

# HIPAA NOTICE OF PRIVACY PRACTICES

## Nebraska Orthopedic Associates, LLP

**Effective Date: April 14, 2003**

**THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION**

### **PLEASE REVIEW IT CAREFULLY**

If you have any questions about this notice, please contact Renee Walburn, Practice Manager, at (402) 552-2500.

#### **WHO WILL FOLLOW THIS NOTICE:**

Nebraska Orthopedic Associates, LLP, at the following locations:

Suite 409  
4230 Farnam St.  
Omaha NE 68131

Suite 105  
2206 Longo Drive  
Bellevue, NE 68005

Atlantic Medical Ctr  
1501 E. 10<sup>th</sup> St Box 429  
Atlantic, IA 50022

Suite 110  
2725 So. 144<sup>th</sup> St.  
Omaha, NE 68144

Jennie Edmundson Drs. Bldg  
One Edmundson Pl Suite 200  
Council Bluffs, IA 51503

Clarinda Regional Health Ctr  
17<sup>th</sup> & Wells, PO Box 217  
Clarinda, IA 51632

Shenandoah Outpt Clinic      Physicians Clinic  
1 Jack Foster Dr                      1700 14<sup>th</sup> Ave  
Shenandoah, IA 51601      Nebraska City, NE 68410

All these entities, sites, and locations follow the terms of this notice. In addition, these entities, sites, and locations may share health information with each other.

#### **OUR PLEDGE REGARDING HEALTH INFORMATION:**

We understand that health information about you is personal. We are committed to protecting health information about you. We create a record of the services you receive from us. We need this record to provide you with quality services and to comply with certain legal requirements. This notice applies to all of the records that we accumulate due to the services that we provide. This notice will tell you about the ways in which we may use and disclose health information about you. We also describe your rights to the health information we keep about you, and describe certain obligations we have regarding the use and disclosure of your health information.

We are required by law to:

- make sure that health information that identifies you is kept private;

- give you this notice of our legal duties and privacy practices with respect to health information about you; and
- follow the terms of the notice that is currently in effect.

## **HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU.**

The following categories describe different ways that we use and disclose health information. For each category of uses or disclosures, we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

**For Treatment.** We may use health information about you to provide you with recommendations for health care treatment or services. We may disclose health information about you to doctors, nurses, technicians, health students, or other personnel who are involved in taking care of you. They may work at the hospital if you are hospitalized, or at another doctor's office, lab, pharmacy, or other health care provider to whom we may refer you for consultation or for other treatment purposes. We may also disclose health information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

**For Payment:** We may use and disclose health information about you so that the services you receive from us may be billed to and payment collected from you, an insurance company, or a third party.

**For Health Care Operations:** We may use and disclose health information about you for operations of our business.

**Health-Related Services and Treatment Alternatives:** We may use and disclose health information to tell you about health-related services or recommend possible treatment options or alternatives that may be of interest to you. Please let us know if you do not wish us to send you this information, or if you wish to have us use a different address to send this information to you.

**As Required By Law.** We will disclose health information about you when required to do so by federal, state, or local law.

**To Avert a Serious Threat to Health or Safety.** We may use and disclose health information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

**Military and Veterans.** If you are a member of the armed forces or separated/discharged from military services, we may release health information about you as required by military command authorities or the Department of Veterans Affairs as may be applicable. We may also release health information about foreign military personnel to the appropriate foreign military authorities.

**Workers' Compensation.** We may release health information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

**Public Health Risks.** We may disclose health information about you for public health activities.

These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report child abuse or neglect;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify person or organization required to receive information on FDA-regulated products;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe a participant has been the victim of abuse, neglect, or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

**Health Oversight Activities.** We may disclose health information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

**Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose health information about you in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

**Law Enforcement.** We may release health information if asked to do so by a law enforcement official:

- in reporting certain injuries, as required by law, gunshot wounds, burns, injuries to perpetrators of crime;
- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person:
  - Name and address
  - Date of birth or place of birth;
  - Social security number;
  - Blood type or rh factor;
  - Type of injury;
  - Date and time of treatment and/or death, if applicable; and
  - A description of distinguishing physical characteristics.
- about the victim of a crime, if the victim agrees to disclosure or under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct;
- about criminal conduct at our facility; and
- in emergency circumstances to report a crime; the location of the crime or victims; or the identity, description, or location of the person who committed the crime.

**Coroners, Health Examiners and Funeral Directors.** We may release health information to a coroner or health examiner. This may be necessary, for example, to

identify a deceased person or determine the cause of death. We may also release health information about participants to funeral directors as necessary to carry out their duties.

**National Security and Intelligence Activities.** We may release health information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

**Protective Services for the President and Others.** We may disclose health information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

**Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release health information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

## **YOUR RIGHTS REGARDING HEALTH INFORMATION ABOUT YOU.**

You have the following rights regarding health information we maintain about you:

**Right to Inspect and Copy:** You have the right to inspect and copy health information that may be used to make decisions about your care. To inspect and copy health information that may be used to make decisions about you, you must submit your request in writing to Vice President, Corporate Counsel. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies and services associated with your request.

We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to health information, you may request that the denial be reviewed. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

**Right to Amend.** If you feel that health information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as we keep the information. To request an amendment, your request must be made in writing, submitted to Vice President, Corporate Counsel, and must be contained on one page of paper legibly handwritten or typed in at least 10 point font size. In addition, you must provide a reason that supports your request for an amendment.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the health information kept by us;
- is not part of the information which you would be permitted to inspect and copy; or
- is accurate and complete.

Any amendment we make to your health information will be disclosed to those with whom we disclose information as previously specified.

**Right to an Accounting of Disclosures.** You have the right to request a list accounting for any disclosures of your health information we have made, except for uses and disclosures for treatment, payment, and health care operations, as previously described. To request this list of disclosures, you must submit your request in writing to Vice President, Corporate Counsel. Your request must state a time period which may not be longer than six years and may not include dates before April 14, 2003. The first list you request within a 12 month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred. We will mail you a list of disclosures in paper form within 30 days of your request, or notify you if we are unable to supply the list within that time period and by what date we can supply the list; but this date will not exceed a total of 60 days from the date you made the request.

**Right to Request Restrictions.** You have the right to request a restriction or limitation on the health information we use or disclose about you for treatment, payment, or operations. You also have the right to request a limit on the health information we disclose about you to someone who is involved in your care or the payment for your care, such as a family member or friend. For example, you could ask that we restrict a specified nurse from use of your information, or that we not disclose information to your spouse about a surgery you had.

***We are not required to agree to your request for restrictions if it is not feasible for us to ensure our compliance or believe it will negatively impact the care we may provide you.*** If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. To request a restriction, you must make your request in writing to Vice President, Corporate Counsel. In your request, you must tell us what information you want to limit and to whom you want the limits to apply.

**Right to Request Confidential Communications.** You have the right to request that we communicate with you about health matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail to a post office box. To request confidential communications, you must make your request in writing to Vice President, Corporate Counsel. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

**Right to a Paper Copy of This Notice.** You have the right to obtain a paper copy of this notice at any time. To obtain a copy, please request it from Vice President, Corporate Counsel.

## **CHANGES TO THIS NOTICE**

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for health information we already have about you as well as any information we receive in the future. We will post a copy of the current notice in our facility. The notice will contain on the first page, in the top right-hand corner, the effective

date. In addition, each time you register for treatment or health care services, we will offer you a copy of the current notice in effect.

## **COMPLAINTS**

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services. To file a complaint with us, contact Vice President, Corporate Counsel, 987424 Nebraska Medical Center, Omaha, NE 68198-7424; Telephone (402)559-2879, Facsimile (402)552-3266. All complaints must be submitted in writing.

**You will not be penalized for filing a complaint.**

## **OTHER USES OF HEALTH INFORMATION.**

Other uses and disclosures of health information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose health information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose health information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

## **Acknowledgement of Receipt of this Notice**

We will request that you sign a separate form or notice acknowledging you have received a copy of this notice. If you choose, or are not able to sign, a staff member will sign their name, date. This acknowledgement will be filed with your records.

## **Acknowledgement of Receipt of Notice of Privacy Practices**

I, \_\_\_\_\_, have received the Notice of Privacy Practices from Private Practice Associates, LLC and Paramount Group, LLC.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

In lieu of participant signature, I, \_\_\_\_\_, a staff member of Private Practice Associates, LLC and Paramount Group, LLC, state that \_\_\_\_\_ has been given our current Notice of Privacy Practices.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

## Policy and Procedure on Participant's Right to Access Health Information

It is our policy to provide participants the right of access to inspect and obtain a copy of health information about themselves, for as long we maintain the information in our designated record set, with exceptions permitted by law.

It is our policy to comply with all legal requirements and obligations relating to the PHI of minor participants. Under most circumstances, a parent or legal guardian will have legal authority to act on behalf of minor children; in this manor the parent is considered to be the minor's "personal representative." The "personal representative" is entitled to receive PHI and permit its disclosure, as the participant would be. Under the following circumstances, the minor has authority to make his/her health care decisions:

- when the minor has the right under state law and the minor has not requested another person be treated as a personal representative;
- when the minor has the right to obtain a particular health care service;
- when the guardian agrees to an agreement of confidentiality between health care provider and the minor.

### **Definitions:**

*Access* means that participants may inspect their records under the supervision of a staff member for which an inspection fee is charged; or obtain a copy of all or a portion of their records for which a copying fee is charged.

*Designated record set* means records that we use in the process of our services that we provide.

### **Procedure:**

1. Participants may request access to their records by submitting a request in writing on our Authorization for Release of Information Form to our Vice President, Corporate Counsel . This Form specifies that the access will be granted within 30 days of its receipt unless the participant is otherwise notified, and identifies the fees that will be charged for supervision of inspection, for copying all or portions of the record, or for summarizing the record.

The request must state the type of access requested (inspection, copy, or if a summary will be accepted if there are reasons why a complete inspection or copy cannot be released, see step 3.b.), specify the dates and specific information requested, and be signed by the participant.

2. When a request for access to records are made by a participant:

a. Obtain the participant's record and verify the participant's demographic information and signature on the Authorization for Release of Information Form with demographic information and signature on the consent for use and disclosure of health information, or other document signed by the participant contained within the record. If the authenticity of the participant cannot be verified, send a request to the participant to have a new Authorization for Release of Information Form notarized.

b. Review the record according to the request, to determine if:

1.) The information requested is excepted from the participant's right of access (see step 3. Exceptions to access), in which case access must be denied. Follow the procedure in step 4. for Denial of access.

2.) The information requested is complete. If the information is not complete, inform the party responsible for completion that a request for access has been made by the participant and the record will need to be completed within 30 days in order to comply with the participant's request or be found in non-compliance with HIPAA and subject to fines. If the record is not completed within 30 days, send a copy of the Authorization for Release of Information Form to the participant indicating that an extension to providing access will be required because the record is in the process of being completed and indicating the specific date on which access will be granted. This date must not exceed an additional 30 days.

c. If access is not excepted and the information is complete and the participant requests inspection of the record or any portion thereof, schedule an appointment for the participant to visit the office. If the request is only for a portion of a record, remove that portion and place it in a separate folder for purposes of the inspection. Our Vice President, Corporate Counsel must be present with the participant during the time the participant is inspecting the record(s). During this time, the participant may not remove any documents from the record(s) or write any information in the record(s). If the participant wishes to make an amendment to the record(s), follow the Policy and Procedure for Participant's Right to Request Amendment of Health Information. If the participant has any questions concerning the information in the record, inform the participant that an appointment must be made with the President to discuss the information.

d. If access is not excepted and the information is complete and the participant requests a copy of any or all of the record, make the specified copies and mail the information to the participant via postal mail. If the participant requests this information to be mailed to a different address, mailed to a different individual, or be given to someone else who physically presents to our office, this information must be authorized through the Authorization for Release of Information Form. If another individual is designated to physically pick up the copy of the information, verify the individual's identity by requesting a photo identification card and match the name on the card to the name on the Authorization for Release of Information signed by the participant. Have the individual sign the Authorization for Release of Information as having received the information.

3. Exceptions to access are limited to very specific situations. Certain exceptions are unreviewable and for others we must permit the participant to request a review of our decision not to grant access.

Unreviewable grounds for denial of access include:

- when the information was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- when the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Reviewable grounds for denial of access include:

- when a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the participant or another person.
- when the information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
- when the request for access is made by the participant's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the participant or another person.

4. Denial of access is a serious matter under the law. Before the President may make such a denial decision, it is our policy to conduct an internal review of that denial. Any such case should be given to the President who will authorize the denial.

a. If access is denied for one of the unreviewable reasons to deny access, return a copy of the Authorization for Release of Information to the participant indicating that we are unable to comply with the request for access due to the applicable reason. Retain a copy of the Authorization for Release of Information sent to the participant in the participant's record.

b. If access is denied for one of the reviewable reasons, determine if a summary of the record may be made or portions of the record may be provided access such as to prevent the risk associated with denial.

1.) If a summary or access to portions of the record would prevent risk, return a copy of the Authorization for Release of Information to the participant indicating we are not able to comply with the request for access for the specified reason but would be able to provide a summary of information in the record or access to portions of the record.

2.) If such a summary or access to portions of the record is not possible, return a copy of the Authorization for Release of Information to the participant indicating we are not able to comply with the request for access for the specified reason. Indicate on this Form that the participant has the right to have this decision reviewed by another licensed health care professional.

3.) If a request for review is received, give a copy of the Authorization for Release of Information Form, the record, to the President, who will make a final determination. Upon the review and determination, send a response to the participant indicating the result of the review and how the participant may file a complaint with our office or to the Secretary of Health and Human Services (HHS).

4.) File a copy of the Authorization for Release of Information Form and other documentation received from the participant in the participant's record. Place a copy of the Authorization for Release of Information in the appropriate file.

5.) If a request for access to the record is made and the person was not a participant of ours, return a copy of the Authorization for Release of Information Form to the individual indicating we have no records. If we do not have records on this individual but know where the requested information may be maintained (such as at a hospital or other physician's office), return the Authorization for Release of Information Form to the individual and provide the name and address of the location where we believe the records may be maintained. Keep a copy of the Authorization for Release of Information Form in the appropriate file.

## Policy and Procedure on Participant's Right to Request Amendment to Health Information

**The purpose of this policy is to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and to afford our participants the right to request amendment to their protected health information.**

### **General Policy:**

It is our policy to provide our participants the right to request amendment to their protected health information that we maintain in our designated record set, with exceptions permitted by law.

### **Definitions:**

*Amendment* means to add information to an existing record which either provides additional information, clarifies or corrects existing information, or provides an alternative view with respect to information that we have compiled about the participant in the participant's designated record set.

*Designated record set* means records that we use to make decisions about participants.

### **Procedure:**

1. A participant who believes there is an error in information in the record may approach the author of the entry, point out the error, and request the author to correct it. The author may accept any correction believed to be required, and will document the correction.

This documentation must retain the original entry, state the correct information, and reflect the author's identity and date of correction. In electronic information system, the correction should be made in accordance with the vendor's specification for correcting errors such that an audit trail exists to show both the original entry and the new entry. In paper documents, a correction may be made in one of two ways: If an entry is simply erroneous and needs to be deleted, a line may be drawn through the erroneous information, initialed, and dated. If an entry is erroneous and requires correction, the entry should be noted as erroneous and correct information written in a separate note, which must be signed and dated. The author should inquire of the participant if the correction of the error should be disclosed to anyone who may have received this information in the past. If so, the participant should be directed to complete the Form to Request Amendment to Health Information.

2. A participant may also request that information be added to the record.

This request must be made in writing, on our Form to Request Amendment to Health Information, to the Vice President, Corporate Counsel . This Form serves as both documentary evidence of the request and our response, as well as a tracking mechanism to ensure response within 60 days of request (with not more than one 30-day extension) and duty to supply others with the information. This form will be processed in the following manner:

a. Request the participant to complete the Form to Request Amendment to Health Information in triplicate. If this is not received in person, verify the participant's signature on the Form with a sample in the record. The participant should keep the last copy of the Form.

b. Place the remaining two copies of the Form in the participant's record. Route the record to the author of the record.

c. If the author accepts the participant's amendment, the author will sign and date the Form as amendment accepted and make a note at the site in the record to which the amendment applies that an amendment exists. The author may also add a comment to the Form. The second copy of the Form will be returned to the participant indicating that the amendment has been accepted. The original copy of the Form will be used to furnish copies of the amendment to those individuals or organizations the participant deems necessary and documents on the Form. Such disclosures will be noted on the form as having been completed with the signature of the staff member who processed the disclosures. The original Form will be placed in the record.

d. If the author rejects the participant's amendment, the author must indicate one of the following as reasons:

1.) The information subject to amendment was not created by us.

2.) The information subject to amendment is not part of the designated record set.

3.) The information would not be available for access (see our policy on Participant's Right to Access Health Information).

4.) The information contained in the existing record is accurate and complete.

The Form must be signed and dated, and the author must make a note at the site in the record to which the amendment applies that an amendment was requested. The second copy of the Form with this information will be returned to the participant. The original copy of the Form will be filed in the record. The participant may request that the request for amendment and the denial be disclosed with any future disclosures of the information that is the subject of the amendment.

e. If this processing cannot occur within 60 days of receipt of the request, notify the participant in writing that a 30-day extension will be necessary to process the request.

f. The participant may choose to submit a written statement disagreeing with the denial. This statement must be contained on not more than one handwritten or typewritten page of at least 10-point font. Any more information than this that is received will be discarded. When this statement of disagreement is received, it should be forwarded to the author, who will determine whether a rebuttal will be prepared. The statement of disagreement and any rebuttal must also be filed in the record and accompany any future disclosures of the information that is the subject of the amendment.

3. If we are informed by another provider of an amendment to one of our participant's records, the Vice President, Corporate Counsel will review its contents and advise the physician who attended the participant as to any information which appears to require our action. We will place the amendment information in our designated record set.

## Policy and Procedure to Request Restrictions on Use and Disclosure of Protected Health Information

### **Responsibility:**

1. It will be the responsibility of the Nurse Coordinator to receive requests for and agree to any restrictions on use and disclosure of protected health information.
2. It will be the responsibility of the Nurse Coordinator to monitor that any restrictions to which the office agrees will be followed.

### **General Policy:**

1. We will supply any individual who requests restrictions placed on use and disclosure of protected health information a Form to Request Restrictions on Use and Disclosure of Protected Health Information.
2. We will agree to requested restrictions if, in the judgment of a licensed healthcare professional, we believe the restriction will not limit our ability to provide quality services or manage our operations, and if our information management procedures and systems will permit us to comply consistently with the requested restrictions.

### **Procedure:**

1. When an individual requests restrictions, supply the individual with our Form to Request Restriction and Disclosure of Protected Health Information.
2. The Nurse Coordinator will review the Form to Request Restriction and Disclosure of Protected Health Information and determine whether we are able to accept the restrictions. The Nurse Coordinator will complete and sign the Form to Request Restrictions, supply the individual with a copy, and place the original in the individual's permanent health record. The Nurse Coordinator will also make the necessary postings to the individual's health record to enable the restrictions to be carried out.
3. If the individual makes the request for restrictions in our office, we will attempt to complete the Form to Request Restrictions and Disclosure of Protected Health Information during the time the individual is present in our office, but no later than 30 days after receipt.
4. If at any time we find that we cannot carry out the restrictions requested by an individual, we will prepare a written notice to send to the individual terminating our

agreement, which will be applicable only to information created or received after such notice has been sent to the individual.

5. We will accept a written request from the individual to terminate the restrictions at any time or will document any oral request to terminate restrictions from the individual. If an oral request is received, this will be documented on the original Form to Request Restriction and Disclosure of Protected Health Information, a copy of which will be supplied to the individual.

# Policy and Procedure on Requesting Confidential Handling of Information

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Nurse Coordinator

## **Purpose:**

The purpose of this policy is to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and to inform our participants of their right to request confidential handling of their protected health information when it is sent to them.

## **General Policy:**

It is our policy to accommodate reasonable requests regarding the confidential handling of protected health information, and to maintain that confidential treatment consistent with the participant's request.

## **Definitions and Regulatory Requirements**

*Protected health information:* Individually identifiable health information, including information that is maintained in records.

*Confidential Communications Requirements:* Allow individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations.

*Conditions on providing confidential communications:*

- 1.) May require the individual to make a request for a confidential communication in writing.
- 2.) May condition the provision of a reasonable accommodation on:
  - a. When appropriate, information as to how payment, if any, will be handled; and
  - b. Specification of an alternative address or other method of contact.
- 3.) May not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

## **Procedure:**

1. Participants may request confidential handling of health information by submitting a request, in writing, in one of the following ways:
  - a. In person, on our Request for Confidential Handling of Health Information Form;
  - b. By mail, either on our Request for Confidential Handling of Information Form or in a letter containing the necessary information specified below. All requests should be

mailed to:

Private Practice Associates, LLC/Paramount Group, LLC  
987424 Nebraska Medical Center  
Omaha, NE 68198-7424

All requests should be directed to the Nurse Coordinator. The request must supply the following details about the protected health information the individual wants confidentially handled:

- a. The type of information, specifying if the request is limited to a particular illness or treatment or all health information exchanges;
- b. The time period for which the request applies;
- c. The manner in which the participant wishes to receive confidential communications, with any alternate information necessary to deliver information in the requested manner.

2. When a request for confidential handling is made by a participant:

- a. Validate the request with the individual. If the request is received by mail, call the contact phone number and ask to speak with the participant to confirm the request. If the request is made in person, request confirmation of identity, if needed. Employees may not ask the participant why the participant is requesting the confidential communication.
- b. If the request is for an alternate address, enter the address into the participant's address file as the required confidential address.
- c. If the request is to pick-up the confidential information in person, highlight the requirement for easy recognition by staff handling correspondence.
- d. If the request is time limited, flag the end date for confidential handling of information in the appropriate files and systems.
- e. Place a copy of the Request for Confidential Handling of Information Form in the participant's record and place a copy in your Risk Management file.

**Request for Confidential Handling of Health Information**

I, \_\_\_\_\_, request confidential handling of  
correspondence regarding my health information for the period:

FROM: \_\_\_\_\_

TO: \_\_\_\_\_

This request applies to health information involving:

I have selected to receive confidential communications in the following way:

Participant will pick up communications at the office.

Participant will receive any information at an alternate mailing address.

Please use the following mailing address for all health information communications that  
fit in the description provided above.

Name:

CITY: \_\_\_\_\_ STATE: \_\_\_\_\_ ZIP CODE: \_\_\_\_\_

If you have any questions concerning this confidential handling, please contact: **(402)  
552-3377.**

**DATE:** \_\_\_\_\_

\_\_\_\_\_  
**Nurse Coordinator**

\_\_\_\_\_  
**Participant**

# Policy and Procedure on the Handling of Privacy Complaints

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Vice President, Corporate Counsel

## **Purpose:**

The purpose of this policy is to comply with the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) and to afford our participants the right to file complaints, have the complaint investigated and, if appropriate, receive the disposition of the complaint pursuant to the HIPAA privacy rules and our implementing policies and procedures.

## **General Policy:**

It is our policy to keep a record of all complaints and to investigate all valid complaints to determine the circumstances surrounding any concerns our participants raise regarding privacy. If a participant's privacy rights have been infringed upon in any way, or there is evidence that our staff or associates have not adhered to the privacy standards or our policies and procedures, we will take actions consistent with the HIPAA regulations and our Policy and Procedure on Personnel Discipline for Breach of Privacy or Confidentiality and document these actions accordingly.

The HIPAA privacy regulations give all individuals the right to file complaints to Paramount Group, LLC and the Office of the Secretary in the Federal Department of Health and Human Services.

Under no circumstances will the fact that an individual has filed a complaint affect the services provided to that individual. Any staff found to be treating any individual differently in light of a complaint will be sanctioned. Any retaliation is prohibited by law.

## **Procedure:**

1. Participants may file privacy complaints by submitting them, in writing, in one of the following ways:
  - a. In person, on our Privacy Complaint Form;
  - b. By mail, either on our Privacy Complaint Form or in a letter containing the necessary information specified below. All requests should be mailed to:

Private Practice Associates, LLC/Paramount Group, LLC  
987424 Nebraska Medical Center  
Omaha, NE 68198-7424

All privacy complaints should be directed to the Vice President, Corporate Counsel. The complaint must describe the privacy concern in as much detail as possible including

when the infraction of the standards or mishandling of protected health information was believed to have occurred, and who, if known, was believed to have acted inappropriately with respect to protected health information or an individual's privacy rights. The complaint must include the following information:

- a. The type of infraction the complaint involves (ie. inappropriate handling of PHI, appropriateness of privacy policies and processes);
- b. A detailed description of the privacy issue;
- c. The date the incident or problem occurred, if applicable;
- d. The mailing address to which a formal response to the complaint may be sent.

2. When a privacy complaint is filed by a participant:

- a. Validate the complaint with the individual. If the complaint is received by mail, phone, fax or email call existing contact phone number and ask to speak with the participant to confirm the complaint. If the complaint is made in person request confirmation of identity, if needed, and validate the facts of the complaint.
- b. If the complaint appears to be a misunderstanding of the requirements or your policies and procedures, contact the participant and determine if, based on a more in depth discussion of the concern, the individual still wants to file a complaint. Be as courteous as possible. **UNDER NO CIRCUMSTANCES SHOULD A PARTICIPANT FEEL PRESSURED OR COERCED EVEN IF YOU BELIEVE THEY ARE STILL MISUNDERSTANDING THE RULES OR POLICIES.** If the individual does not want to pursue the complaint any further indicate "**no further action required based on clearer understanding**", record the date and time, and file under dismissed complaints.
- c. Once validated and if not dismissed, log the complaint by placing a copy of the complaint form in the complaint file and the participant's record.
- d. Investigate the complaint by reviewing the circumstances with the relevant staff and reviewing any audit and monitoring logs that may have relevance to the complaint. If the complaint involves any issues with an individual's rights that have attendant documentation e.g., consent or authorization processes or confidential requests, pull all relevant forms. Complete the complaint investigation section of the complaint form with a summary of your findings.
- e. If you determine the complaint is invalid, draft a letter stating the reasons the complaint was found invalid. Initially letters should be reviewed by an impartial, knowledgeable staff person or lawyer for tone and rationale. Standard letters will likely emerge over time. File a copy of the letter and form in the investigated complaints file.
- f. If you are uncertain about your findings get a second opinion from your HIPAA privacy committee or your lawyer.
- g. If you determine the complaint is valid and linked to a required process or an individual's rights follow your office sanction policy to the extent that an individual is responsible. If the complaint involves your office's compliance with the standards that do not involve a single individual e.g., policies and procedures themselves versus adherence to them, then begin the process to revise your current policies and procedures.
- h. Once an appropriate sanction or action has been taken with respect to a complaint with merit, or if the response will take more than 30 days, draft a letter explaining the findings and the associated response or intended response. Use the same review process as for the invalid complaint letter in e. Document the disposition of complaint on the complaint form and file the letter and form in the investigated complaints file.
- i. Place a copy of the Complaint Form in the participant's record.
- j. Review complaint files, both invalid and investigated complaints, at least annually to

determine if there are any emerging patterns.

### Privacy Complaint Form

I, \_\_\_\_\_, am registering a formal complaint regarding Private Practice Associates, LLC and/or Paramount Group, LLC.

The complaint involves:

\_\_\_ Appropriateness of Private Practice Associates, LLC and/or Paramount Group, LLC privacy policies and processes.

\_\_\_ My privacy rights to notice, consent, authorization, access, amend, request restrictions, confidential communications or accounting of disclosures.

\_\_\_ Inappropriate handling of protected health information.

\_\_\_ Other

A detailed description of the privacy issue involved in the complaint is provided below:  
The incident or problem occurred on \_\_\_\_\_ (month/day/year), if applicable.  
I can be reached at \_\_\_\_\_ (please provide a day time number).

\_\_\_\_\_  
PARTICIPANT SIGNATURE

DATE: \_\_\_\_\_

Please use the following mailing address for a formal response to this complaint.

PRINT MAILING ADDRESS:

\_\_\_\_\_  
Print City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

If you would like to follow up on the status of your complaint, please contact:

Vice President, Corporate Counsel  
**(402) 552-3377**

For Office Use  
Only  
Dismissed Investigated Invalid Has Merit  
Summary of investigation:  
Response to complaints with merit:  
Staff involved in review:

NAME: \_\_\_\_\_

DATE: \_\_\_\_\_

## Policy on Minimum Necessary Information

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Nurse Coordinator

It is crucial that every staff member understands the minimum necessary policy for use, disclosure and request of protected health information.

Staff are entitled to use PHI consistent with their roles in this organization. Each staff member must also understand that with this right comes certain responsibilities such as limiting the viewing, use, disclosure and requesting to only that data necessary to serve the need of participants. It is considered a breach of policy and the participant's trust to seek information beyond what is appropriate for the staff role and the participant needs. In the event of an emergency, the strict limits of access may be breached when appropriate for the benefit of the participant, specifically when the potential benefit to the participant is judged to outweigh the risk to participant privacy.

### **Purpose:**

The purpose of this policy is to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and to ensure our participants' rights to the minimum necessary use and disclosure of their protected health information.

### **General Policy:**

1. When using or disclosing protected health information or when requesting protected health information from another covered entity, each staff member of Private Practice Associates, LLC and Paramount Group, LLC must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This requirement does not apply to disclosures to a health care provider for treatment, uses or disclosures made to the individual, uses or disclosures made pursuant to an authorization for release signed by the participant or the participant's representative, disclosures made to the Secretary of Health and Human Services, disclosures that are required by law (as described by Sec. 164.512(a) of the Privacy Regulation) and uses or disclosures that are required for compliance with the Privacy Regulation.

2. It is necessary that the different roles in Private Practice Associates, LLC and Paramount Group, LLC be defined so that each staff member understands their own rights and responsibilities.

### **Office Role Categories:**

**Direct Healthcare Provider** - A licensed healthcare professional who provides direct or indirect participant care or consulting services.

**Technical Staff** - Staff who provide participant care at the request of a direct healthcare provider.

**Direct Support Staff** - Staff who work within the office providing a variety of professional and direct administrative support that involves the delivery of services.

**Indirect Support Staff** - Staff who work within the office providing administrative support.

#### **Data Access Categories:**

**Full Health Information Access** - Access to full health information as needed for health or payment operations. Staff in this category may access and read all appropriate information.

**Summary Data Access** - Access to summary data with treatment or diagnostic codes as needed to function. Staff in this category should confine the use of protected health information to the absolute minimum required and should not access or read full records.

**Minimum Information Access** - Access to participant demographic data with only minimum reference to treatment or diagnostic information as needed to function.

**Emergency Information Access** - Access to any individually identifiable health information should not be granted except in emergency situations.

#### **Usage Assignments:**

Data Access Categories are assigned in accordance with the operational requirements for minimum necessary use. Direct Healthcare Providers have access to full health information with the clear understanding that access and reading is limited to need for treatment, reimbursement or operations.

Technical Staff have access to summary data with the clear understanding that access and reading is limited to need for treatment, reimbursement or operations.

Direct Support Staff have access to minimum health information with the clear understanding that access and reading is limited to need for treatment, reimbursement or operations.

Indirect Support Staff have access to emergency information with the clear understanding that access and reading is limited to need for treatment, reimbursement or operations.

Paramount Group, LLC will maintain a current office role directory that lists every defined position within the office. This will ensure that each position will be granted the correct access authorization as defined in the Usage Assignments section of this policy. It is incumbent on every staff member to report any observed violation of these usage rules to the Vice President, Corporate Counsel or another senior staff member. Every staff member must be trained in their roles and responsibilities with reference to the minimum use and access to participant data.

It is considered a breach of organization policies and the participant's trust to seek information beyond what is appropriate for the staff role and the participant needs. In the event of an emergency, the strict limits of access may be breached when appropriate for the benefit of the participant, specifically when the potential benefit to the participant is judged to outweigh the risk to participant privacy.

### **Disclosures for Treatment, Payment or Health Operations:**

The regulations establish that routine and recurring disclosures of protected health information can be made for treatment, payment or health operations without specific participant authorization.

The minimum necessary requirements still pertain to all of these disclosures. Minimum necessary determinations will be made for all routine and recurring disclosures for all categories (other than those that are excepted); these categories will include, for example, additional medical information for medical necessity determination, sample records for accreditation and audits, records review for protocol adherence, participant information for participation in a clinical trial, paper claims, phone referral certification information and other categories as determined necessary.

Full health information will be provided to routine and recurring requests from:

- 1)Healthcare Providers
- 2)Participants

Summary data with treatment and or diagnostic codes will be provided to routine and recurring requests from:

- 1)Billing Services
- 2)Clearinghouses

Minimum information - participant demographic data with only minimum reference to treatment or diagnostic information - will be provided to routine and recurring requests from:

- 1)Answering Services

Every effort will be made to comply with these disclosure categories except where the cost of extracting information is not reasonable and the risk of breach of participant privacy is considered low. In all situations, the requestor will be informed of their responsibilities towards this data and appropriate agreements entered into.

All non-routine and/or non-recurring requests will be considered on a case-by-case basis and determination of the level of response will be based on criteria that take into account the minimum necessary requirements.

### **Requests for Information:**

The regulation establishes that for routine and recurring requests the responsibility for determining the minimum necessary data falls on the requestor, in all situations where data are requested, staff members must ensure that minimum necessary evaluation is made. In situations where the determination has not been made, questions should be

directed first to the Vice President, Corporate Counsel and then to the Nurse Coordinator.

Minimum necessary determinations will be made for all routine and recurring requests for all categories; these categories will include, for example:

- Reason for visit
- Vital medical stats
- Medical records for referral
- Referral authorization, if non-standard
- Test results
- Participant messages from an answering service

## Office Role Directory

### **Private Practice Associates, LLC/Paramount Group, LLC**

The following is a current list of all positions currently defined for Paramount Group, LLC. They are listed according to the Office Role Category (as defined in the Policy on Minimum Necessary Information) to which they belong. The Office Role Category determines the type of information access each position requires to function.

#### **Direct Healthcare Providers:**

- 1) Physicians
- 2) Nurses
- 3) Medical Directors

#### **Technical Staff:**

- 1) Phlebotomists
- 2) Lab Techs

#### **Direct Support Staff:**

- 1) Interpreter
- 2) Administrator
- 3) Operations Managers
- 4) Consultants
- 5) Interns
- 6) Independent Contractors

#### **Indirect Support Staff:**

- 1) Marketing Coordinator
- 2) Accounting/Bookkeeping

# Policy and Procedure on Uses and Disclosures of Protected Health Information

**Authority:** Vice President, Corporate Counsel

**Responsibility:**

1. It will be the responsibility of the Nurse Coordinator to obtain a signed Authorization Form from our participants, or the participants authorized representative, when they request release of information.
2. It will be the responsibility of the Vice President, Corporate Counsel at 402-552-3377, to respond to questions about the Authorization Form.

**General Policy**

1. It is mandatory that a valid authorization from the participant, personal representative, legal guardian if the participant is incompetent, or next-of-kin if the participant is unable to consent, be provided in order for any protected health information to be released, except as provided for in #2. When a person other than the participant requests disclosure of PHI, staff should verify the identity of the individuals and obtain any documentation, statements, or representation of the person's requesting the information.
2. Uses and disclosures for which consent, authorization, or opportunity to agree or object is not required, can only occur under special circumstances. See excerpt from federal regulations, **Federal Register, Thursday, December 28, 2000, 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule**, for specific guidance.
3. It is our policy to fulfill requests for information within 30 days of receipt of a valid Authorization for Release of Information Form.

**Procedure**

1. When a request for release of information is made, the Authorization for Release of Information Form must be completed by the participant, legal guardian, or next-of-kin. The Form must contain:
  - a. Name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure, or to whom we may make the requested use or disclosure. Obtain complete information on the name, address, phone and fax number of the person(s) or class of persons to whom the participant is authorizing release of information.
  - b. Description of the information to be used or disclosed must be checked off and dates or date range specified.
  - c. Date on which the authorization expires. This is 90 days from the date of the request. This date should be calculated and recorded in the "FOR OFFICE USE ONLY" box on the Authorization of Release of

Information Form.

d. Signature of participant, personal representative, legal guardian or next-of-kin, and date signed. If someone other than the participant is signing the authorization form, that individual's relationship to the participant must be stated. If a request for release of information is received in the mail or via fax, verify the signature on the Form against a sample signature in the record.

2. The form requests the participant to identify the purpose of the disclosure. This is not required, but is desirable in order for us to provide a proper accounting for disclosures of information, should the participant so request such an accounting.

3. If we are requesting the participant to authorize release of information, we must supply a reason on the Form in response to question #4 on the Form and indicate whether or not we will receive financial or in-kind compensation in exchange for using or disclosing the health information described. If this does not apply to a given participant, this section should be marked through.

4. We do not charge a fee for fulfilling requests for release of information to other physicians, for continuing care, for school purposes, for insurance, or for Workers' Compensation. For all other requests for release of information we will charge a fee of \$0.25. Record the amount collected in the "FOR OFFICE USE ONLY" box on the Authorization of Release of Information Form. We may waive this fee under special circumstances.

5. Upon fulfilling the request, we will indicate the date the request was made and who filled out the request. At this time, the expiration date should be verified to ensure that the release of information is timely. If the information was supplied to someone other than the participant, in person, we will obtain photo identification before releasing the information to that individual.

Record in the "FOR OFFICE USE ONLY" box on the Authorization of Release of Information Form what type of photo identification was checked (e.g., drivers' license, passport).

6. If the request for a disclosure of PHI is made when participant authorization is not necessary, verify the identity of the person or the public official, if the request is made face-to-face, otherwise validate that the company letterhead is official. If an employee has a doubt on the validity, the employee should contact the Privacy Official prior to making a disclosure.

7. If the request is from an attorney, it will be honored only upon receipt of a valid Authorization for Release of Information Form or court order directing the office to release information to the specific named attorney. If the request is from an attorney or marked for legal purposes, all physicians who attended the participant must be notified.

8. If the request is from a participant for access to his or her own information, follow our Policy and Procedure on Participant's Right to Access Health Information. Such requests must be fulfilled within 30 days of receipt of the request.

# Policy and Procedure for Informing Individuals Concerning Opportunity to Accept/Reject Certain Uses and Disclosures

**Authority:** Vice President, Corporate Counsel

**Responsibility:**

It will be the responsibility of the Nurse Coordinator and/or PPA/Paramount President to exercise professional judgment to use or disclose information where authorization is not required, but the individual must be given an opportunity to agree or object.

**General Policy:**

Our Notice of Privacy Practices will identify the circumstances in which we may use or disclose protected health information for which authorization is not required, but the individual must be given an opportunity to agree or object. These circumstances include:

1. Uses and disclosures of protected health information that we believe in our professional judgment to be in the individual's best interest for purposes of care or for notification of the individual's general condition, location, or death. Such disclosures may include making health information directly relevant to the individual's care or payment related to care available to a family member, other relative, close personal friend, or any other person identified by the individual as involved in care or payment of care. We may disclose health information to notify a family member, personal representative, or another person responsible for the individual's care concerning the individual's general condition, location, or death. We may also disclose health information about the individual to an entity assisting in a disaster relief effort so that the individual's family can be notified about the individual's general condition, location, or death.
2. Using and disclosing protected health information to contact the individual as a reminder that the individual has an appointment. We must give the individual the right to request that such confidential communication be sent to an alternative location or by an alternative means.
3. Using and disclosing protected health information to tell the individual about health-related services or recommend possible treatment options and/or alternatives that may be of interest to the individual. Such marketing communications must occur in one of two ways:
  - a. In a face-to-face encounter with the individual.
  - b. In a written communication from us or one of our business associates concerning products or services of nominal value where we are identified as making the communication, we prominently state if we have received or will receive direct or indirect remuneration for making the communication, and we describe how the individual may opt out of receiving future such communications.
4. Using and disclosing PHI for a facility directory, without specific written authorization from the individual. The directory may include the following information: name, location in facility, condition in general terms (no specific medical information may be disclosed), and religious affiliation. Information in the directory may be disclosed (a) to members of

the clergy or (b) to individuals who ask for the individual by name. If the individual objects or wishes to restrict or prohibit some or all uses of the information for the purpose describe above, Nurse Coordinator and/or PPA/Paramount President shall make the necessary notes/edits to the participant's charts and/or registration materials to ensure that the information is restricted.

5. Using protected health information about the individual to contact the individual in an effort to raise money for our not-for-profit operations. We may disclose health information to a foundation related to our practice so that the foundation may contact the individual in raising money for our practice. We only will release contact information; such as the individual's name, address, and phone number and the dates the individual received treatment or services from us. The fundraising communication must include a description of how the individual may opt out of receiving any further fundraising communications.

**Procedure:**

1. When an individual is present or otherwise available prior to a use or disclosure for which an authorization is not required but the individual must be given an opportunity to agree or object, we may obtain the individual's oral agreement, inform the individual of our intent and provide the individual the opportunity to object, or reasonably infer from the circumstances that the individual does not object to the disclosure. For example, if we request an individual to complete an appointment reminder post card, we may infer from the individual's completion of the card that there is no objection to this disclosure. If we plan on calling the individual, however, we will inform the individual that a call will be made and ask if there is any objection or alternative telephone number for us to call.

2. If the individual is not present or the opportunity to agree or object cannot practicably be provided because of the individual's incapacity or an emergency circumstance, we may exercise professional judgment to determine whether the disclosure is in the best interest of the individual. If so, we will disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. If a known family member, other relative, close personal friend, or other person involved in the individual's care is present in our office and does not volunteer to act on behalf of the individual, we will not infer that there is no objection to disclosing protected health information and we will not disclose such information.

3. If the individual is sent any marketing or fundraising communications for which we do not have specific restrictions on file, we will ensure they meet the requirements set forth in HIPAA's privacy rule and will include a description of how the individual may opt out of receiving any further such communications.

4. If the individual has filed a Form to Request Restrictions that cover any of the above disclosures of protected health information, we will accept such restrictions and take every measure practicable to not disclose such information.

# Policy and Procedure on De-Identification of Protected Health Information

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Nurse Coordinator; Vice President, Corporate Counsel

## General Policy

Our policy on Uses and Disclosures of Protected Health Information serves as our guideline as to when it is acceptable to release individually identifiable health information to other persons or organizations. For all other uses and disclosures, we will require the removal of information which may be used to identify the individual participant. We will de-identify individually identifiable health information by removing the following specified identifying characteristics of the individual participant or of relatives, employers, or household members of the individual participant:

### Names

All geographic subdivisions smaller than a state including:

Street address

City

County

Precinct

Zip code, and their equivalent geocodes, except for the initial three digits of a zip code.

All elements of dates (except year) for dates directly related to an individual. This will include:

Birth date

Date of death

All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

Telephone numbers

Fax numbers

Electronic mail addresses

Social security numbers

Medical record numbers

Health plan beneficiary numbers

Account numbers

Certificate/license numbers

Vehicle identifiers and serial numbers, including license plate numbers

Device identifiers and serial numbers

Web Universal Resource Locators (URLs)

Internet Protocol (IP) address numbers

Biometric identifiers, including finger and voice prints

Full face photographic images and any comparable images

Any other unique identifying number, characteristic, or code

If we have any reason to suspect or know that, after de-identifying the information, the individual participant could still be identified, we will take additional reasonable steps to remove such information.

If we are unable to adequately de-identify data for a requested purpose, we will either seek written authorization to release the data or will refuse to release the data. De-identified data will result in the creation of a new set of data. It will not require the destruction or altering of original data.

Should we believe we will have need to re-identify the information at any time in the future, we may assign the de-identified information for each individual participant a special code. This code may not be derived from or related to information about the individual and may not be able to be translated in such a manner as to identify the individual except by persons authorized in this practice to do so. No one outside of this practice is permitted to disclose the codes or their means of creation that are designed to re-identify individual participants. Any such disclosure will constitute disclosure of protected health information and if disclosed in a manner inconsistent with our policy on Uses and Disclosures of Protected Health Information will be subject to disciplinary action up to and including termination in accordance with our Human Resources Policy. This policy applies regardless of whether the original information is in manual or electronic form.

### **Procedure on De-Identification of Protected Health Information**

1. All employees will be trained in the de-identification policy and importance of de-identifying individually identifiable information except:
  - a. for uses or disclosures for treatment, payment or operations;
  - b. when disclosure is required by law or other disclosures allowable without authorization; and
  - c. when an authorization to release the information has been obtained.
2. It is generally the responsibility of the Nurse Coordinator; Vice President, Corporate Counsel to assure that participant information has been de-identified in accordance with our Policy on De-Identification of Protected Health Information. This responsibility can be delegated to other health information management (HIM) specialists or information system specialists within our company as appropriate.
3. Where large quantities of information, from either a manual or electronic source must be de-identified, we may engage the services of an outside business entity. That entity will be required to execute our Business Associate Contract before releasing any participant health information to them for purposes of de-identifying it.
4. If unable to adequately de-identify information for a requested purpose other than as specified in #1 above, seek written authorization to release the information, or refuse to release the information.

# Policy and Procedure on Accounting for Disclosures

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Nurse Coordinator; Vice President, Corporate Counsel

## **Purpose:**

The purpose of this policy is to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and to afford our participants the right to request and receive an accounting of disclosures we make concerning their health information.

## **General Policy:**

It is our policy to keep an accurate accounting of all applicable disclosures that we make of our participants' protected health information; and to provide an accounting of those disclosures to participants who may request an accounting, as permitted by law.

## **Definitions:**

*Disclosure* means the release, transfer, provision of access to, or divulging in any other manner of information outside of this office.

*Applicable disclosure* refers only to those disclosures of participants' protected health information made *for reasons other than:*

To carry out treatment, receive reimbursement, or carry out our operations;

To the participants themselves;

Relating to a use or disclosure otherwise permitted or required;

Pursuant to an authorization;

To persons involved in a participant's care;

For national security or intelligence purposes (as specified in our policy on Authorization for Release of Information);

To correctional institutions or law enforcement officials under certain circumstances (as specified in our policy on Authorization for Release of Information);

As part of a limited data set; or

Those that occurred prior to April 14, 2003.

*Protected health information* means individually identifiable health information, including that maintained in our records.

## **Procedure:**

1. Participants may request an accounting of disclosures by submitting a request in writing on our Request for Accounting for Disclosures Form to our Nurse Coordinator; Vice President, Corporate Counsel. The request must state the time period for which the accounting is to be supplied, which may not be longer than six years and may not include dates before April 14, 2003.

2. When a request for an accounting of disclosures is made by a participant:

a. Obtain the participant's record.

- b. Review the record to determine if it contains a written statement from a health oversight agency or law enforcement official that such an accounting to the participant must be suspended because such an accounting would impede the agency's activities. If such a statement exists, review the time period of the suspension. If the suspension is for less than 60 days from the date of receiving the request, hold the request until the suspension period has ended and then process the request. If the suspension is for more than 60 days from the date of receiving the request, send the Accounting for Disclosures Form indicating that we are temporarily unable to process the accounting due to a suspension required by law, but will comply with the request when the suspension has been lifted, and specify the date on which the suspension will be lifted. If the time period for suspension has passed, proceed to process the request.
- c. Review the section of the record that contains authorizations and requests for disclosures to determine which disclosures are applicable to the accounting (see Definitions above) and within the time period being requested.
- d. Complete the Accounting for Disclosures Form to supply the date(s) of disclosure(s), name(s) and address(es) of organizations or persons to whom the disclosure(s) were made, a brief description of the protected health information disclosed, the purpose of the disclosure(s), and the name of our Nurse Coordinator; Vice President, Corporate Counsel and date the Form was mailed.
- e. If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose for 50 or more individuals, the accounting may provide the name of the protocol or research activity, a description the protocol or research activity (including the purpose of the research and the criteria for selecting particular records), a brief description of the type of protected health information that was disclosed, the date of disclosure(s), the name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed and a statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or research activity. Also, then we will provide assistance if an individual or entity requests in contacting the entity that sponsored the research and the researcher.
- f. Frequent Disclosures. If multiple disclosures of PHI have been made to the same person or entity for a single purpose, the accounting may describe the four elements listed above for the first disclosure during the accounting period, the frequency or number of disclosures during the accounting period, and the date of the last disclosure.
- g. Send the Accounting for Disclosures Form to the participant within 60 days of receiving the request. If we are unable to complete this process within 60 days, send the Accounting for Disclosures Form to the participant indicating we will need a 30 day extension to complete the process, indicate the date on which we will supply the accounting, and check off the reason for the delay.
- h. Place a copy of the Accounting for Disclosures Form in the participant's record and place a copy in your appropriate file.

3. We will provide the first accounting to a participant in any 12-month period without charge. For any subsequent request within the 12-month period, we will charge \$25.00, as specified on the Request for Accounting for Disclosures Form. (A participant who does not wish to pay for subsequent accountings may withdraw the request and no accounting will be made.)

**Request for Accounting for Disclosures of Health Information**

I, \_\_\_\_\_, request an accounting for disclosures of my health information for the period:

FROM: \_\_\_\_\_

TO: \_\_\_\_\_

I understand that this accounting for disclosures will include disclosures made only to those organizations or persons *other than*:

to those for whom use and disclosure of my health information was made to carry out my treatment, process payment for my health care, or carry out your operations to myself or persons involved in my care for national security or intelligence purposes (as specified in your Notice of Privacy Practices) to correctional institutions or law enforcement officials under certain circumstances (as specified in your Notice of Privacy Practices) that occurred prior to April 14, 2003.

\_\_\_\_ I understand that I may receive the first accounting for disclosures within a 12-month period at no charge.

\_\_\_\_ I understand that I am requesting a second or subsequent accounting in a 12-month period and will pay the charge of \$25.00 for this accounting.

**Send this accounting to:**

PRINT MAILING ADDRESS:

\_\_\_\_\_

CITY: \_\_\_\_\_ STATE: \_\_\_\_\_ ZIP CODE: \_\_\_\_\_

\_\_\_\_\_  
PARTICIPANT SIGNATURE

DATE: \_\_\_\_\_

**Accounting for Disclosures**

\_\_\_\_ There were no applicable disclosures made of your health information for the period you specified.

\_\_\_\_ Disclosures of your health information were made by this office to:

**Date of Disclosure**

**Name and Address to Whom Disclosed**

**Description of Information**

**Disclosed**

**Purpose of Disclosure**

We are temporarily unable to process the accounting for disclosures you have requested due to:

\_\_\_\_ a suspension required by law.

\_\_\_\_ other: \_\_\_\_\_

but will comply with your request by the date of: \_\_\_\_\_

If you have any questions concerning this accounting for disclosures, please contact:

\_\_\_\_\_  
Signature of Nurse Coordinator/Vice President, Corporate Counsel

Date: \_\_\_\_\_

# Privacy Official Job Description

## **JOB DESCRIPTION:**

**Job Title:** Privacy Official

**Summary:** The Privacy Official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures covering the privacy of and access to participants' protected health information in compliance with federal and state laws and the practice's information privacy practices.

### **Duties:**

1. Identifies need for, develops, implements, and maintains the practice's policies and procedures for protecting individually identifiable health information, in coordination with the Management Board.
2. Performs information privacy risk assessment and conducts related ongoing compliance monitoring activities in coordination with the practice's other compliance and operational assessment functions.
3. Works with the company's Management Board and legal counsel to develop and maintain appropriate consent forms, authorization forms, notice of privacy practices, business associate contracts, and other documents required under HIPAA's Standards for Privacy of Individually Identifiable Health Information.
4. Ensures compliance with the practice's privacy policies and procedures and consistent application of sanctions for failure to comply with privacy policies for all members of the practice's workforce (as defined in HIPAA's Standards for Privacy of Individually Identifiable Health Information) and business associates.
5. Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the practice's privacy policies and procedures.
6. Oversees, directs, delivers, or ensures delivery of, including the tracking of attendance, information privacy training for the practice and other appropriate parties. Initiates, facilitates, and promotes activities to foster information privacy awareness within the practice and related entities.
7. Reviews all information system-related security plans to ensure alignment between security and privacy practices.
8. Cooperates with the Office of Civil Rights, other legal entities, and Management Board in any compliance reviews or investigations.

**Reporting Relationship:** For this function, the Information Security Officer reports to the Management Board.

**Qualifications:**

Current knowledge of applicable federal and state privacy laws and accreditation/licensure standards pertaining to health care. Familiar with advancements in information privacy strategies and technologies to ensure practice adaptation and compliance. Experience in health information access controls, release of health information, and health information release control strategies and technologies. Demonstrated organization, facilitation, communication, and presentation skills. Professional certification as a Registered Health Information Administrator (RHIA) or Registered Health Information Technician (RHIT) through the American Health Information Management Association (AHIMA) is desirable.

# Overview of Policies and Procedures on Privacy and Security

**Authority:** Vice President, Corporate Counsel

**Purpose:**

***A copy of this document should be given to each staff member.***

While there are many policies directed at singular aspects of privacy and confidentiality, this overview is directed at developing a simple overall guideline for the understanding of the relationship between the staff and the clients of PPA/Paramount Group.

The electronic and paper record resources of PPA/Paramount Group are provided for the singular purpose of facilitating participant care and business processes. Any person who uses PPA/Paramount Group's paper records and/or computing resources for non-business or unauthorized purposes may be subject to disciplinary action, up to and including termination, and civil or criminal legal action.

Management at all levels is responsible for monitoring the actions of their staff and enforcing the intent of this overview. All questions, concerns or infractions should be directed to the Vice President-Corporate Counsel.

## **Prohibited Activities**

The following are examples of prohibited activities:

1. Using PPA/Paramount's computing systems or data for personal business or gain;
2. Specific violations of PPA/Paramount's electronic mail, Internet and facsimile machine policy;
3. Unauthorized browsing of participant, personnel, financial, or other records for the purpose of personal curiosity or with the intent of improperly disclosing the information contained in those records;
4. Interfering with the operation of any PPA/Paramount's computing systems or using a PPA/Paramount computer to disrupt any external computing system;
5. Altering or deleting any of PPA/Paramount's data or software, except when performing authorized business functions; and
6. Installing unauthorized or illegally copied software on any of PPA/Paramount's computer terminals.

## **Responsibilities**

1. Every staff member is accountable for all computing activities he/she performs.
2. Users shall take the following precautions to safeguard systems and data:
  - Unique Passwords and User I.D.;
  - Computers are logged off and shut down at the end of the workday;
  - Non-Staff members are not permitted to use the system;
3. User identification codes are not to be shared, except under special circumstances approved by the Privacy Official.
4. Passwords shall not be divulged, orally or in writing.
5. Workstations and terminals to be left unattended shall be logged off or locked up.
6. All suspected or known breaches of confidentiality or computer security shall be reported to the Vice President, Corporate Counsel or another member of management immediately.

## **Organizational Policies and Training**

The management of PPA/Paramount will instruct users in Information Confidentiality, Privacy, and Security policies, standards, and procedures; and the principles of information confidentiality and computer security.

Each member of the workforce must be trained by April 14, 2003. Each new member of the workforce who begins work after April 14, 2003 shall be trained regarding privacy policies and procedures within a reasonable period of time after the person joins the covered entity's workforce. If there is a change to any policies or procedures related to PHI, each employee affected by such a change shall be trained about the change within a reasonable period of time after the material change becomes effective. We will document that the training described in this policy has been provided. Management of PPA/Paramount shall make written policies on the management of private participant information and other protected data that is readily available to staff.

## **Behavior in Interacting with Participants**

Staff or volunteers of PPA/Paramount are obligated to make sure that medical information is not disclosed *inappropriately, accidentally or negligently*. In order to do this we must take appropriate precautions to safeguard medical information, as described below.

1. Do not allow medical information to be visible to visitors.
2. Keep documents face down. Never leave them out where others can see them.
3. Use confidential trash bins when disposing of medical information. Any documents with a participant's name, insurance number or partial medical record is considered medical information.
4. Speak softly over the phone and try to avoid excessive use of the participant's name.
5. Do not discuss participant information with anyone in a social conversation.
6. Make a habit of speaking to participants in private areas only.
7. Do not discuss the reason for a participants in front of others.
8. Anticipate participant privacy needs when giving out test results, setting up appointments and obtaining or explaining referrals.

## **General Areas for Consideration**

### **Participant's Rights**

1. Right to be informed of their Rights. Responsibilities for implementing procedures for ensuring that the participant is informed of the policies related to participant information should be defined.
2. Right to Privacy. Relevant participant information may only be disclosed to those directly involved in the care of the participant, for the protection of the public health as provided by law, for the payment of services as authorized by the participant, to assist researchers as authorized by the participant, or for any other purposes required by law or authorized by the participant. These rights are defined in the Policy and Procedure on Uses and Disclosures of Protected Health Information.
3. Right to Review Information. Participants are entitled to know which information about them is in the possession of the organization and are entitled to review that information.

Any category of information that may be withheld from the participant in accordance with the law should be defined in the Policy and Procedure on Participant's Right to Access Health Information.

4. Right to Clear and Complete Presentation of Information. Policies related to making information from the computer-based participant record available to the participant in a clear, logical, understandable format should be developed. Any policies for presenting information in a format not maintained by the organization should be defined. The organization's policies related to the costs associated with presentation of information should also be defined.

5. Right to Amend Correct Information. Information cannot be deleted, but erroneous information can be marked as such and correct information amended. The rights of the participant to provide supplemental information or an appendix should also be defined in the Policy and Procedure on Participant's Right to Request Amendment of their Health Information.

6. Right to Restrict the Use and Disclosure of Specific Information. The participant's rights to segment information and block the release of specific information should be clearly stated in the Policy and Procedure to Request Restrictions on Use and Disclosure of Protected Health Information. The rights of the organization to identify and explain any consequences of such blockage should also be included.

7. Right to an Accounting for Disclosures of Information. The participant's rights to know which individuals, organizations, and government agencies have authority to access, and have actually gained access to, specific information identified with the participant should be clearly defined in the Policy and Procedure on Accounting for Disclosures.

8. Right to Protection of Information Released to Third Parties. The policy should define the commitment for protection required from a third party prior to the release of information to that organization. The policy may also specify the responsibility for monitoring these commitments.

9. Right to Integrity and Availability. Records must be protected from unauthorized modification and destruction. The participant has the right to expect that the organization will take reasonable precautions to protect the information from destruction by accident or vandalism, and by fire, flood, earthquake, or other disasters. Policies requiring that provisions be made for the participant records to survive the organization in the event of mergers, bankruptcy, and similar events should be established.

#### Protection of Information

1. Privacy. The caregivers' personal privacy should be preserved. Relevant caregiver information may only be disclosed for the protection of the public health as provided by law, for any other purposes as required by law, or as authorized by the caregiver.

2. Review of Information. The caregiver is entitled to know which information about the caregiver is in the possession of the organization. Caregivers' are also entitled to know which information they have a legal right to review. Caregivers should have the right to review information they have placed in the participant's record.

3. Clear and Complete Presentation of Information. Information about the caregiver and participant information authorized to the caregiver should be made available in a clear, logical, understandable format.
4. Right to Append Corrected Information. The caregivers' rights to identify erroneous information and append correct information pertaining to their employment or contractual arrangements should be defined.
5. Release of Specific Information. The caregiver may be granted the right to segment information and block the release of specific information where permitted by law.
6. Notification of Disclosure of Information. The caregiver is entitled to know which individuals, organizations, and government agencies have authority to access and have actually gained access to information about the caregiver.
7. Protection of Information Released to Third Parties. The policy should define the commitment for protection required from a third party prior to the release of information to that organization.
8. Integrity and Availability of Records. Records must be protected from unauthorized modification and destruction. The caregiver has the right to expect that the organization protect the information from destruction by accident or vandalism, and by fire, flood, earthquake, or other disasters. Provisions must be made for the records to survive the organization in the event of closure, mergers, bankruptcy, and similar events.
9. Responsibility to Protect Information. The caregivers' responsibility for the protection of the information to which the caregiver has access should be stated.

### **The Release of Data**

Although the requirements for release of some participant information are defined by law, PPA/Paramount has policies addressing the responsibilities and determining the methods of complying with these laws.

The organizations policies related to complying with the law for the release of participant, caregiver, and institutional information to public health authorities should be defined.

Factors to consider in the release and sharing of information include:

Which information may be released?

To whom may information be released?

What responsibility does the institution have regarding the protection of information it has released from its custody?

Data should never be released without the express, specific, written consent of the participant or a court order. In all cases, where there is any question as to the appropriateness of the release of data, the Privacy Official, or a member of management, must be contacted for a decision before any data is released.

# Policy and Procedure on Personnel Discipline for Breach of Privacy or Confidentiality

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Vice President, Corporate Counsel

## **Purpose:**

This plan provides guidance for the appropriate response to breaches in participant privacy and confidentiality at PPA/Paramount. This guidance is intended to ensure that staff and management understand the appropriate seriousness of any breach and the stated penalties and actions. PPA/Paramount has a very strong commitment to protecting the confidentiality of its participants' medical records and clinical information. To ensure compliance with the policy by all staff and to ensure consistency in the discipline and actions taken upon evidence of breach in participant confidentiality by staff, PPA/Paramount has adopted the disciplinary process set forth below.

## **General Policy**

PPA/Paramount and its staff are entrusted with information regarding our participants and we recognize that the medical record is highly confidential and must be treated with great respect and care by all staff. Any breach in participant confidentiality by a staff person is subject to formal disciplinary action as delineated in this policy. A breach in participant confidentiality occurs when a member of the PPA/Paramount staff:

- a. views or accesses private participant health information for any reason not related to the provision of care and treatment or another authorized purpose;
- b. discusses with or reveals to any individual(s), private participant health information for purposes not related to participant care and treatment or another authorized purpose; or
- c. violates the provisions of PPA/Paramount's policy on the confidentiality of private participant health information as stated in the general overview policy as provided to the staff.

For any breach in participant confidentiality the staff member shall be subject to disciplinary actions as set forth in the "Procedures" section below.

**Every staff member should receive and read a copy of this document and "Overview of Policies and Practices in Privacy and Security".**

## **Procedures**

1. Review. The Vice President, Corporate Counsel is responsible for the content and administration of this policy. The policy shall be reviewed and evaluated one year from its effective date with specific focus on the Disciplinary Process section, and then every two years thereafter.

2. Level of Breach. Breaches in participant confidentiality have been divided into the following three levels, with the corresponding disciplinary actions for each level of breach.

### **A. Level 1 - Carelessness**

This level of breach occurs when a member of the PPA/Paramount staff unintentionally or carelessly accesses, reviews or reveals participant information to him/herself or others without a legitimate need to know the participant information.

Disciplinary Sanctions:

- 1.) Depending upon the facts, counseling, oral warning, written warning, final written warning or suspension, documented in writing and maintained in the employee's personnel record, or termination.
- 2.) Except in the case of termination, the employee shall be required to repeat the confidentiality training module on his/her own time.
- 3.) Level 1 disciplinary sanctions shall be administered in a progressive manner.
- 4.) Disciplinary sanctions shall be reported to the applicable professional licensing board as appropriate.

### **B. Level 2 - Curiosity or Concern (no personal gain)**

This level of breach occurs when an employee intentionally accesses or discusses participant information for purposes other than the care of the participant or other authorized purposes, but for reasons unrelated to personal gain.

Disciplinary Sanctions:

- 1.) First offense: Depending upon the facts, oral or written warning documented and maintained in the employee's personnel record.
- 2.) Second offense: Depending upon the facts, a final written warning and suspension for 3-30 days without pay, documented and maintained in the employee's personnel record, or termination.
- 3.) Third Offense: Termination.
- 4.) Except in the case of termination, the employee shall be required to repeat the confidentiality training module on his/her own time.
- 5.) Disciplinary sanctions shall be reported to the applicable professional licensing board as appropriate.

### **C. Level 3 - Personal Gain or Malice**

This level of breach occurs when an employee accesses, reviews or discusses participant information for personal gain or with malicious intent.

Disciplinary Sanctions:

- 1.) First offense: Termination.
- 2.) Report to applicable professional licensing board.

3. Disciplinary Process. The following process must be followed when an employee breaches, or is suspected of breaching, participant confidentiality.

### **A. Initial Reporting**

- 1) Individual who observes or is aware of a breach reports it to Vice President, Corporate Counsel (Privacy Official.)
- 2)The Vice President, Corporate Counsel (Privacy Official) reports this to the President, who consults with the Management Board as appropriate.
- 3)Failure to report a breach of which one has knowledge will result in appropriate disciplinary action.
- 4)Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

#### **B. Activity Upon Clear Evidence of Breach of Confidentiality**

- 1)Document suspected breach.
- 2)Request written response.
- 3)Vice President, Corporate Counsel (Privacy Official) reports this to the President, who consults with the Management Board as appropriate.
- 4)Vice President, Corporate Counsel (Privacy Official)will reprimand or dismiss party. Staff to repeat privacy training.

#### **C. Reporting and Filing Requirements**

- 1)Document the breach.
- 2)Copies of breach will go to Vice President, Corporate Counsel (Privacy Official), staff member, management board and personnel file.

#### **D. Imposition of Appropriate Discipline**

For all levels of breach, after final resolution, the initial report and all written documentation relating to the breach shall be filed in a confidential file in the Privacy Official's office and a referring note placed in the Security Log. The disciplinary action and appropriate documentation shall also be placed in the employee's personnel file.

4. Upon investigation of a level breach, or higher, the following actions should be taken.
  - a. The Privacy Official should ensure that the access of the accused employee to any paper or electronic medical records is immediately suspended.
  - b. The Privacy Official should retrieve keys and/or badges from the accused employee that allow access to secure areas where participant records are kept.
  - c. The Privacy Official should inform all appropriate supervisors about the suspension or removal of the access privileges of the accused employee.
  - d. The Privacy Official should include a written report of all actions in the a confidential file in the Privacy Official's office and a referring note placed in the Security Log. The disciplinary action and appropriate documentation shall also be placed in the employee's personnel file.

After reading this policy, sign and date the next page and return to your immediate supervisor. Detach the acknowledgement and retain the policy for your records.

## ACKNOWLEDGEMENT

I have received a copy of Private Practice Associate, LLC/Paramount Group, LLC's *Policy and Procedure on Personnel Discipline for Breach of Privacy or Confidentiality* and *Overview of Policies and Procedures on Privacy and Security*.

I agree to keep all Private Practice Associate, LLC /Paramount Group, LLC's participant information, as outlined in the above documents, strictly confidential. I understand that a breach in participant confidentiality, as defined in the above documents, will result in disciplinary action, up to and including termination of employment.

**Name:** \_\_\_\_\_

**Date:** \_\_\_\_\_

# Policy and Procedure on Physical Security

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Vice President, Corporate Counsel

**Purpose:**

A Physical Security policy document should exist detailing the measures taken to protect buildings in regard to disasters (flooding, fire, earthquakes, explosions, power outage), theft, physical access, computer rooms and wiring cabinets.

**General Policy:**

All PPA/Paramount staff should understand and support the control of access to the public, clients, general staff and staff with specific access privileges. Upon observation or detection of any breach of physical access, staff members should implement provisions of the procedures below according to their best judgement, but in all instances a follow-up report should be made to the Vice President, Corporate Counsel for action and record.

The Vice President, Corporate Counsel has overall responsibility for physical security and for oversight of procedures listed below. In the event that the Vice President, Corporate Counsel is unavailable, the Vice President, Operations will assume responsibility for the procedures in this policy.

**Procedures:**

1. Definition of Areas

- Zone 1: Areas open to the public;
- Zone 2: Areas not open to the public, open to company clients and staff;
- Zone 3: Areas not open to the public, not open to company clients, open to staff only;
- Zone 4: Protected areas. Only accessible with identification, access strictly controlled.

2. Warning Signs

Signs clearly identifying the right of access to an area should be placed at every juncture between zones. All staff should be clearly aware of requirements and should not hesitate to challenge inappropriate persons. Specific badges and or actual tokens may be issued to validate authorized entry into different areas.

3. Emergency Telephone Numbers

Emergency telephone numbers for private security, police, plumber, etc. should be placed at all telephone handsets. If possible, the Vice President, Corporate Counsel should manage incidents or disasters, but in emergency situations, the call should be made by any available staff member. In all instances, follow-up reports should be made to the Vice President, Corporate Counsel for recording in a confidential file.

#### 4. Response to Physical Intrusion or Any Disaster

a. When staff, clients and/or participants are present:

- 1.) Staff should take the immediate, appropriate action to safeguard the clients and/or participants, confidential participant information and the physical and electronic infrastructure.
- 2.) The Vice President, Corporate Counsel , the Vice President, Operations or the most available staff member should call the appropriate authorities to respond to the situation.
- 3.) In all instances, follow-up reports should be made to the Vice President, Corporate Counsel for recording in a confidential file.

b. Detected outside of hours of operation:

- 1.) If immediate action is necessary, arrangements should be made for the office's security service to contact the Vice President, Corporate Counsel , or the Vice President, Operations in the event that the Vice President, Corporate Counsel is unavailable, who should contact the appropriate authorities and take any necessary steps to secure the premises until a complete evaluation of the damage can be made.
- 2.) In all instances, follow-up reports should be made to the Vice President, Corporate Counsel for recording in a confidential file.
- 3.) If no immediate action is necessary to mitigate the loss, reports should be made to the Vice President, Corporate Counsel for action and for recording in a confidential file.

#### 5. Routine Destruction of Paper Records

Paper records with private health information printed on them should not be discarded as regular trash. All paper that has private health information printed on it should be segregated from regular trash and destroyed only by methods that ensure the privacy and confidentiality of the information.

#### 6. Routine Destruction of Defective Confidential Disks and Tapes

Disks, tapes or any other storage medium with private health information contained on it should not be discarded as regular trash. All storage mediums that have private health information contained on them should be segregated from regular trash and destroyed only by methods that ensure the privacy and confidentiality of the information.

#### 7. Repair and/or Access to Computer Equipment

Access to private participant information by any service technician should be minimized either by direct supervision or by securing the information source. If possible, business associate contracts should be in place for each type of service technician.

#### 8. Prevention

- a. Clear instructions on the right of access to an area should be posted at all junctures between zones.
- b. All staff should be proactive about monitoring access to restricted zones.
- c. Access to restricted zones for repair or delivery should be minimized and those entrants should understand PPA/Paramount's confidentiality requirements.
- d. Any support contracts that involve on-site, non-staff personnel should include standard Business Associate Contract language on privacy, confidentiality and security.
- e. Staff identification and/or badges should be implemented, if not already in use.
- f. Procedure on locking doors and windows should be clearly understood by all staff members. While all staff members should enforce the procedure, it is the responsibility of the Vice President, Corporate Counsel to monitor these physical security actions. In the event of the absence of the Vice President, Corporate Counsel , the Vice President, Operations will assume responsibility for monitoring these physical security

procedures.

g. Upon termination of a staff member for any cause, all office keys should be retrieved from the departing staff member.

h. Key registers and logs should be maintained by the Vice President, Operations.

i. Keys that are marked "Do Not Duplicate" should be issued to staff members to avoid unauthorized copies of office keys being made.

## 9. Work Station Use

a. Workstations should be placed, as much as possible, so that the screens are not seen by unauthorized persons.

b. Systems should be configured so that monitors time out after 10 minutes of non-use and require a password to re-enter.

c. If there is no automatic screen shut down within the system configuration, users should logout of the computer system if the user leaves the terminal unattended.

d. If the configuration of the workstations vary across the system, signage should be used to indicate the preferred mode of behavior at each station.

## 10. Record Handling

a. Records should not be left on desks or cabinets unattended.

b. Records pulled from cabinets for future treatment session should be left in a secured area until needed by staff members.

c. All staff should pro-actively gather up unattended records and return them to a secured area.

# Policy on Use of Electronic Mail, Internet and Facsimile Machines

**Authority:** Vice President, Corporate Counsel

**Responsibility:** Vice President, Corporate Counsel

## **Purpose:**

This plan provides guidance for the appropriate use of electronic mail, Internet and facsimile machines at PPA/Paramount Group, LLC. This guidance is intended to ensure the privacy and confidentiality of participant data at PPA/Paramount.

## **General Policy**

Never forward participant-identifiable data to a third party without the participant's express permission. Material that is sexually explicit, obscene, embarrassing, fraudulent, hostile, harassing, or otherwise inappropriate or unlawful shall not be forwarded or sent by electronic communication or displayed on or stored on company computer resources. Users receiving or viewing this kind of information shall immediately report the incident to the Vice President, Corporate Counsel.

Unless expressly authorized by the Vice President, Corporate Counsel, downloading, sending, transmitting, or otherwise disseminating proprietary information, trade secrets, or other sensitive privacy act information is strictly prohibited.

### 1. Electronic Mail

Paramount Group, LLC owns the electronic mail service, and considers electronic-mail private, direct communication between sender and recipient(s) or recipient(s)' designee(s); however, employees cannot expect absolute confidentiality. The contents will not be monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender and recipient(s) or recipient(s)' designee(s) unless specifically authorized by the Privacy Official, a law enforcement representative or the Information Security Official.

Electronic mail is considered official correspondence of PPA/Paramount, and users must avoid the inclusion of inappropriate or derogatory language in their messages.

Electronic mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion. The messages may be disclosed in the same manner as paper records. Reasons for recovery of electronic mail messages may include legal discovery, external investigations by law enforcement personnel and internal security investigations.

A recipient may designate another employee to receive and read work-related mail for business reasons. Personal messages are forwarded to the intended recipient. If that is not possible, they are destroyed. Messages are not examined further than is necessary to determine the category into which they fall.

In anticipation of the finalization of the Security Regulation of HIPAA, no personally identifiable health information should be sent by public or private electronic networks without adequate safeguards against interception and/or misuse.

## 2. Internet

Standard use of the Internet, via the office network, must be primarily for PPA/Paramount business or professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade PPA/Paramount's public image through their activities or adversely affect the availability of network resources.

## 3. Facsimile Machines

All staff shall take precautions when using facsimile (fax) machines to transmit documents. Facsimile machines shall not be located in areas accessible to the general public, unless the facsimile machine is intended for public use. In this case the publicly available facsimile machine should not be used by staff members to send or receive faxes containing participant information of any kind.

Staff shall not use company facsimile machines for transmitting personal documents.

Facsimile machine cover pages shall include the following information:

- a. The sender's name, business address, business phone number, and business facsimile machine number;
- b. the recipient's name, business address, business phone number, and business facsimile machine number;
- c. transmission time and date (if not stamped by facsimile machine or computer);
- d. classification of the document (CONFIDENTIAL documents).

Staff shall verify the facsimile machine number of the recipient before transmitting.

A recipient of a document containing CONFIDENTIAL information (e.g., for the recipient's eyes only or containing participant-identifiable information) must be notified by phone before the document is transmitted. If at all possible, this type of document should not be faxed.

All pages, including the cover page, of CONFIDENTIAL documents to be faxed must be marked "Confidential" before they are transmitted.

Time, date, sender, recipient, and sender or recipient phone number for all materials sent and received by facsimile machine should be documented in a facsimile machine log to be kept with the facsimile machine. It is crucial that no personal health data be explicitly revealed in this log.