

# **HIPAA PRIVACY PROCEDURES MANUAL**

**Dr. Scott Spector's Eyecare Centers  
New Vision Cataract Center  
New Vision Laser Center**

**As of March 12, 2003**

This document contains the procedures to be followed by all workforce members and contractors to comply with privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Questions concerning the contents of this document should be referred to Privacy Official, 203-853-1110.

Table of Contents

<a href="#"><u>PROCEDURE: ACCESS REQUEST PROCESSING</u></a> .....	3
<a href="#"><u>PROCEDURE: AMENDMENTS TO PROTECTED HEALTH INFORMATION</u></a> .....	6
<a href="#"><u>PROCEDURE: COMPLAINT HANDLING</u></a> .....	8
<a href="#"><u>PROCEDURE: CONFIDENTIAL COMMUNICATIONS REQUESTS</u></a> .....	10
<a href="#"><u>PROCEDURE: DISCLOSURE ACCOUNTING REQUEST PROCESSING</u></a> .....	11
<a href="#"><u>PROCEDURE: HIPAA EXCEPTIONS ALLOWING USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION</u></a> .....	13
<a href="#"><u>PROCEDURE: INDIVIDUAL PERMISSION PROCESSING</u></a> .....	17
<a href="#"><u>PROCEDURE: INFORMATION REQUEST AND DISCLOSURE-MINIMUM NECESSARY</u></a> .....	21
<a href="#"><u>PROCEDURE: MINIMUM NECESSARY ACCESS</u></a> .....	23
<a href="#"><u>PROCEDURE: NOTICE OF PRIVACY PRACTICES AND ACKNOWLEDGEMENT</u></a> .....	24
<a href="#"><u>PROCEDURE: PERSONAL REPRESENTATIVES</u></a> .....	26
<a href="#"><u>PROCEDURE: RESTRICTION REQUEST PROCESSING</u></a> .....	29
<a href="#"><u>PROCEDURE: WORKFORCE TRAINING AND AWARENESS</u></a> .....	31

**Note: Requests concerning minors.** Physicians in Connecticut who are treating minors under circumstances in which the minor independently consents to health care are prohibited from disclosing medical information concerning the minor without the minor's written authorization. (For further information on the rights of minors in Connecticut, see the reference document entitled "Special Consent Rights of Minors Under Connecticut Law").

**Note: Requests by persons other than the patient.** Except in limited circumstances, HIPAA permits a patient's personal representative to request and receive access to the patient's protected health information. Connecticut law will determine whether an individual has the authority to act as a patient's personal representative and thus have the right to request and receive access to the patient's protected health information. (For further information on personal representatives, see the procedure entitled "Personal Representatives").

### **General Note to all Part of this Document**

The office managers have been appointed as the Dr. Scott Spector's Eyecare Centers "privacy officials". Throughout this document, wherever there is made reference to the "privacy officials", the meaning is the office managers.

## ***Procedure: Access Request Processing***

### **Actions to be taken for requests to access:**

1. All requests for inspection or copying will be forwarded to the privacy officials.
2. The privacy officials will inform the patient or his or her personal representative that this medical practice requires the request to be submitted using our Request for Patient Access to Health Information form. This form will be given to the patient or representative at our office, or mailed or faxed; if the patient expresses concerns about completing a form he or she will be referred to the privacy officials, who will provide assistance in completing the form.
3. Once the Request for Patient Access to Health Information form is received the privacy officials will review the request form. This review will verify the scope of the requested access-all records or a portion. The review will also determine if the patient or his or her personal representative has requested a) an inspection only, b) copies only or c) inspection and copies. In addition, if this medical practice does not have the information the patient has requested to access, we will, if possible, inform the patient where to direct his or her request.

The privacy officials will determine whether the request will be granted or denied. Whether a request may be denied will depend upon the type of information to which access has been requested.

4. The privacy officials will document the decision to grant or deny the requested access on the Response to Request for Patient Access to Health Information form. A copy of the Response form will be sent by certified (receipt) mail. If the request is granted and the patient has requested copies, the copies must be provided to the patient within thirty days from the date the patient's request was received. If the patient has requested only to inspect the information, the Response form will be sent to the patient within thirty days of the patient's request and the inspection may occur within a reasonable time thereafter.
5. If a request is granted and the patient has requested copies, the privacy officials will ensure that the Response clearly states the fee that will be charged for the copies. If a request is granted and the patient has requested inspection, the privacy officials will arrange a convenient time for the inspection.
6. This practice will charge) no more than \$0.45 per page, including any research fees, handling fees and the cost of first class postage, if applicable, for copies of the information requested. This practice will also charge the patient as necessary to cover the cost of materials for providing a copy of an x-ray. However, a fee will not be charged to any patient that requests copies of medical information for purposes relating to a claim or appeal under any provision of the Social Security Act, if that patient provides documentation of the claim or appeal.
7. For approved inspection requests, the privacy officials (or another employee designated by the privacy officials) will be present at all times when the patient is reviewing any original records.
8. If a request for access is denied, the Response will clearly state (a) the basis for the denial, (b) if applicable (see step 11), a description of the patient's right to have the denial reviewed by a licensed health care professional who was not directly involved in the decision to deny the request and (c) a description of how the patient may file a complaint with this medical practice and with the Secretary of DHHS.
9. The patient will have a right to request a review of the denial only where the request has been denied for one of the following three reasons:
  - **a licensed health care provider determines that the access requested is reasonably likely to endanger the life or physical safety of the patient or someone else**

- **the information references another person to whom the access is reasonably likely to cause substantial harm**
- **the request is made by the patient's Personal Representative and a licensed health care provider determines that providing access to the Personal Representative is reasonably likely to cause substantial harm to the patient or someone else.**

10. If the patient has the right to request a review, and the patient or his or her personal representative requests a review, the privacy officials will promptly arrange for the review to be conducted by a licensed health care professional who may or may not be in this practice who did not participate in the original review and denial.

11. The review must be completed within a reasonable amount of time. The results of the review will be documented. The patient will be provided with written notice of the decision. If access is granted, the patient will be allowed to inspect or obtain a copy of his or her information in accordance with these procedures.

12. The privacy officials will file all completed Requests, Responses and review decisions in this organization's HIPAA Compliance file and not with the patient's medical record. A list of the designated record sets that may be accessed by patients will also be kept in the HIPAA Compliance file.

## ***Procedure: Amendments to Protected Health Information***

### **Actions to be taken for amendments:**

1. All requests for amendment will be forwarded to the privacy officials.
2. The privacy officials will inform the patient or his or her personal representative that this practice requires the request to be submitted using our Request for Amendment form. This form will be given to the patient at our office, or mailed or faxed to the patient; if the patient expresses concerns about completing a form they will be referred to the privacy officials, who will assist them in completing the form.
3. Once the Request for Amendment is received, the privacy officials will review the Request for Amendment. The request may be denied for any of the following reasons: (1) the information that the patient has requested to amend was not created by this medical practice (unless the patient provides a reasonable basis to believe that the person or entity that did create the information no longer exists, (2) the information that the patient has requested to amend is not part of the medical or billing records of the medical practice and is not information that is used to make decisions about the patient, (3) the patient does not have a right to access the information they have requested to amend or (4) the information the patient has requested to amend is already accurate and complete.
4. The privacy officials will determine whether to grant or deny the patient's request for amendment and complete a Response to Request for Amendment. The Response form must be provided to the patient within 60 days unless the patient has been informed, in writing, by the privacy officials of the following: that there will be a 30 day delay, the reasons for the delay and the date by which the patient can expect to receive a response.
5. If the request is denied, the Response form must be completed to indicate the basis for the denial, instructions as to how the patient may submit a Statement of Disagreement, a statement that if the patient does not submit a Statement of Disagreement, the patient may request that the medical practice include the patient's Request for Amendment and the medical practice's Response form denying the request with any future disclosures of the information to which the patient requested the amendment and a description of how the patient may file a complaint with the medical practice or the Secretary of DHHS.
6. If the patient's request is denied and the patient chooses to file a Statement of Disagreement with the medical practice, the privacy officials will determine

whether to complete a Rebuttal Statement on behalf of the medical practice. If a Rebuttal Statement is completed, a copy will be sent to the patient.

7. With respect to any information in the patient's medical and billing records for which a requested amendment was denied, a link must be provided to the location of the patient's Request for Amendment, the medical practice's Response, the Statement of Disagreement, if any, and the Rebuttal Statement, if any.
8. If the patient submits a Statement of Disagreement, future disclosures of information to which the amendment was denied must include a copy of the patient's Request for Amendment, the medical practice's Response, the Statement of Disagreement and the Rebuttal Statement (if there is one) or an accurate summary of these documents.
9. If the patient does not submit a Statement of Disagreement, future disclosures of information to which the amendment was denied must include, only if the patient so requests, a copy of the patient's Request for Amendment and the medical practice's Response.
10. If the request for amendment is approved, the privacy officials will insert a copy of the amendment into the medical record (chart) in a special section or tab titled "Amendments". A colored label will be placed on the front of the chart indicating that an amendment is in place. For any information in the patient's medical and billing records that is affected by the amendment, a link to the relevant tab must be provided.
11. If the request for amendment is approved, a copy of the patient's Request for Amendment form, clearly marked "GRANTED", will be sent to each individual or entity that the patient or his or her personal representative requested that we notify on the Request for Amendment form.
12. If the patient has NOT restricted, on his or her request for Amendment form, notification to other individuals or entities that we know have received the information that is the subject of the amendment, we will send a copy of the patient's Request for Amendment form, clearly marked "GRANTED", to those individuals or entities who have received the information and may rely on it to the detriment of the patient.
13. Future disclosures of the information that the patient requested to amend must include, if the request was granted, a copy of the amendment.
14. The privacy officials will file the original Request and the Response, the Statement of Disagreement, if any, and the Rebuttal Statement, if any, in this organization's HIPAA compliance file.

## ***Procedure: Complaint Handling***

### **Actions to be taken for all complaints received:**

1. When any staff member receives a privacy complaint from a patient, the patient's personal representative, or any other person, the staff member will document the complaint and inform the privacy officials. The information to be documented and reported to the privacy officials and must include, at a minimum:
  - the name of the complainant;
  - the date and time of the complaint;
  - the name of the staff member who received the complaint;
  - the circumstances giving rise to the complaint.
2. The privacy officials will contact the person making the complaint as soon as possible and no later than ten business days of the date of the complaint.
3. The privacy officials will request that the patient complete a written complaint form.
4. If the privacy officials are on vacation or temporarily unavailable, another staff member will be appointed to handle complaints in his or her absence. The staff will be advised as to who has been appointed to perform these duties. This organization will always respond to privacy complaints within ten business days.
5. The privacy officials will file the completed complaint form in the HIPAA compliance file and not as part of the patient's medical record. The privacy officials will take reasonable steps to investigate the issues raised in the complaint.

### **Actions to be taken when no compliance violation has occurred:**

1. If the privacy officials determine that there has been no violation of this organization's privacy policies or of HIPAA, he or she will document these findings on the complaint form. (*IMPORTANT: If, in the course of investigating the privacy complaint, the privacy officials determine that the complaint is related to clinical or medical care, the situation will be referred to the appropriate person in the organization.*)

2. The privacy officials will provide the patient with a written record of the complaint resolution. A copy will also be placed in the organization's HIPAA compliance file.
3. The privacy officials will document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.

**Actions to be taken when a compliance violation has occurred:**

1. If the privacy officials determine that a violation of this organization's privacy policies or HIPAA has occurred, he or she will document this fact on the complaint form.
2. The privacy officials will, as soon as possible, review the violation and develop a remediation plan. The privacy officials will document the remediation steps on the complaint form and the action plan established to complete them. The privacy officials will advise the appropriate workforce members or other persons (if any) who bear responsibility for implementing the corrective action plan. The privacy officials will also impose the appropriate sanctions on responsible personnel. *(IMPORTANT: If, in the course of investigating the privacy complaint, the privacy officials determine that the complaint is related to clinical or medical care, the situation will be reported to the appropriate person in the organization.)*
3. The privacy officials will also provide the patient with a written record of the complaint resolution. A copy will also be placed in the organization's HIPAA compliance file.
4. The privacy officials will document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.
5. The privacy officials will be updated on a regular basis as to the status of the remediation plan until all corrective activities have been accomplished.
6. The privacy officials will notify appropriate individuals within the organization who have risk management responsibilities for the complaint, the findings of the investigations and any actions taken.

## **Procedure: Confidential Communications Requests**

### **Actions to be taken for confidential communications requests:**

1. All requests taken by staff or physicians will be forwarded to the privacy officials.
2. All patients or their representatives who request a confidential communication will be asked to complete the "Confidential Communications Request form.
3. If possible, the privacy officials will review the completed form while the patient is still present. If not, Dr. Scott Spector's Eyecare Centers will respond to requests within a reasonable amount of time.
4. The privacy officials will review completed written requests and determine whether the request can be reasonably accommodated. If the request is reasonable it will be granted. If the request is one that this organization cannot reasonably accommodate it will be denied. Grants and denials will be documented on the Response to Confidential Communications Request form.
5. The privacy officials or staff of Dr. Scott Spector's Eyecare Centers may not require the patient or his or her personal representative to give a reason as to why the request is being made.
6. The grant or denial will be made in person if the privacy officials have reviewed the request while the patient is still present. The privacy officials will provide the patient with a copy of the Response.
7. If the Response is not given to the patient in person, the privacy officials will mail a copy of the Response form to the patient.
8. If the request is granted, the privacy officials will place one copy of the Confidential Communications Request/Response form in the patient's medical record. An additional copy will be filed in this organization's HIPAA Compliance file.
9. If a request is granted, the privacy officials will meet with the appropriate workforce members to ensure that the request is implemented in their operational activities.

## ***Procedure: Disclosure Accounting Request Processing***

### **Actions to be taken for disclosure accounting requests:**

1. All requests for disclosure accounting will be forwarded to the privacy officials.
2. The privacy officials will inform the patient or his or her personal representative that this practice requires the request to be submitted using our Request for Accounting of Disclosures of Protected Health Information form. This form will be given to the patient or representative at the office or mailed or faxed to the patient; if the patient expresses concerns about completing the form he or she will be referred to the privacy officials, who will assist with completing the form.
3. Once the Request for Accounting of Disclosures of Protected Health Information Request form is received, the privacy officials will review the request form. The privacy officials will identify all disclosures made during the relevant accounting period (six years unless the patient specifies otherwise), including disclosures made by our business associates, for which the patient has a right to receive an accounting under state law or HIPAA.
4. The patient has a right to receive an accounting of all disclosures of PHI except disclosures that were made:
  - Prior to April 14, 2003;
  - To the patient;
  - Pursuant to a valid Authorization;
  - To carry out treatment, payment or health care operations;
  - As incidental disclosures made in connection with a use or disclosure that is otherwise permitted or required by the Privacy Rule;
  - As part of a limited data set;
  - For purposes of a facility directory;
  - To persons involved in the patient's care or other notification purposes;
  - For national security or intelligence purposes; or
  - To a law enforcement official or correctional institution having lawful custody of the patient at the time of the disclosure.
5. Even if an accounting is not required by HIPAA, an accounting may be required by Connecticut law if the disclosure includes HIV-related information. Under Connecticut law, all disclosures of HIV-related information must be accounted for except those disclosures that are made to:

- A federal, state, or local health officer when required or permitted by law
- Persons reviewing information or records in the ordinary course of ensuring that a health facility is in compliance with applicable quality of care standards or any other authorized quality of care standards, program evaluation, program monitoring or service review; and
- Life and health insurers, government payers and health care centers in connection with underwriting and claim activity for life, health, and disability benefits.

An accounting will be required for a disclosure of HIV-related information unless an exception applies under Connecticut law. For example, if HIV-related information was disclosed pursuant to an Authorization, an accounting would not be required by HIPAA. However, an accounting would still be required by Connecticut law unless one of the three exceptions above applied.

6. The patient's first accounting in each 12-month period will be provided free of charge. The patient will be informed in advance that, if the patient has already requested an accounting within the past twelve months, there will be a charge for preparing the Accounting. The privacy officials will not complete the Accounting until the fee has been paid.
7. The privacy officials will prepare an accounting of disclosures by using the Accounting of Disclosures of PHI form. For each disclosure, the privacy officials will record, on the Response to Request for Accounting of Disclosures of PHI form, the following information: date of the disclosure, name and, if known, address of the person or entity to whom the disclosure was made; a brief description of the PHI that was disclosed and a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure. This form will be sent by certified (receipt) mail. The Accounting will be completed and mailed within 60 days of receipt of the Request for Accounting of Disclosures of PHI form, unless the patient is informed in writing that there will be a delay (of up to thirty days), the reasons for the delay, and the date by which the patient can expect to receive the accounting.
8. The privacy officials will place a copy of the following forms in this organization's HIPAA Compliance file:
  - Request for Accounting of Disclosures of PHI form;
  - Response to Request for Accounting of Disclosures of PHI form; and
  - Accounting of Disclosures of PHI form.

## ***Procedure: HIPAA Exceptions Allowing Uses and Disclosures of Protected Health Information***

**Note:** This procedure addresses HIPAA exceptions permitting use or disclosure of PHI without an Authorization or the opportunity to object. In some instances, state law may require an authorization or otherwise limit disclosure. Examples include disclosures of HIV-related information or information concerning diagnosis or treatment of a psychiatric condition or substance abuse.

### **Actions to be taken for situations in which Authorization or the opportunity to agree or object does not apply:**

1. PHI may be used or disclosed without obtaining a HIPAA Authorization or allowing patients an opportunity to agree or object under the following circumstances
  - A. The use or disclosure is required by law. The use or disclosure must comply with, and be limited to, the relevant requirements of the law.
  - B. The disclosure is to a public health authority for a public health activity such as reporting disease, injury, or disability.
  - C. The disclosure is to a public health or government agency authorized to receive reports of child abuse or neglect.
  - D. The disclosure is to the Food and Drug Administration for purposes such as reporting adverse events, reporting product defects, tracking products, enabling product recall, repairs or replacements or performing post marketing surveillance.
  - E. The disclosure is to a person who may have been exposed to a communicable disease, if this medical practice is authorized by law to notify the person.
  - F. The disclosure is to a government authority, including social services or a protective services agency, that is authorized by law to receive reports of adult abuse, neglect, or domestic violence if:
    - The disclosure is required by law;
    - The patient agrees; or
    - The disclosure is authorized by law and:
      - is necessary to prevent serious harm, or

- the patient is incapacitated and the authorized public official represents that the PHI will not be used against the patient and is needed for immediate enforcement activity.
  - This medical practice will promptly inform the patient of the disclosure unless:
    - This medical practice believes that informing the patient will increase the harm
    - This medical practice would be informing the patient's personal representative, and we believe the personal representative is responsible for the abuse, neglect or domestic violence.

G. The disclosure is to a health oversight agency for health oversight activities authorized by law, such as audits; civil, administrative or criminal investigations; inspections and licensure or disciplinary actions.

H. The disclosure is for a judicial or administrative proceeding and is:

- In response to a court order, if this medical practice discloses only the PHI expressly authorized by the court order
- In response to a subpoena, discovery request, or other lawful process, not accompanied by an order of a court if:
  - This medical practice receives satisfactory assurance that the party seeking the information has notified the patient of the request; or
  - This medical practice receives assurance that the party seeking the information has made efforts to secure a qualified protective order.
  - HIPAA regulations contain detailed requirements for obtaining and documenting assurances.

I. The disclosure is permitted for law enforcement activities. For example, the disclosure is in compliance with a:

- Court order, or a court-ordered or issued warrant, subpoena, or summons;
  - Grand jury subpoena; or
  - Administrative request provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used.
- This medical practice may also disclose PHI in response to a law enforcement officer's request for information for the purpose of identifying or locating a suspect, fugitive, material

witness, or missing person provided that only specific information is disclosed

- This medical practice may disclose PHI about an individual who is or is suspected to be a victim of a crime if:
  - The disclosure is required by law;
  - The individual agrees to the disclosure; or
  - The Organization is unable to obtain the individual's agreement because of incapacity or other emergency circumstance provided that:
    - The law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred and that information is not intended to be used against the victim;
    - The law enforcement official represents that immediate law enforcement activity depends upon the PHI and will be adversely affected by waiting until the individual is able to agree to the disclosure; and
    - The disclosure is in the best interests of the individual as determined by the practice.
- This medical practice may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the practice has a suspicion that such death may have resulted from criminal conduct.
- This medical practice may disclose to a law enforcement official PHI that the practice believes in good faith is evidence of criminal conduct that occurred on its premises.
- If emergency health care is provided in response to a medical emergency not on the premises of this practice, we may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
  - The commission and nature of a crime
  - The location of the crime or the victim(s) of the crime
  - The identity, description, and location of the perpetrator of the crime

J. The disclosure is to a coroner or medical examiner to:

- Identify a deceased person;
- Determine a cause of death; or
- Perform other duties as authorized by law.

K. The disclosure is to funeral directors consistent with applicable law, as necessary to carry out their duties with respect to the decedent.

Information disclosed may include PHI prior to, and in reasonable anticipation of, the individual's death.

L. The disclosure is to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs for the purpose of facilitating the transplantation.

M. The use or disclosure is to avert a serious threat to health or safety if in good faith the practice believes the use or disclosure:

- Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat or
- Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that may have caused serious physical harm to the victim or where it appears from circumstances that the individual has escaped from lawful custody.

N. For individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure proper execution of the military mission and other special government functions.

O. The disclosure is to a correctional facility or law enforcement official having lawful custody of an inmate or other individual, provided certain required representations are made.

P. As authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault.

Q. For research provided specific conditions are satisfied.

2. The privacy officials will review each request for a use or disclosure of PHI to determine if the disclosure may be made without obtaining a HIPAA Authorization or allowing the patient an opportunity to agree or object to the use or disclosure.

## ***Procedure: Individual Permission Processing***

### **Introduction:**

The procedures in Section I of this document will be followed when a patient's written Authorization is required. A written Authorization is generally required for uses and disclosures of protected health information ("PHI") for purposes other than treatment, payment or health care operations, unless the use or disclosure is otherwise permitted by both state law and HIPAA. (*For further information, refer to "Procedure: HIPAA Exceptions That Do Not Require Authorization"*).

In certain limited circumstances, a patient may verbally agree to the use or disclosure of PHI, and a written Authorization will not be required. A patient's verbal agreement will be obtained only in accordance with Section II of this document.

### **Actions to be taken for obtaining individual permission:**

#### **I. Obtaining Written Authorization**

**Note on Marketing:** HIPAA established special requirements for marketing activities. The patient's authorization must be obtained for all marketing activities except:

1. face-to-face communication by the physician or other employee of the physician practice; or
2. promotional gifts of nominal value provided to the patient by the physician practice.

In addition, the authorization must indicate whether the physician practice receives direct or indirect remuneration from a third party in connection with the marketing activities.

"Marketing" is defined by HIPAA to include all communications that encourage the purchase or use of a product or service except communications for:

1. treatment;
2. case management or care coordination of the individual, or direct or recommended alternative treatments, therapies, health care providers or settings of care;

3. certain other health plan communications concerning benefits; or
  4. to describe a health-related product or service (or payment for a product or service) that the Covered Entity provides
1. The privacy officials will complete and maintain an accurate and up to date list of uses and disclosures of PHI for which an Authorization is required by HIPAA or state law or other federal law. Examples may include:
    - Physical examinations known as “pre-employment exams” for which we are paid by a patient’s employer.
    - Disclosure of medical records for life insurance, disability insurance or health insurance underwriting of a new policy for an existing patient.
    - Independent medical exams that we perform and for which we are paid as an expert by a third party.
    - Disclosures of PHI that contain psychotherapy notes, psychiatric communications, information relating to AIDS or HIV, or substance abuse records
  1. The privacy officials will coordinate with the front office staff to obtain a written Authorization from a patient or the patient’s personal representative whenever this organization will be disclosing PHI that requires Authorization.
  2. The privacy officials will review all completed Authorizations to ensure they are valid and not defective.
  3. The privacy officials will ensure that a written Authorization is on file prior to the disclosure of any PHI for which an Authorization is required.
  4. The privacy officials will provide the patient or the patient’s personal representative with a copy of the completed Authorization.
  5. This medical practice will not condition treatment or future care on the patient’s provision of an Authorization, except that (a) the provision of research-related treatment may be conditioned on provision of an Authorization for use or disclosure of PHI for the research and (b) the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party may be conditioned on provision of an Authorization for disclosure of PHI to the third party.
  6. The patient may revoke an Authorization, to the extent that this medical practice has not already taken action in reliance on the Authorization, by submitting the revocation in writing to the privacy officials.

## **II. Verbal Agreement**

1. Provided that the patient is given an opportunity to agree or to object, the patient's health information may be shared with friends or family involved in the patient's care, or payment for the patient's care, without a written Authorization. This organization will seek a patient's verbal agreement prior to disclosing PHI to a family member or friend involved in the patient's care or payment for the patient's care. The patient's agreement or objection will be documented.
2. The privacy officials will train all clinical staff on this requirement and the importance of proper documentation.
3. If a patient presents with a family member or friend who is not the patient's personal representative, when appropriate, clinical staff will ask the patient if the patient gives permission for PHI regarding the current treatment of this patient to be shared with that individual.
4. If the patient provides verbal agreement, clinical staff must document this in the medical record. The date, time, name and telephone number of the family or friend will be documented. If the patient objects, the patient's objection should be similarly documented.
5. The privacy officials will train front and back office staff, including the physician and providers not to discuss or disclose any information pertaining to the patient to any individual where the patient has objected to the disclosure.
6. If the patient is not able to agree or object because he or she is incapacitated, or an emergency circumstance exists, PHI may be disclosed to a family member, relative or close personal friend only if a staff member determines, in the exercise of professional judgment, that the disclosure is in best interests of the patient.
7. A patient's verbal agreement to a use or disclosure may also be obtained for purposes of notifying a patient's family member, personal representative, friend or other person identified by the patient of the patient's location or general condition. If the patient is not able to agree or object because he or she is incapacitated, or an emergency circumstance exists, a family member, personal representative or friend may be notified of the patient's location, general condition, or death, if a staff member determines, in the exercise of professional judgment, that the disclosure is in best interests of the patient.
8. PHI may be used and disclosed if, under emergency circumstances, this medical practice coordinates with a disaster relief organization to notify our patients' friends or families of the patients' locations, general conditions or

deaths. Each patient will be given the opportunity to agree or to object, unless this medical practice determines, in the exercise of professional judgment, that providing the patients with the opportunity to agree or to object would interfere with the ability to respond to the emergency.

## ***Procedure: Information Request and Disclosure-Minimum Necessary***

### **Actions to be taken for information request and disclosure:**

#### **Uses and Disclosures:**

1. All uses and disclosures of protected health information (“PHI”) will be limited to that which is the minimum necessary, except:
  - disclosures made to a health care provider for treatment
  - disclosures made to the patient
  - uses or disclosures made pursuant to an authorization
  - disclosures made to the Secretary of DHHS to determine this medical practice’s compliance with the Privacy Rule,
  - uses or disclosures that are required by law
  - and uses or disclosures that are required for this medical practice to comply with the Privacy Rule.
2. The privacy officials have reviewed our PHI inventory and determined which types of disclosures this practice makes on a routine and recurring basis. The privacy officials have developed procedures that limit the protected health information that is disclosed during these routine disclosures to the amount that is reasonably necessary to achieve the purpose of the disclosure. All employees who are responsible for disclosing PHI must follow the procedures developed by the privacy officials when making routine disclosures of PHI.
3. With respect to disclosures of PHI that this practice makes on a non-routine basis, the privacy officials have developed a set of criteria to be reviewed each time a disclosure is made so that the PHI disclosed is limited to that which is reasonably necessary to accomplish the purpose of the disclosure. Employees who are responsible for responding to requests for disclosures of PHI will review each request based on the criteria established by the privacy officials.
4. In any of the following instances, employees responsible for responding to requests for disclosure may rely on a requested disclosure as the minimum necessary for the stated purpose of the request:
  - the request for disclosure is made by a public official, the disclosure does not require the individual’s authorization, and the public official represents that the requested information is the minimum necessary

- the request is made by another person or entity that is covered by the Privacy Rule
  - the request is made by a professional member of this practice's workforce, or by our business associate for purposes of providing us with professional services, and the professional represents that the requested information is the minimum necessary
  - a person requesting the information for research purposes has complied with other HIPAA research requirements
5. The entire medical record will not be disclosed unless the entire medical record is specifically justified as the amount of information needed to accomplish the purpose of the use or disclosure..

**Requests:**

1. Except for requests made for purposes of treatment, this medical practice will take reasonable steps to limit any PHI we request from another person or entity covered by the Privacy Rule to that which is the minimum necessary to accomplish the purpose of the request.
2. The privacy officials have reviewed the PHI inventory for this organization and determined the types of requests for PHI that this practice makes on a routine and recurring basis. The privacy officials have developed procedures that limit the protected health information that is requested during these routine requests to the amount that is reasonably necessary to achieve the purpose of the request. All employees who are responsible for requesting PHI must follow the procedures developed by the privacy officials when making routine requests for PHI.
3. The privacy officials have met with both the front and back office staff and trained them on the need to conform routine requests for PHI to the standards defined in item 2.
4. With respect to requests for PHI that this practice makes on a non-routine basis, the privacy officials have developed a set of criteria to be reviewed each time a request is made so that the PHI requested is limited to that which is reasonably necessary to accomplish the purpose of the request. Employees who are responsible for making requests for PHI will ensure that each request satisfies the criteria established by the privacy officials.
5. An entire medical record will not be requested unless the entire medical record is specifically justified as the amount of information needed to accomplish the purpose of the request.

## ***Procedure: Minimum Necessary Access***

### **Actions to be taken for minimum necessary access:**

1. The privacy officials will complete and maintain an up to date listing of staff and their job descriptions. The privacy officials will identify the staff members and/or job titles that need access to protected health information to carry out their job descriptions. For each staff member or job title, the privacy officials will identify and document the categories of protected health information to which access is required, and any conditions that will be imposed on the access.
2. Staff training and orientation will include identification of the PHI access required for each job function. Staff will be advised to limit their access to their job description and warned of the sanctions for violating this procedure.
3. Where applicable, technical controls for electronically maintained PHI will be implemented to provide access based on job description and function.

## ***Procedure: Notice of Privacy Practices and Acknowledgement***

### **Actions to be taken for Notice and acknowledgement:**

#### **NOTICE OF PRIVACY PRACTICES:**

1. By April 14, 2003 the privacy officials will create a Notice of Privacy Practices. The privacy officials are responsible for maintaining the Notice and updating it when changes to this organization's privacy practices occur.
2. The privacy officials will maintain all versions of the Notice in this organization's HIPAA Compliance file.
3. The most current version of the Notice will be posted in the waiting room.
4. As of the compliance date, April 14, 2003 all patients will be given the Notice at their next office visit, after they check in for their office visit. A patient need only receive the organization's Notice on one occasion.
5. Patients who need to receive the Notice and sign an acknowledgement will be advised to arrive ten minutes early for their scheduled appointment.
6. When the Notice changes, the privacy officials will post the revised Notice in the waiting room and provide a copy to any patient upon request.

#### **Acknowledgement:**

1. Each patient receiving the Notice will be asked to sign an Acknowledgement of Receipt of Notice of Privacy Practices. The Acknowledgement is a separate page that is attached to every Notice. If the patient is not competent, the Notice should be given to and the Acknowledgement signed by the Personal Representative (see Procedures on Personal Representatives)
2. The patient's signed Acknowledgement will be filed in the patient's medical record.
3. If the patient refuses to sign the Acknowledgement, the privacy officials will be contacted. The privacy officials will answer any questions or concerns the patient may have.

4. The patient may not be denied treatment because he or she refuses to sign the Acknowledgment (unless a specific exception permitted by HIPAA applies).
5. If the patient continues to refuse to sign the Acknowledgement, the efforts to obtain the patient's signature, and the reason why the signature was not obtained, will be documented on the Acknowledgement form.
6. Patients initially seen by the physician in the emergency room or at the hospital will be covered by the hospital's Notice. However, upon their first visit to this practice they will be provided a Notice and asked to complete the Acknowledgement.
7. The privacy officials will train the front office to recognize patient concerns or issues with the Notice. Specifically the front office will understand that the presentation of the Notice is a time when a patient may request special privacy protections, confidential communication channels, request to amend PHI, disclosure accounting, or inspection or copying of PHI. All such requests will be forwarded to the privacy officials.

## ***Procedure: Personal Representatives***

**For purposes of HIPAA, a Personal Representative is a person who is legally authorized to act on behalf of an individual with respect to Protected Health Information (“PHI”). Under HIPAA, an individual’s Personal Representative must be treated as the individual, and must be permitted to exercise the rights of the individual regarding PHI that is relevant to the personal representation.**

### **Actions to be taken to determine a patient’s Personal Representative:**

1. The following persons will be treated as a patient’s Personal Representative concerning PHI that is relevant to the personal representation:
  - A. For adults and emancipated minors who are incapable of making their own decisions, a Personal Representative is any person who has legal authority to act on behalf of the adult or emancipated minor in making health care decisions. In Connecticut, depending on the circumstances, this may include a conservator, guardian, person holding a durable power of attorney for health care, health care agent, family member or significant other.
  - B. For minors, a Personal Representative is a parent, guardian or other person acting *in loco parentis* (such as the Department of Children and Families for committed children) who has the legal authority to act on behalf of the minor in making decisions related to health care (for further information, see the document entitled “Special Consent Rights of Minors Under Connecticut Law”).
  - C. For deceased individuals, a Personal Representative is an executor or administrator of the estate or, if no estate is filed, a close family member or other person.
2. A person will not be treated as a patient’s Personal Representative if:
  - A. There is reason to believe that the patient has been or may be subjected to domestic violence, abuse or neglect by such person or treating the person as the patient’s Personal Representative may endanger the patient; and

B. We determine, in the exercise of professional judgment, that it is not in the patient's best interests to treat the person as the patient's Personal Representative.

3. A staff member will document in the patient's medical record the reasons that support any determination not to treat a person as the patient's Personal Representative.

**Actions to be taken when disclosing PHI to Personal Representatives:**

1. PHI will be disclosed to a Personal Representative only to the extent that the PHI is relevant to matters on which the Personal Representative is authorized to represent the patient and the Personal Representative is involved in making decisions for the patient.
2. If a person's identity or authority to act as a patient's Personal Representative is not known, a staff member will obtain documentation, statements or representations to verify the Personal Representative's identity and authority.
3. Where applicable, evidence of the Personal Representative's legal authority to act on behalf of the patient, including the scope of such authority, will be included in the patient's medical record (for example, durable power of attorney for health care decisions, court order for appointment of conservator, etc.).
4. Any concerns as to whether a person has the legal authority to act as a patient's Personal Representative, or whether PHI is relevant to the personal representation, will be directed to the privacy officials.

**Actions to be taken when obtaining an Authorization from a Personal Representative:**

1. We will permit a patient's Personal Representative to provide an Authorization on behalf of the patient.
2. The Authorization form will include a description of the Personal Representative's authority to act for the patient.

**Other actions to be taken with respect to Personal Representatives:**

A patient's Personal Representative must be allowed to exercise any other right not specifically addressed in this policy that is granted an individual under HIPAA, including but not limited to the right to file a complaint, the right to receive a Notice of Privacy Practices, the right to request privacy protections for the patient's PHI, the right to access and inspect the patient's PHI, the right to

request amendment of the patient's PHI and the right to request an accounting of disclosures of the patient's PHI.

## ***Procedure: Restriction Request Processing***

### **Actions to be taken for restriction requests:**

1. The privacy officials will be responsible for receiving and processing requests by patients or their personal representatives to restrict the uses or disclosures of health information that pertain to the individual.
2. This medical practice will allow a patient to request that we restrict disclosures of the patient's health information to friends and family who are involved in the patient's care or payment for the patient's care. A patient may also request that we restrict uses or disclosures of the patient's health information to carry out treatment, payment or health care operations. All requests for restriction will be forwarded to the privacy officials.
3. The privacy officials will inform the patient or his or her personal representative that this practice requires the request to be submitted using our Request for Special Privacy Protections form. This form will be given to the patient at the office, or mailed or faxed to the patient; if the patient expresses concerns about completing the form, he or she will be referred to the privacy officials, who will assist him or her in completing the form.
4. Once the Request for Special Privacy Protections form is received, the privacy officials will determine whether to agree to the restriction. This medical practice is not required to agree to any restriction.
5. The privacy officials will document his or her decision to grant or deny the restriction on the Response to Request for Special Privacy Protections form (which is incorporated into the Request for Special Privacy Protections form). The Response to Request for Special Privacy Protections form will be sent to the patient by mail.
6. If the request is granted, the privacy officials will place one copy of the Request for Special Privacy Protections in the patient's medical record under a separate tab. A colored label will also be affixed to the front of the chart to alert staff to the restriction. Where appropriate a note will be made on the actual location of protected health information. A second copy will be filed in this organization's HIPAA Compliance file.
7. If the request is granted, the privacy officials will meet with the appropriate workforce members to ensure that the request is implemented in their operational activities.

8. If the request is granted, this practice will not use or disclose the patient's health information in violation of the agreed upon restriction. However, if the patient is in need of emergency medical treatment, the restricted health information may be used and disclosed as necessary to provide the emergency treatment. In addition, the restriction will not prevent this practice from making any disclosure that is required by the Secretary of DHHS to determine our compliance with the Privacy Rule, any use or disclosure for purposes of our facility directory, or any use or disclosure that does not require the patient's authorization or an opportunity for the patient to agree or to object.
9. The privacy officials will only act on requests that are documented in writing. The privacy officials will require the patient to complete a new Request for Special Privacy Protections for any new or additional requests.
10. The patient may terminate a restriction at any time. All patient requests to terminate a restriction will be referred to the privacy officials. This practice may also terminate a restriction by notifying the patient of the termination. The patient may be notified orally. The termination will be effective only with respect to health information that is created or received after the patient is informed of the termination, unless the patient agrees to the termination in writing or the patient agrees orally and the patient's agreement is documented.
11. The privacy officials will document any termination of restrictions on the original Request for Special Privacy Protections form and notify workforce members as appropriate.

## ***Procedure: Workforce training and awareness***

### **Actions to be taken for workforce training:**

1. The privacy officials will be responsible for establishing and maintaining a workforce training and awareness program. The privacy officials will identify the training resources appropriate for this organization.
2. The privacy officials will complete and maintain an up to date listing of staff and their job descriptions. Each job description will be mapped to appropriate policies and procedures.
3. The privacy officials will keep up to date a quick training reference guide using the PrivaPlan PowerPoint training materials and PrivaPlan Stat.
4. The privacy officials will conduct an initial HIPAA training on or around March 25, 2003 using the quick training guide.
5. New staff as well as temporary staff will have a basic orientation in the policies and procedures related to their job function.
6. New staff must complete training within two weeks of their start date.
7. The privacy officials will include a HIPAA awareness-training component in the monthly staff lunch hour meetings or other similar meeting.
8. If it is possible for the privacy officials to review patient privacy complaints with the workforce without unnecessarily disclosing patient identifying information, the privacy officials may do so as a part of the awareness training.
9. The privacy officials will maintain the Workforce Training Log.