Neera Agarwal-Antal, M.D.

HIPAA Policies and Procedures

HIPAA POLICIES & PROCEDURES

This packet includes the following HIPAA policies, procedures and model forms:

HIPAA GENERAL OPERATING POLICY

POLICY:

It is the policy of Dr. Neera Agarwal-Antal's physician practice ("Practice") to protect the privacy of patient health information in accordance with applicable state and federal privacy laws and regulations.

Privacy Officer

The Practice shall designate a Privacy Officer to develop and implement HIPAA policies and procedures and oversee compliance with the HIPAA Privacy Rule.

Policies and Procedures

The Privacy Officer shall oversee the Practice's HIPAA compliance program and shall develop and implement HIPAA policies and procedures necessary to ensure compliance with the HIPAA Privacy Rule.

Notice of Privacy Practices

The Practice shall provide a copy of its "Notice of Privacy Practices" to all individuals who present for care. The Notice shall also be posted in prominent areas where patients and visitors will see it, on the Practice's website (if any), and shall be available upon request.

Consents and Authorizations

A consent is *different* than an authorization. A consent is required by Ohio law. A consent form is typically signed by patients on admission and allows the Practice to release the patient's health information to third parties identified in the consent.

An authorization is a form created in the HIPAA Privacy Rule. HIPAA does not require that the patient sign anything (i.e. a consent) if the Practice is releasing the patient's health information for treatment, payment, or health care operations. However, if the patient's health information is going to be released for a purpose other than treatment, payment, or health care operations, the patient must sign an "authorization" form that contains certain statements required by the HIPAA Privacy Rule.

Ex: The Practice wishes to release patient health information to the patient's insurer for payment. The consent form signed by the patient upon admission allows for this release. A HIPAA authorization form is *not* required because the information is being released for payment purposes.

Ex: The patient requests that his or her health information be released to their employer. Since the information will be released to the employer for a reason other than treatment,

payment, or health care operations, a HIPAA authorization form is needed. Once this is signed by the patient, it is sufficient to satisfy the state law consent requirement.

Treatment, Payment & Health Care Operations

The Practice shall implement policies and procedures consistent with this rule allowing for the use and disclosure of patient health information for treatment, payment, or health care operations.

Authorizations

HIPAA requires that an individual sign an "Authorization Form" that contains certain required statements before the individual's health information can be used or disclosed for reasons other than treatment, payment, or health care operations. The Practice shall develop a model Authorization Form and policies and procedures necessary to comply with this requirement.

Business Associates

The Practice shall have Business Associate Agreements in place with all persons or entities that provide services for the Practice who need access to or will create patient health information. Examples of business associates include third party billing companies, shredding companies, collection agencies, consultants, legal counsel for the Practice, etc.

Training

The Practice shall train existing members of its workforce on the HIPAA Privacy Rule requirements and the Practice's policies and procedures related to the privacy of patient health information on or before April 14, 2003. New employees will receive HIPAA training as part of their orientation.

Safeguards

The Practice shall have appropriate administrative, technical, and physical safeguards in place to reasonably safeguard patient health information from intentional or unintentional unauthorized use or disclosure.

Complaints & Reporting

The Practice shall implement a policy and procedure giving individuals the ability to make complaints concerning potential violations of their privacy rights and providing workforce members with a process for reporting potential privacy violations.

Sanctions

The Practice shall discipline workforce members who fail to comply with the HIPAA Privacy Rule and related policies and procedures.

Minimum Necessary

The Practice shall make reasonable efforts to limit the use and disclosure of patient health information to the minimum necessary amount to accomplish the purpose of the use, disclosure or request.

Access, Amendments & Accountings

The Practice shall implement policies and procedures to allow individuals access to their health information for inspection and/or copying, to make amendments to their medical record, and to receive an accounting of the disclosures of their health information.

Definitions

The following terms are used in the HIPAA policies and procedures and have the meaning ascribed to them below:

HIPAA Privacy Rule means the privacy provisions the Health Insurance Portability and Accountability Act of 1996 (HIPAA) found in 45 CFR Parts 160 and 164.

Patient Health Information means health information that identifies an individual, is transmitted or maintained in any form, and is protected from improper use or disclosure under the HIPAA Privacy Rule.

Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.

Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.

Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Personal Representative means a person who has the authority under applicable law to make health-care related decisions for an individual.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Practice is under the direct control of the Practice regardless of whether they are paid by the Practice.

Minimum Necessary means the minimum necessary amount of patient health information to accomplish the purpose of the use, disclosure or request.

Psychotherapy notes are notes by a health care provider who is a mental health professional documenting his or her discussions with the patient during a counseling session that *are separated from* the rest of the patient's medical record. These notes generally capture the therapist's impressions.

AUTHORIZATION TO USE OR DISCLOSE HEALTH INFORMATION

POLICY: The Practice shall obtain a HIPAA Authorization Form signed by the individual or his or her legal representative before using or disclosing the individual's health information for purposes other than treatment, payment, or health care operations.

PROCEDURE:

1. Authorization Needed. Complete the HIPAA "Authorization for Release of Information" form before using or disclosing patient health information for reasons other than treatment, payment or health care operations. Have the individual or his or her legal representative sign the form.

   Psychotherapy Notes. An authorization is also needed to release psychotherapy notes, except as follows:

   a. For the use by the originator of the notes.

   b. Use or disclosures by the Practice in training programs in which trainees in mental health learn to improve their counseling skills.

   c. Use to defend a legal action brought by the patient who is the subject of the notes.

   d. When required by the Secretary of Health and Human Services.

   "Psychotherapy notes" are notes by a health care provider who is a mental health professional documenting his or her discussions with the patient during a counseling session that *are separated from* the rest of the patient's medical record. These notes generally capture the therapist's impressions.

2. Form Requirements. The "Authorization for Release of Information" form contains language required by the HIPAA Privacy Rule. Thus, it may not be revised without consulting risk management or legal counsel. The form must be completed in its entirety, dated, and signed by the patient or his or her legal representative.

3. You must provide a copy of the signed authorization to the patient/legal representative.

4. The authorization form may not be combined with another other document.

5. A patient may revoke his or her authorization at any time in writing. When the authorization is revoked, you must stop making further uses and disclosures pursuant to the authorization.

6. HIPAA requires that you retain signed authorization forms for at least 6 years from the date signed, or the date last in effect, whichever is later.

7. You cannot deny a patient treatment on the basis of his or her refusing to sign an authorization.

8. No Authorization Needed. You do not need patient authorization for the following uses or disclosures:

   a. Disclosures for treatment, payment, or health care operations. For example, you do not need patient authorization to release medical information to the patient's physician or insurance company paying the medical bills (except for psychotherapy notes).

   b. Disclosures required by state or federal law.

   c. Disclosures to public health agencies and health oversight agencies.

   d. Disclosures to authorities for abuse, neglect, and domestic violence.

   e. Disclosures for judicial and administrative proceedings, law enforcement purposes, coroners, and medical examiners.

   f. Disclosures to organ donation procurement agencies.

   g. Disclosures for workers' compensation.

   h. Disclosures to avert serious threats to public health or safety.

   i. Disclosures to family and friends directly involved in the patient's care.

AUTHORIZATION FOR RELEASE OF INFORMATION

I hereby authorize the use or disclosure of my health information as described below. I understand that this authorization is voluntary and I may refuse to sign it. I understand that the information used or disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and no longer protected by the federal privacy regulations.

Patient name: _____ ID Number (if known): _____

Date of Birth: _____

Title and name of person releasing my health information:

_____

Person(s) receiving my health information [Example: "My employer"]:

_____

Description of information being disclosed for the following date(s) of service: _____
_____

[ ] Complete Health Record
[ ] History and Physical Exam
[ ] Progress Notes
[ ] Radiology Reports
[ ] Abstract/Pertinent Information
[ ] HIV/AIDS information
[ ] Drug and Alcohol treatment information
[ ] Other: _____
[ ] Discharge Summary
[ ] Consultation Reports
[ ] Laboratory Tests
[ ] Emergency Department Record

Purpose of the Disclosure [Example: "At the request of the patient"]:
_____

Expiration: If the health information to be disclosed contains HIV/AIDS or drug and alcohol abuse treatment records, this authorization expires in 60 days. Otherwise, you may select either of the following expiration events:

[ ] 1 year from the date in which I, or my legal representative, signs this authorization;

[ ] upon the happening of the following event: _____
_____ [Example: "Upon release of the above records"].

Right to Revoke: I understand that I may revoke this authorization at any time by providing written notice to the Privacy Officer at 1325 Corporate Drive, Suite A, Hudson, Ohio 44236. I understand that my revocation won't have any affect on any actions taken by the organization before they received the revocation and is not effective if the authorization was obtained as a condition of obtaining insurance coverage and the insurer has the legal right to contest a claim under my insurance policy.

I understand that the organization will not condition my treatment, payment, enrollment in a health plan, or eligibility for benefits on my signing this authorization.

I understand that I have the right to inspect or copy the health information to be used or disclosed pursuant to this authorization.

TO BE COMPLETED BY THE ORGANIZATION IF THIS AUTHORIZATION IS FOR MARKETING: The organization will receive financial or in-kind compensation in exchange for using or disclosing the health information described above: Yes _____ No _____.

_____ _____

Signature of Patient or Legal Representative Date

If signed by the patient's legal representative:

Printed Name of representative: _____

Relationship to the patient: _____

- PROVIDE COPY TO THE PATIENT AND MAINTAIN A COPY IN THE PATIENT'S RECORD -

PATIENT'S RIGHT TO ACCESS AND/OR COPY HEALTH INFORMATION

POLICY: The Practice shall afford individuals the right to access, inspect, and obtain a copy of their health information in accordance with the provisions of the HIPAA Privacy Rule.

PROCEDURE:

1. Request for Access and/or Copying Form. An individual who seeks to access and/or copy his or her health information, must complete the form entitled "Patient's Request to Access and/or Copy Health Information" and submit it to the Privacy Officer. The individual can obtain the form from the Privacy Officer.

   The completed form should be forwarded to the Privacy Officer who will then decide whether to grant or deny the individual's request in accordance with the rules set forth in this policy.

2. The Privacy Officer shall respond to the request within 30 days if the information sought is on-site and 60 days if the information is off-site. The Privacy Officer may extend the deadline once for no more than 30 days by providing the patient with a written statement of the reasons for the delay and the date in which the Privacy Officer will complete the request.

   The Privacy Officer will notify the individual of where to direct his or her request for access if the Practice does not maintain the information sought but knows where it can be obtained.

3. Granting Access. If the Privacy Officer grants access, he or she will provide the individual with access to the records in the form requested (unless not producible in such a form) and the chance to copy the records. The Privacy Officer may provide the individual with a summary of the information requested if the individual agrees in advance to this method and the fees associated with the summary.

4. Denying Access

   The patient/legal representative is entitled to written notice of a denial. The patient/legal representative may request a review of some denials, others are not reviewable.

   a. Unreviewable - An individual has no right to access the following information and the Privacy Officer does not have to provide the individual with a chance for review:

      i. Psychotherapy notes (if denying for this reason, first consult with the Privacy Officer)

      ii. Information compiled in anticipation of civil, criminal, or an administrative action or proceeding.

iii. Health information that is subject to CLIA to the extent the provision of access to the individual would be prohibited by law.

iv. Health information that was obtained from another person (other than a health care provider) under a promise of confidentiality and granting access would likely reveal the source's identity.

b. Reviewable – The Privacy Officer may deny access for the following reasons but must give the individual a chance to seek a review of the denial:

i. A physician chosen by the Practice has determined that access is likely to endanger the life or safety of the patient or another individual.

ii When the health information sought makes reference to another person and a physician chosen by the Practice determines that access is likely to cause harm to that person.

iii. When the request for access is made by a personal representative and a physician chosen by the Practice determines that providing access to the representative is likely to cause harm to the patient or another person.

If the patient/legal representative requests a review, a physician chosen by the Practice who was not involved in the original denial must determine, within a reasonable period of time, whether the denial was proper and provide written notice to the determination to the requestor.

c. Denial Notice - If you deny access *for any reason*, you must provide the patient with a written denial using the form entitled "Response to Patient's Request to Access and/or Copy Health Information," which includes (a) the basis for the denial, (b) a statement of the individuals right to have the denial reviewed and how such right may be exercised, and (c) a description of how the individual can file a complaint with the Practice and the Secretary of Health and Human Services. The description must include the name (or title) and telephone number of the person or office responsible for receiving complaints.

5. You must document and retain (a) the records that are subject to access and (b) the title of the person or office responsible for processing the request for access for 6 years.

PATIENT'S REQUEST TO ACCESS AND/OR COPY HEALTH INFORMATION

Please complete the following:

1. Name of Requestor (print): _____

   Patient name (if different): _____

   Patient's birth date: _____
2. Address: _____
3. Phone: _____
4. If you are not the patient, your relationship to the patient: _____

   _____
5. Do you wish to [ ] access (e.g. review) the health information, [ ] a copy of the health information or [ ] both.
6. Describe the information you want to access (e.g., lab test results, physician notes): _____

   _____
7. Identify the date(s) of information you want access to (e.g., date of office visit, treatment, or other health care services): _____

   _____

There is no charge to access your health information. If you would like a copy of the information, we will charge a reasonable fee for the copying, postage, and to prepare a summary (if you request a summary). We will inform you by [ ] phone [ ] letter (pick one) of the cost of your copy before we make the copy and verify that you agree to pay for the copy. We will require you to pay for your copy before you receive it. We will notify you in writing within 30 days of your request (60 days if the health information requested is not maintained or accessible on-site) if and when your health information will be available for access, where you will need to come to access your health information to read and review it, or where to come to pay for and pick up your copy. We will notify you within 30 days if we need one additional period of 30 days to respond to your request. In specific circumstances, we may deny access to your health information, or to a portion of your health information. If we deny access we will return this form to you with our written reasons for our denial and explain your right to review the denial, if applicable. The Practice reserves the right to supervise your access.

_____ _____

Signature of patient or legal representative Relationship to the patient

Date: _____

- Submit this request form to the Privacy Officer -

RESPONSE TO PATIENT'S REQUEST TO ACCESS AND/OR COPY HEALTH INFORMATION

Your request to [] access, [] copy, or [] both access and copy your health information is:

[ ] **Approved.** Your health information will be available for access on _____ _____ between the time of _____.

[ ] A copy of your health information will cost $_____ plus postage if we mail the copy to you. If you wish to have the information mailed to you, please send a check or money order for $_____ to _____. You may save the postage cost by picking up your copy on the date and time listed above. Please bring a check or money order for the copying costs.

[ ] **Denied**

[ ] Your request was denied because the health information sought includes the following information that is exempt from access. You may not seek a review of the denial.

[ ] Psychotherapy notes;

[ ] Information that was compiled in anticipation of, or for use in, civil, criminal or administrative legal actions or proceedings;

[ ] Health information that relates to the Clinical Laboratory Improvement Amendments of 1988 (CLIA), to the extent that CLIA would prohibit individual access, or other information that is exempt from CLIA.

[ ] The health information was obtained from another person (other than a health care provider) under a promise of confidentiality and granting access would likely reveal the source's identity.

[ ] Your request was denied because the health information you sought was reviewed by a physician chosen by the Practice who determined that the following circumstances exist:

[ ] Access is reasonably likely to endanger the life or safety of the patient or another person.

[ ] Access is reasonably likely to cause substantial harm to another person.

[ ] Access is sought by the patient's legal representative and access is reasonably likely to cause substantial harm to the patient or another person.

If your access request was denied for one of these three reasons, you may seek a review of the decision by submitting a written request for review to the Privacy Officer of Medical Record. The Privacy Officer will provide you a written answer within 30 days.

[ ] **Extension of Deadline.** The Practice will require an additional 30 days to process your request.

Reason for extension:_____

Your health information will be available for access and/or copying on _____ _____ between the time of _____.

Complaints. If you disagree with our decision concerning access to your health information, you may send a written complaint to our Privacy Officer at 1325 Corporate Drive, Suite A, Hudson, Ohio 44236 or call the Privacy Officer at 330-650-4200. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services at 200 Independence Avenue, SW, Washington D.C. 20201 or call 1-877-696-6775. There will be no retaliation for filing a complaint.

Privacy Officer Signature: _____

Date: _____

RIGHT TO AN ACCOUNTING

POLICY: Upon request, the Practice shall provide individuals with an accounting of the uses and disclosures of their health information in accordance with the HIPAA Privacy Rule.

PROCEDURE:

1. A patient has the right to receive an accounting of disclosures of his or her health information made in the 6 years prior to the date on which the patient requests the accounting. The Privacy Officer shall handle all requests for an accounting. Patients must request an accounting in writing by completing the Request for Accounting form and submitting it to the Privacy Officer.

2. The Privacy Officer does <u>not</u> need to account for the following disclosures:

    a. Disclosures occurred prior to April 14, 2003.
    b. Disclosures for treatment, payment or health care operations.
    c. Disclosures made pursuant to the patient's authorization.
    d. Disclosures made to the patient.
    e. Disclosures to family or friends involved in the patient's care.
    f. Disclosures that are incidental to an otherwise permitted disclosure.
    g. Disclosures for national security or intelligence purposes.
    h. Disclosures to correctional institutions or law enforcement officials.
    i. Disclosures pursuant to a limited data set.

3. Examples of disclosures that must be accounted for include:

    a. To a governmental authority required by law for abuse, neglect or domestic violence.
    b. For health oversight activities required by law to audit and investigate.**
    c. To a governmental authority required by law for child abuse or neglect.
    d. To a law enforcement official concerning crime victims or criminal conduct.**
    e. To a coroner or medical examiner required by law for a decedent.
    f. To a public authority required by law for disease reporting.
    g. To an employer, where we have been requested by the employer to conduct an evaluation of the patient.
    h. To the Food and Drug Administration.
    i. To a public health authority required by law to collect information regarding injury or disability (trauma, gunshot).
    j. For organ procurement.
    k. For research purposes (except if the patient signed an authorization).
    l. Pursuant to a subpoena, discovery request, or a court order.
    m. For aversion of threats to public health or safety.
    n. For administration of the Department of Veterans Affairs.
    o. To a public health authority required by law to collect vital statistics.

*Please note that disclosures pursuant to #3(a)-(o) do not need to be included in an accounting if the patient signed an authorization for the disclosure.

**If you are disclosing a patient's health information to law enforcement officials or a health oversight agency and the agency or official provides you with a statement indicating that disclosure in the accounting would impede their investigation, you must *exclude* this disclosure from your accounting.

4. An accounting must include the following information:

   a. The date of the disclosure.
   b. The name of the entity or person who received the patient's health information and, if known, their address.
   c. A brief description of the health information disclosed.
   d. A brief statement of the purpose of the disclosure that informs the patient of the basis for the disclosure, or, in lieu of this statement, a copy of the written request for a disclosure from the patient.

5. You must provide an accounting no later than 60 days after receiving the patient's request. If you cannot meet the 60-day deadline, you may extend the deadline by 30 days if you inform the individual of the extension in writing within the original 60-day deadline. Your extension notice must state the reason for the delay and the date in which you will provide the requested accounting. You may only extend the deadline once.

6. The first accounting in any 12 month period must be provided free of charge. You can charge a reasonable fee for a subsequent accounting in the same period.

7. For 6 years, you must document and retain the information included in the accounting to an individual, a copy of the written accounting that was provided to the individual, and the title of the person or office responsible for receiving and processing the accounting.

8. You can deny a request for an accounting when made by the personal representative of a patient if:

   a. The patient has been or may be subject to domestic violence, abuse, or neglect by the person requesting the information and the accounting could endanger the patient; or

   b. The Privacy Officer decides that it is not in the best interest of the patient to treat the person as the patient's representative.

REQUEST FOR ACCOUNTING

You have the right to receive an accounting of certain disclosures of your health information. Please complete the following information so that we may process your request.

Patient Name _____

Address to receive accounting _____
_____

Home telephone number _____

Period of time requested._____

The following disclosures of your health information will not be provided in an accounting to you:

- Disclosures made pursuant to an authorization signed by you or your representative;
- Disclosures to carry out our own or other providers' treatment, payment and health care operations;
- Disclosures made to you or your personal representative;
- Disclosures made to persons involved in your care or notification of next-of-kin or family members;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials about inmates or others in custody; or
- Disclosures that occurred prior to April 14, 2003.
- Disclosures pursuant to a limited data set.

If you request more than one accounting in any 12 month period, we will charge you a reasonable fee for the accounting.

Name of Person Requesting the Accounting (print): _____

Signature: _____

Date: _____

If personal representative, your relationship to patient: _____

HIPAA PRIVACY TRAINING

POLICY: The Practice will train all new and existing workforce members (which includes volunteers and students) on the requirements of the HIPAA Privacy Rule and related policies and procedures. The Privacy Officer will develop and implement the training program.

PROCEDURE:

1. The Privacy Officer shall provide HIPAA training for all existing members of the workforce by April 14, 2003 and new members of the workforce upon their initial orientation.

2. Workforce members are required to sign the "HIPAA Training and Confidentiality Pledge" indicating that they have received HIPAA privacy training and agree to protect the confidentiality of patient health information. Documentation of the type, amount, and date the training will be retained for six years.

HIPAA TRAINING AND CONFIDENTIALITY PLEDGE

I acknowledge that, on the date below, I received training on the HIPAA Privacy Rule and the Practice's policies and procedures for preserving the privacy of patient health information.

I understand that I am to consider all patient health information strictly confidential and shall not use or disclose such information in any manner contrary to the HIPAA Privacy Rule or the Practice's policies and procedures.

I further understand that I may be subject to discipline, including termination of employment, if I improperly use or disclose patient health information.

Name of Workforce Member:_____

Signature: _____

Date: _____

NOTICE OF PRIVACY PRACTICES POLICY

POLICY: To provide individuals with written notice of the permitted uses and disclosures of their health information, their rights with respect to the information, and the Practice's duties to comply with the HIPAA Privacy Rule and preserve the confidentiality of such information.

PROCEDURE:

1. All patients will be given a copy of the Practice's model "Notice of Privacy Practices" on their first service date. The Notice shall also be available for individuals upon request.

2. The Practice will post the Notice prominently in places individuals will to see the Notice, such as admitting, registration, and waiting areas.

3. All patients receiving a copy of the Notice will be asked to sign an acknowledgement of their receipt of the Notice. Acknowledgements will be retained for at least 6 years. If you are unable to obtain the patient's written acknowledgment, do document your efforts to do so and the reason why the acknowledgement could not be obtained.

4. If your Practice maintains a website, the Notice will be posted on the website and made available electronically through the website.

5. The model Notice of Privacy Practices contains language that is required by law. Do not revise the Notice without consulting risk management and legal counsel.

6. The Notice will indicate that all complaints will be forwarded to the Privacy Officer.

7. If the Notice is revised, the Practice will make the revised notice available upon request and will post it in a clear and prominent location where it is reasonable to expect individuals to see it.

BUSINESS ASSOCIATE POLICY

POLICY: To secure business associate contracts with all persons or entities that provide services for the Practice who will have access to patient health information. Business associate agreements are required by HIPAA to ensure that the business associate takes appropriate steps to safeguard patient health information.

PROCEDURE:

1. Identify business associates. Complete the appropriate fields of the model Business Associate Agreement for each business associate and obtain a signed agreement. If you are unsure whether a Business Associate Agreement is needed, contact the Privacy Officer for guidance. Examples of business associates include a collection agency, billing company, consultants, accrediting body, legal counsel, JCAHO, etc.

2. A Business Associate Agreement is NOT required for disclosures to:

    a. Treatment providers involved in the patient's care are <u>not</u> considered business associates and therefore no business associate contract is necessary. Example: a hospital lab that is performing laboratory testing for the Practice's patients.

    b. Health plans for payment.

    c. Employees, students, and other members of your workforce.

    d. Janitorial, housekeeping staff (since they are not expected to have access to patient health information as part of their job duties).

3. The model Business Associate Agreement contains statements that are required by law. Changes to the Agreement must be approved by the Practice's legal counsel.

4. Business Associate Agreements must be in place by April 14, 2003 except as follows:

    a. If you have a written contract in place before October 15, 2002 it will be deemed in compliance until it is revised or until April 14, 2004, whichever is sooner.

    b. Contracts with automatic renewals must be amended to include a Business Associate Agreement when revised, or by April 14, 2004, whichever is sooner.

5. In you learn that a business associate is misusing patient health information, you must report the violation to the Privacy Officer. The Privacy Officer will contact the business associate to take steps to cure the violation. If the steps are unsuccessful, the Privacy Officer will terminate the Business Associate Agreement or, if it cannot be terminated, contact the Secretary of HHS.

RIGHT TO AMEND HEALTH INFORMATION

POLICY: Individuals will have the right to amend their protect health information in accordance with the HIPAA Privacy Rule as described in this policy.

PROCEDURE:

1. Role of Privacy Officer. If a patients requests to amend his or her medical records, he or she should complete the "Request for Amendment" form and submit it to the Privacy Officer. The Privacy Officer is responsible for receiving and processing requests for amendments.

2. The Privacy Officer shall decide whether to grant or deny the request within 60 days of receiving the request. If are unable to do so in this time period, the Privacy Officer may extend the deadline once by 30 days by providing written notice to the individual of the reason for the delay and when the request will be completed.

   The Privacy Officer shall consult with the Privacy Officer if unsure as to whether to grant or deny a request for amendment.

3. The Practice is not required to delete information contained in the medical record. It may attach information as necessary to ensure that the record is accurate and complete.

Denying a Request to Amend

1. The Privacy Officer may deny an individual's amendment request if:

   a. The individual's health information is accurate and complete.
   b. The individual's health information is not part of the hospital record.
   c. The individual's health information was not created by the Practice, unless the patient provides you with the basis to indicate that the originator of the health information is no longer available to act on the request for amendment.
   d. The individual's health information is not available for inspection under the rules allowing a patient access to his or her information (such as psychotherapy notes).

2. Denial Notice - If the Privacy Officer denies a request, he or she must provide the individual with a written denial indicating:

   a. The reason for the denial;
   b. The individual's right to submit a written statement of disagreement with the denial and how to file the statement;
   c. A description on how the person can file a complaint with the Practice (including the title and telephone number of the person responsible for processing complaints) and the Secretary of Health and Human services; and

d. A statement that, if the individual does not submit a statement of disagreement, he or she may ask that you include their request for amendment and the denial with future disclosures of their health information.

4. Statement of Disagreement - If the individual files a statement of disagreement, the Privacy Officer may prepare a written rebuttal and send a copy to the individual. The Privacy Officer must identify the record that is subject to the dispute, attach the patient's request for the amendment, the denial notice, the statement of disagreement, and rebuttal (if any), and forward this information with subsequent disclosures.

5. If the request for amendment is denied and the patient does not file a statement of disagreement, you do not need to include the request for amendment and denial with subsequent disclosures unless the patient requests.

Granting a Request to Amend

1. To amend the record, attach the Request for Amendment form to the applicable portion of the medical record being amended. Notify the individual that the amendment has been accepted within the 60-day timeframe and make efforts to obtain the individual's agreement to contact the following persons or entities concerning the amendment:

   a. Persons identified by the individual as having health information needing amendment; and
   b. Persons, including business associates, that you know to have patient health information that is subject to the amendment.

REQUEST FOR AMENDMENT

The Practice is not required to delete information contained in the medical record. Please complete the following:

1. Date _____
2. Patient name _____
3. Address _____
4. Birth Date _____
5. Please describe the information you want amended (e.g., lab test results, physician notes)

   _____

   _____

   _____

   _____

6. Date(s) of information you want amended (e.g., date of office/clinic visit, treatment, or other health care services) _____

   _____

7. State your reason for making this request? _____

   _____

   _____

   _____

8. Describe how the entry is incorrect, incomplete, or outdated? _____

   _____

   _____

9. What should the entry say to be more accurate or complete? _____

   _____

   _____

10. Do you know of anyone who may have received or relied on the information in question such as your doctor, pharmacist, health plan, or other health care provider? yes no

    If yes, please specify the name(s) and address(es) of the organization(s) or individual(s)

    _____

    _____

11. If your request for amendment is granted, do you give us permission to contact the persons identified in item 10 above so that they may amend the information also?

yes no.

Name of Person Requesting Amendment (print): _____

Signature: _____

Date: _____

If personal representative, relationship to patient: _____

Patient: Please forward this Request to the Privacy Officer

****

FOR PRACTICE USE ONLY

Amendment has been: [ ] Accepted [ ] Denied

If denied, check the reason(s) for denial:

[ ] the health information was not created by this organization.

[ ] the health information is not part of the patient's record.

[ ] the law forbids making the health information in question available for inspection (e.g., psychotherapy notes).

[ ] the health information is accurate and complete.

Comments _____

_____

_____

Privacy Officer's Signature: _____ Date _____

Privacy Officer: Attach this form to the portion of the medical record being amended & provide a copy to the patient.

VERIFICATION POLICY

POLICY: To establish reasonable means to verify the identity and authority of an individual requesting access to a patient's health information.

PROCEDURE:

1. If the identity or authority of a person requesting patient health information is not known, you must verify their identity and authority and document your actions.

   Exceptions: You do not need to verify the identity of a family member or friend involved in the patient's care.

2. The requestor's identity can be verified by knowing the requestor or by asking for his or her driver's license, passport, or state identification card with photograph. If the request is made by fax or phone, call the requestor back from the main switchboard.

3. The requestor's authority can be verified by, for example, obtaining a copy of a power of attorney, or court guardianship papers, or asking questions to determine that an adult acting for a young child has the requisite relationship to the child.

4. Public Officials

   Identity - You may rely on the following information to verify the identity of a public official seeking patient health information:

   a. If the request is made in person, the requestor provides an ID badge, official credentials or other proof of government status.

   b. If the request is in writing, the letter is written on the appropriate governmental letterhead.

   c. If the disclosure is to a person acting on behalf of a public official, their identity may be verified by a written statement on government letterhead that the person in acting on the government's behalf or other documentation establishing the same.

   Authority - You may rely on the following information to verify the authority of a public official seeking patient health information (a) a written or oral statement of the official's authority to request the information; or (b) if the request is made pursuant to a subpoena, order, warrant of other legal process you may presume authority.

MINIMUM NECESSARY POLICY

POLICY: It is the policy of the Practice that all uses and disclosures of patient health information shall be limited to that which is reasonably necessary to accomplish the intended purpose of the use or disclosure, unless otherwise permitted by law.

PROCEDURE:

1. The Privacy Officer shall identify the persons, as appropriate, who need access to patient health information to carry out their duties and the types of health information to which access is needed. The following types of uses are not subject to the minimum disclosure requirements:

    a. Uses to prepare information to give to a patient or to the patient's representative.
    b. Uses and disclosures that the patient has authorized in a signed Authorization Form.
    c. Disclosures to another treatment provider.
    d. Disclosures to another covered entity for non-treatment purposes.
    e. When disclosure is requested by a business associate who represents that the information is the minimum necessary.
    f. Disclosures to public officials who represent that the information sought is the minimum necessary.
    g. Disclosures to the Secretary of HHS for compliance or enforcement activities.
    h. Disclosures for any purpose required by law.

    Contact the Privacy Officer for guidance if you are in doubt about when the minimum necessary standard applies.

2. Each determination of what information constitutes the minimum necessary must be individually evaluated on a case-by-case basis to ensure that the information disclosed is the minimum necessary to accomplish the purpose of the disclosure. You may develop standard protocols for routine and recurring disclosures.

3. As a general rule, you may not disclose the patient's entire medical record except in those instances when the entire medical record is justified as the amount that is reasonably necessary.

COMPLAINT AND REPORTING POLICY

POLICY: To establish a process for individuals and workforce members to make complaints regarding suspected privacy violations. The intent of this policy is to promptly resolve complaints and mitigate the harmful effects of any privacy violation.

PROCEDURE:

1. Role of Privacy Officer. The Privacy Officer is responsible for receiving and investigating all suspected privacy violations. The Privacy Officer shall log all complaints on a complaint log indicating the date, time, name of the individual making the complaint, and a description of the complaint. The Privacy Officer shall investigate the complaint and take all appropriate steps to mitigate the effects of any privacy violation. The Privacy Officer shall notify the individual who made the complaint of the outcome of the investigation and how the complaint was resolved.

2. Notice of Privacy Practices. The Practice's Notice of Privacy Practices shall inform individuals of how to file complaints with the Privacy Officer and/or the Secretary of HHS.

3. Documentation. The Privacy Officer shall document all complaints, their resolution, and any actions resulting from the complaint. The documentation must be retained for a minimum of 6 years from the date of the final resolution.

4. No Retaliation. At no time shall any individual who makes a complaint to the Privacy Officer be retaliated against.

How to file a Complaint

1. Individuals should file a privacy complaint using the "Reporting Form for Privacy Violations." The form should be submitted to the Privacy Officer. The form allows the complainant to remain anonymous and may be placed in the anonymous reporting box for privacy violations. However, individuals may make complaints directly to the Privacy Officer in accordance with the complaint process in the Notice of Privacy Practices.

2. The Privacy Officer will educate workforce members of their reporting obligation and how to file a complaint.

REPORTING FORM FOR PRIVACY VIOLATIONS

Name: _____ (unless you wish to remain anonymous)

Date: _____

Are you a patient [ ], member of the workforce [ ], or other [ ]. If other, please describe:
_____

Description of possible violation:_____
_____
_____

When did this occur?_____

Person(s) involved:_____

How did you come to learn of the incident?_____
_____

Do you have any evidence to prove the above allegations? If so, please describe?
_____
_____

Would you be willing to discuss the above allegations with the Privacy Officer? YES NO
If yes, what is the best way to contact you: _____
_____

Have you discussed the above allegations with anyone else? If so, who?
_____

Do you have any further information to provide or any suggestions for verifying the allegations described above? _____
_____

Are you aware of any other individuals who may be able to provide further information regarding the above allegations? If so, who?
_____
_____

Please forward this form to the Privacy Officer or place in the Anonymous Reporting Box for suspected privacy violations.

DISCIPLINARY POLICY FOR PRIVACY RULE VIOLATIONS

POLICY: The Practice shall take appropriate disciplinary action against members of the workforce (employees, volunteers, trainees, etc.) who fail to comply with the HIPAA Privacy Rule and the Practice's policies and procedures for protecting the confidentiality of patient health information.

PROCEDURE:

1. During their HIPAA training sessions, workforce members will be made aware of the potential sanctions for violating HIPAA policies and procedures, including possible termination.

2. The employee may be subject to discipline, taking into account:

    a. the severity of the violation.

    b. whether the violation was accidental or intentional.

    c. whether the violation was part of a pattern of violations.

    d. the Practice's standard disciplinary process.

3. Disciplinary action may range from a verbal warning to termination.

4. A workforce member who reports suspected HIPAA violations to a governmental agency, accreditation organization, an attorney, or other agency or body under applicable whistleblower laws or regulations will not be disciplined for making the report.

SAFEGUARDING PATIENT HEALTH INFORMATION
(To be developed)

The HIPAA Privacy Rule requires that you have in place appropriate administrative, technical, and physical safeguards to protect the privacy of patient health information. The Privacy Rule does not identify the measures you must take to meet this standard. However, the rule does include examples such as, shredding documents, requiring doors to medical records departments to remain locked, and limiting the personnel who have permission to access patient health information.

This policy will have to be developed after consultation with the Practice's medical records and information systems personnel.

DISCLOSURE TO FAMILY AND FRIENDS

POLICY: To establish a process for disclosing patient health information to family members, relatives, or friends who are involved in the patient's care.

PROCEDURE:

1. If the patient is present (or otherwise available) and is capable of making decisions, you must obtain the patients agreement (can be oral), or provide the patient with an opportunity to object to the disclosure, or reasonably infer from the circumstances that the patient does not object to the disclosure.

2. If the patient is not present or capable of making decisions, the Practice must determine whether it is in the patient's best interest to disclose information to a family member or friend and disclose only that information that is relevant to that persons involvement in the patient's care.

3. Examples of acceptable disclosures include disclosures to relatives involved in the patient's care, disclosures to a friend concerning the patient's mobility if the friend is driving the patient home from the hospital.

4. If you suspect that an incapacitated individual is a victim of domestic violence and that the person seeking information about the individual may have abused the patient, do not disclose the information to the suspected abuser. Consult risk management or legal counsel.

FUNDRAISING USES AND DISCLOSURES

POLICY: The Practice shall limit the use and disclosure of patient health information for fundraising activities to that which is permissible under the HIPAA Privacy Rule as described in this policy.

PROCEDURE:

1. Fundraising means any appeal for money or other donations, sponsorship of events, etc. that is undertaken on behalf of the Practice.

3. No Patient Authorization Needed. The only information the Practice may use or disclose for fundraising activities is (a) the individual's demographic information (e.g. name, address, sex, age, and insurance status); and (b) the dates in which the individual received care. The Practice does not need to obtain the individual's authorization to use or disclose this information to a business associate or related foundation raising funds for the Practice:

   - A related foundation means a foundation that qualifies as a nonprofit charitable foundation under sec. 501(c)(3) of the Internal Revenue Code and that has in its charter statement of charitable purposes an express relationship to the Practice.

3. Patient Authorization Needed. If the Practice wishes to use or disclose an individual's health information for fundraising activities other than as described in #2 above, the Practice must first obtain a signed HIPAA Authorization Form from the individual specifically allowing the use or disclosure. All fundraising efforts under this Section #3 must be disclosed to the Privacy Officer before commencement.

4. Required Notice to Individual. The Practice's Notice of Privacy Practices shall include a statement that it may contact the individual to raise funds and how the individual can opt-out of receiving fundraising materials.

   The Practice will also include the following statement in any fundraising materials it sends to an individual of how the individual may opt-out of receiving further information.

   > You have the right to request that we not send you any future fundraising materials and we will use our best efforts to honor such request. You may make the request by sending your name and address to the Practice's Privacy Officer together with your request to be removed from our fundraising mailing and contact lists.

5. The Practice shall not send any fundraising materials to an individual who has indicated that he or she does not want to receive this information (e.g. opted-out).

MARKETING USES AND DISCLOSURES

POLICY: The Practice shall limit the use and disclosure of patient health information for marketing activities to that which is permissible under the HIPAA Privacy Rule.

PROCEDURE:

1. Marketing means a communication about a product or service that encourages recipients to purchase or use the product or service.

2. General Rule - Authorization is Required. The Practice may not use or disclose an individual's health information for marketing unless the individual first signs a HIPAA Authorization Form specifically allowing the use or disclosure.

3. Exceptions – When Authorization is not Required. Patient authorization is not required for two types of marketing:

   a. Face-to-face disclosures.
   b. A promotional gift of nominal value provided by the Practice.

   Patient authorization is also not required to make the following communications to individuals because they are not considered marketing:

   a. Communications about a participating provider and health plans in a network, the services offered by a provider, or the benefits covered by a health plan.

   b. Communications about the individual's treatment.

   c. Communications about case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual.

RESEARCH USES AND DISCLOSURES

The rules for use and disclosure of patient health information for research purposes are complex and offer various options for the health care provider. Consultation with the health care provider is necessary to determine which option it prefers and draft the policy accordingly.

DISCLOSURES TO PERSONAL REPRESENTATIVES

POLICY: To allow for disclosures of patient health information to the patient's personal representative as permitted under the HIPAA Privacy Rule.

PROCEDURE:

1. Personal representatives include individuals designated as the patient's attorney-in-fact under a durable power of attorney for health care, parent (or guardian) of a minor, court-appointed guardian, or the executor or administrator of a deceased patient's estate.

2. The Practice shall treat a personal representative the same as the individual (e.g. patient) with respect to disclosing the individual's health information.

3. The Practice must verify the personal representatives identity and authority to act on behalf of the individual. See Verification Policy.

4. Abuse, Neglect and Endangerment Situations - Do not disclose an individual's health information to his or her personal representative if you have reason to believe that:

    a. the patient has been or may be subjected to domestic violence, abuse or neglect by the personal representative or treating such individual as the personal representative could endanger the patient; and

    b. you determine, in the exercise of professional judgment, that it is not in the best interest of the patient to treat the individual as the patient's personal representative.

RIGHT TO REQUEST RESTRICTIONS

POLICY: To allow patients to restrict the use or disclosure of their health information in accordance with the HIPAA Privacy Rule.

PROCEDURE:

1. An individual has the right to request a restriction on the use or disclosure of his or her health information (a) for treatment, payment, or health care operations, and (b) disclosures to family and friends involved in the individual's care.

2. When an individual requests a restriction, the person receiving the request (ex: nurse, admission personnel, etc) should complete the "Request for Restrictions" form and obtain the individual's signature. Place the completed form in the patient's medical record. For new admissions, include the signed Request for Restrictions in the admission packet sent to the unit.

3. All reasonable requests for restrictions shall be honored, except that the individual may not restrict information disclosed to the Department of Health and Human Services for compliance purposes and other disclosures required by law.

4. In emergency situations, where the individual needs emergency care and the restricted information is needed to provide the care or disclose information to another health care provider, you do not have to follow the agreed-upon restrictions. If restricted information is disclosed to a health care provider for emergency treatment, you must request that the health care provider not further use or disclose the information.

5. You may terminate a restriction if:

    a. the individual agrees or requests the termination in writing; or
    b. the individual orally agrees to the termination and the oral agreement is documented; or
    c. you inform the individual that you are terminating its agreement to a restriction, except that the termination is only effective with respect to health information received after you have informed the individual.

6. Document and retain agreed-upon restrictions (in written or electronic form) and an individual's oral agreement to terminate a restriction for 6 years from the date created or last date of use, whichever is later.

7. <u>Denying Restrictions</u>. If, within your professional judgment, a request for restriction should be denied, please contact the Privacy Officer for guidance. If denied, please notify the individual requesting the restriction of the denial.

REQUEST FOR RESTRICTIONS

Please indicate below the restrictions you are requesting on the use and disclosure of your health information. We do not have to honor the request. If we agree to the restriction, we are bound to follow it. If we deny the restriction, we will notify you of the denial.

Requested Restriction:

_____

_____

_____

_____

Print Name: _____

Signature: _____

Date: _____

If legal representative, relationship to patient: _____

****

FOR PRACTICE'S USE ONLY:

Restriction Accepted [ ], Denied [ ].

Signature: _____

Date: _____

-Place this form in the patient's medical record-

DISCLOSURES TO HEALTH OVERSIGHT AGENCIES

POLICY: To allow for the disclosure of patient health information to agencies involved in health oversight activities as permitted or required by the HIPAA Privacy Rule.

PROCEDURE:

1. Contact the Privacy Officer if you receive a request for patient health information from a health oversight agency.

2. The Privacy Rule allows you to disclose patient health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of the health care system.