or at alternative locations be made in writing. These writing requirements are detailed in our Notice of Privacy Practices.
2. Patients may request to receive communications of PHI by alternative means or at alternative locations at the time of their initial visit or admission, at subsequent visits, or at any time during the course of their care.
3. Patient requests may be made to any member of THE WESTCHESTER HEADACHE CENTER staff.
4. When patients make such a request, either formally or informally, the staff member receiving the request should document it in writing.
5. THE WESTCHESTER HEADACHE CENTER must accommodate patient requests that are reasonable, and we must accommodate patient requests that are reasonable, if the patient states that the disclosure of PHI could endanger him or her.
6. THE WESTCHESTER HEADACHE CENTER determines whether a request is “reasonable” based solely on the administrative difficulty of accommodating the request. OUR Privacy Officer will determine whether such requests are “reasonable.”
7. THE WESTCHESTER HEADACHE CENTER may not require that patients provide any particular reason for their request.
8. THE WESTCHESTER HEADACHE CENTER may require that such requests contain a statement that disclosure of PHI could endanger the patient. (These statements may be oral or written. Our staff may ask patients if disclosure of PHI could put them in danger, or patients could fill out a request form that contains a checkbox question about possible endangerment due to PHI disclosure.)

- 9.** THE WESTCHESTER HEADACHE CENTER may not deny requests based on our perception of whether patients have a good reason for making the request. A patient's reason for making a request cannot be used to determine whether the request is reasonable.
- 10.** THE WESTCHESTER HEADACHE CENTER may deny patient's requests if:

 - a. The patient does not specify an alternative address or other method of contact
 - b. The patient does not provide information as to how payment, if applicable, will be handled
- 11.** If THE WESTCHESTER HEADACHE CENTER grants a patient's request, the decision must be documented by maintaining a written or electronic record of the action taken, and If THE WESTCHESTER HEADACHE CENTER grants a patient's request, we must provide appropriate staff with the communication requirements and require our staff to adhere to them.

THE WESTCHESTER HEADACHE CENTER'S PRIVACY OFFICER

Policy:

The Westchester Headache Center's privacy officer oversees our activities related to The Westchester Headache Center's policies and procedures concerning the privacy of and access to patient Protected Health Information (PHI) in compliance with appropriate Federal and state laws and The Westchester Headache Center's information privacy practices.

Responsibilities:

- Provides guidance and assists The Westchester Headache Center with The Westchester Headache Center's information privacy policies and procedures in coordination with management, administration and our legal counsel.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with The Westchester Headache Center's compliance and operational assessment functions.
- Helps to insure that The Westchester Headache Center has and maintains appropriate privacy and confidentiality consent, authorization and other forms, and those information and other notices and materials reflecting the practices and requirements.
- As directed, may oversee, and direct and/or deliver such privacy training and orientation to all our employees (including regular employed staff and volunteers, medical and professional staff, business associates and/or other contractors, and other appropriate third parties) as instructed.
- As directed, may participate in the development of, and ongoing compliance monitoring of all trading partner and business associate agreements, to assure privacy concerns and responsibilities are appropriately addressed.
- As directed may establish with The Westchester Headache Center's management required procedures to track access to protected health information, as instructed and as may be required by law and to allow qualified individuals to review or receive reports on such activity.
- As directed, works in supervising patient rights and to inspect, amend, and restrict access to protected health information as and when appropriate.
- As directed, may establish, maintain and administer The Westchester Headache Center's process for receiving, documenting, tracking, investigating, and taking required action on all privacy complaints concerning The Westchester Headache Center's privacy practices, including with management and, when necessary, our legal counsel.
- As directed, may assure compliance with privacy practices and the application of sanctions for failure to comply with The Westchester Headache Center's privacy

policies as regards our staff, all individuals in our workforce, and for third parties including our business associates.

- As directed, may promote activities to strengthen information privacy awareness within The Westchester Headache Center and our contractors and business associates.
- As directed, may overview our computer -related information security plans throughout The Westchester Headache Center for purposes of security and privacy practices.
- As directed, may work with The Westchester Headache Center's personnel who are involved with any aspect of release of protected health information, to assure compliance with our policies, procedures and legal requirements

The preceding is intended to serve as a scalable framework for The Westchester Headache Center in our development of a position description for the privacy officer. Our privacy officer may be assigned less or additional duties and responsibilities from time to time as directed by The Westchester Headache Center's management.

SECURITY STANDARDS

Policy:

It is the policy of The Westchester Headache Center to establish and maintain appropriate security standards and practices in order to ensure privacy and confidentiality as required.

Procedure:

The Westchester Headache Center acknowledges that HIPAA calls for security standards. It is our policy to take those steps necessary to protect all electronic protected health information (“PHI”) from improper access or alteration, and to protect against loss of PHI, identifiable health information and other records.

The electronic signature standard, applicable with respect to use with the specific transactions defined in the Health Insurance Portability and Accountability Act will use an appropriate electronic signature where such must be used or is otherwise required.

The Westchester Headache Center will take appropriate procedures to comply with the following 6 areas:

1. Administrative Procedures:

- Certification
- Chain of trust Partner Agreements
- Contingency Plan
- Formal Mechanism for Processing Records
- Information Access Control
- Internal Audit
- Personnel Security

2. Physical Safeguards:

- Assigned Security Responsibility
- Media Controls
- Physical Access controls
- Policy / Guidelines on Workstation Use
- Secure Workstation Location
- Security Awareness Training

3. Security Configuration Management:

- Security Incident Procedures
- Security Management Process

- Termination Procedures
- Training

4. Technical Security Services:

- Access Controls
- Audit Controls
- Authorization Controls
- Data Authentication
- Entity Authentication

5. Technical Security Mechanism:

- Communication/Networking Controls
- Network Controls

6. Electronic Signature:

- Digital Signature

The Westchester Headache Center has designated our Privacy Officer as the individual having the responsibility of ensuring that The Westchester Headache Center complies with the minimal level of security as outlined in the regulations and as set forth above.

The Westchester Headache Center will carry out its security responsibilities by utilizing (but not limited to) the following procedures:

Employing Chain of Trust Partner Agreements

Implementation of our "Minimum Necessary" procedures regarding PHI

Controlling access to PHI, including but not limited to:

- Keeping physical PHI and patient records in lockable areas
- Restricting access to PHI to authorized staff
- Preventing non-employees access to areas where PHI is kept and/or maintained
- Utilizing such other access controls as may be appropriate from time to time

THE WESTCHESTER HEADACHE CENTER'S SECURITY OFFICER

Policy:

The Westchester Headache Center's security officer oversees our activities related to The Westchester Headache Center's policies and procedures concerning the security of patient Protected Health Information (PHI) in compliance with appropriate Federal and state laws and The Westchester Headache Center's information privacy practices.

Responsibilities:

- Provides guidance and assists The Westchester Headache Center with The Westchester Headache Center's security policies and procedures in coordination with management, administration and our legal counsel.
- Performs initial and periodic information security risk assessments and conducts related ongoing compliance monitoring activities in coordination with The Westchester Headache Center's compliance and operational assessment functions.
- Helps to insure that The Westchester Headache Center has and maintains appropriate security for our PHI and the physical practice, it's data, and general access to data including the practice itself, it's data and our computerized data and PHI and The Westchester Headache Center's computer system. As directed, may oversee, and direct and/or deliver such privacy training and orientation to all our employees (including regular employed staff and volunteers, medical and professional staff, business associates and/or other contractors, and other appropriate third parties) as instructed.
- As directed, may participate in the development of, and ongoing compliance monitoring of all trading partner and business associate agreements, to assure privacy concerns and responsibilities are appropriately addressed.
- As directed may established with The Westchester Headache Center's management required procedures to track access to protected health information, as instructed and as may be required by law and to allow qualified individuals to review or receive reports on such activity.
- As directed, works in supervising patient rights and to inspect, amend, and restrict access to protected health information as and when appropriate.
- As directed, may establish, maintain and administer The Westchester Headache Center's process for receiving, documenting, tracking, investigating, and taking required action on all privacy complaints concerning The Westchester Headache Center's privacy practices, including with management and, when necessary, our legal counsel.
- As directed, may assure compliance with our security procedures and practices and the application of sanctions for failure to comply with The Westchester Headache

Center's security policies as regards our staff, all individuals in our workforce, and for third parties including our business associates.

- As directed, may promote activities to strengthen The Westchester Headache Center's security, both within The Westchester Headache Center and our contractors and business associates.
- As directed, may overview our computer-related information security plans throughout The Westchester Headache Center for purposes of security thereof.
- As directed, may work with The Westchester Headache Center's personnel who are involved with any activities having an effect on the security of protected health information or of The Westchester Headache Center in general, to assure compliance with our policies, procedures and legal requirements

The preceding is intended to serve as a scalable framework for The Westchester Headache Center in our development of a position description for a practice security officer. Our security officer may be assigned less or additional duties and responsibilities from time to time as directed by The Westchester Headache Center's management.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR MARKETING PURPOSES

Policy

It is the policy of THE WESTCHESTER HEADACHE CENTER to secure an authorization to use or disclose Protected Health Information (PHI) for marketing purposes in compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996.

Procedure

THE WESTCHESTER HEADACHE CENTER will obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of a face-to-face communication with the patient or a promotional gift of nominal value provided by THE WESTCHESTER HEADACHE CENTER.

If any such marketing involves THE WESTCHESTER HEADACHE CENTER receiving direct or indirect remuneration by a third party, the authorization will state that such remuneration is involved.

For purposes of this Policy, the term “marketing” is defined as:

- To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
- An arrangement involving The Westchester Headache Center or another covered entity whereby PHI is disclosed by The Westchester Headache Center or the other covered entity/entities in exchange for direct or indirect remuneration, so that the other entity or any affiliate thereof can make a communication that encourages the purchase or use of its own product or service.

The following are examples of situations that do not meet the definition of marketing:

- Communications that are merely promoting good health and not about a specific product or service does not meet the definition of “marketing.” So mailings reminding women to get an annual mammogram, or with information about how to lower cholesterol, about new developments in health care like new diagnostic tools or about health or “wellness” classes, support groups and health fairs are permitted and not considered marketing.
- Communications about government-sponsored programs do not fall within the definition of marketing. There is no commercial component to communications about benefits available through public programs. So covered entity is permitted to use/disclose PHI to communicate about eligibility for Medicare supplement benefits, or SCHIP.
- Covered entities may make communications in newsletter format without authorization so long as the content of such does not fit the definition of “marketing.”

Exceptions to the Scope of Marketing Activities so that a particular authorization is not needed:

Marketing does not include:

- Oral or written communications that describe THE WESTCHESTER HEADACHE CENTER's network or covered services.
- Communications about treatment for the patient.
- Communications about case management or the coordination of patient care, or recommendations for treatment alternatives and/or care options, including health care providers or particular settings in which such care may be provided.

The following are examples of the above exceptions:

- The Westchester Headache Center and other covered entities can convey information to beneficiaries and members about health insurance products offered by covered entity that could enhance or substitute for existing health plan or other insurance coverage. For example, if a child is about to "age out" of coverage under a patient's family insurance policy, this provision will allow the plan to send the family information about continuation coverage for their child. This does NOT extend to excepted benefits such as accident-only policies or to other lines of insurance.
- Physicians may write a prescription for, or make referrals of an individual patient to a specialist for follow-up tests and/or treatment, because these are communications about treatment.

The following are examples of situations that require authorization:

The HIPPA Rules DO NOT ALLOW The Westchester Headache Center or another covered entity to sell lists of patients or enrollees to third parties, or to disclose PHI to a third party, for any independent marketing activities of such third party. For example, a pharmaceutical company cannot pay a provider for a list of patients with a particular condition or who may be taking a particular medication and then use that list to market its own drug products directly to those patients.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR JUDICIAL & ADMINISTRATIVE PROCEEDINGS

Policy

THE WESTCHESTER HEADACHE CENTER may disclose PHI in the course of any judicial or administrative proceeding in response to an order from a court or administrative tribunal or in response to a subpoena or a subpoena duces tecum, warrant or other court order. Disclosure may also occur in response to a discovery request, or other lawful process that may not be accompanied by an order of a court or administrative tribunal.

Procedure

We may only release PHI in such instances if at least one of the following three events has occurred:

1. We may release PHI if we receive *written* “satisfactory assurance” from the party requesting the information that reasonable efforts have been made by such party to ensure that the patient who is the subject of the PHI has been given notice of the request.

“Satisfactory assurance” that the requesting party has tried to notify the patient of the PHI request means the following:

- The requesting party has given THE WESTCHESTER HEADACHE CENTER a *written statement and accompanying documentation* demonstrating that the requesting party has made a good faith attempt to provide written notice to the patient (if the patient’s location is unknown, documentation showing that a notice was mailed to the patient’s last known address).
 - The notice provided by the requesting party to the patient contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient’s PHI.
 - The time for the patient to raise objections to the court or administrative tribunal has passed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court’s resolution.
2. We may also release PHI to a requesting party if we receive satisfactory *written* assurance from the requesting party that reasonable efforts have been made by such party to secure a *qualified protective order*. A *qualified protective order* is an order of a court or administrative tribunal or a stipulation by the parties to the proceeding that prohibits the parties from using or disclosing PHI for any purpose other than the proceeding for which the information was requested and requires the parties to return the

PHI (including all copies made) to the THE WESTCHESTER HEADACHE CENTER at the end of the proceeding.

“Satisfactory assurance” in this instance means that we have received from the requesting party a written statement and accompanying documentation demonstrating that:

- The parties to the dispute giving rise to the request for PHI have *agreed* to a qualified protective order and have presented it to a court or administrative tribunal with jurisdiction over the dispute.

OR:

- The requesting party has asked for a qualified protective order from such court or administrative tribunal.

3. We may release PHI to a requesting party even without satisfactory assurance from that party if we either:

- a. Make reasonable efforts to provide notice to the patient about releasing his or her PHI, so long as the notice meets all of the following requirements:
 - The notice is written and given to the patient (if the patient’s location is unknown, we should establish documentation showing that a notice was mailed to the patient’s last known address).
 - The notice contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient’s PHI.
 - The time for the patient to raise objections to the court or administrative tribunal has elapsed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court’s resolution.

OR:

- b. Seek a qualified protective order from the court or administrative tribunal or convince the parties to stipulate to such order.

PROHIBITION OF RETALIATION AGAINST EMPLOYEES (WHISTLE BLOWERS)

Policy

THE WESTCHESTER HEADACHE CENTER will take all necessary steps to refrain from intimidating, threatening, coercing, discriminating against, or taking any other retaliatory action against any employee, individual, or other for the exercise of any right under, or for participation in any process established applicable laws and/or regulations.

1. It is the responsibility of The Westchester Headache Center and all of our employees to report perceived misconduct including actual or potential violations of laws, regulations, policies, or procedures.
2. Our office will maintain an open-door policy at all levels of The Westchester Headache Center to encourage staff to report problems and concerns.
3. We will follow all necessary procedures to protect against any retaliation toward any of our employees or other individuals for exercising their rights or participation in any process pursuant to internal policies, applicable State or Federal laws or regulations.
4. Any employee who commits, aids, abets, encourages or condones any form of retaliation will be subject to discipline up to, and including termination.

Procedures

We will not retaliate against employees, individuals, or others for:

- Exercising any right under, or participating in any process established by federal, state, or local law, regulations, or policy.
- Filing a complaint with The Westchester Headache Center management and/or the owner of The Westchester Headache Center and/or the Department of Health and Human Services.
- Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing.
- Opposing in good faith any act or practice made unlawful by federal, state, or local law, regulation, or policy, provided that the manner of the opposition is reasonable and does not itself violate law.