**HIPAA Voluntary Compliance Manual for PMCs**

**Instructions**

 This manual was created to assist Pregnancy Medical Clinics (PMCs) to voluntarily comply with federal Health Insurance Portability and Accountability Act (**HIPAA***)*standards. There may be additional state requirements that will require these Policies & Procedures and Forms to be modified. **NIFLA** and the Alliance Defending Freedom (**ADF**) are partnering to research each state’s medical privacy laws.

 Review: 1) ***Legal Tips,*** August 2013***, 2) Legal Tips*** September 2013***,*** and 3) ***Clinic Tips,*** September 2013, for important legal information regarding the Forms and Policies and Procedures contained herein.

 **NIFLA** strongly recommends that you adopt the following Policies & Procedures and Forms to conform them to your operations as soon as possible. The first step is to appoint a Privacy Officer, usually the Nurse Manager, who will implement these Policies & Procedures and Forms your PMC.

**Table of Contents**

1. ***Protected Health Information (PHI) – Policy & Procedure Page 2-4***

 ***Form:*** Patient Permission to Use Images and Medical Information in Publications and Promotional Materials

1. ***Notice of Privacy Practices (NPP) – Policy & Procedure Page 5-11***

 ***Form:*** Notice of Privacy Practices

 ***Form:*** Notice of Privacy Practices Acknowledgement

1. ***Release of Health Information – Policy & Procedure Page 12-13***

 ***Form:*** Authorization for Release of Health Information

1. ***Business Associate Agreements (BAA) – Policy & Procedure Page 14-17***

 ***Form:*** Business Associate Agreement

1. ***Contact by Telephone, Email, Fax or Text – Policy & Procedure Page 18-19***

1. ***Breach Assessment and Notification – Policy & Procedure Page 20-21***
2. ***HIPAA Training – Policy & Procedure Page 22-23***

 ***Form*:** **HIPAA** Training Verification

**© 2013 National Institute of Family and Life Advocates. All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means – electronic, mechanical, photocopying, recording, or otherwise – without prior permission.**

**Policy: Protected Health Information (PHI)**

 The Pregnancy Medical Clinic (PMC) will take reasonable steps to limit the use of, disclosure of, and requests for Protected Health Information (**PHI)** to the minimum necessary to accomplish the intended purpose.

**Procedure:**

1. **PHI** will be kept private and secure. The Privacy Officer will conduct regular risk assessments to ensure the privacy and security of all **PHI** collected and maintained by the PMC. See *Guidance on Risk Analysis Requirements at:* [*http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html*](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html)

2. Electronic records will be password protected. Other records will be maintained in secure files and kept in locked file cabinets and/or rooms. Access to **PHI** will be limited to personnel who have a reasonable need to use such information.

3. Use or disclosure of **PHI** will be allowed to occur without the patient's prior authorization when undertaken for purposes of treatment or related to the PMC’s healthcare operations. For other uses or disclosures, the PMC will seek prior authorization from the patient, except when such use or disclosure may be required by law, required for public health reasons, required to avert a threat of harm to the patient or a third person, or when other circumstances may reasonably warrant such use or disclosure without prior authorization.

4. Each patient will be given a written Notice of Privacy Policy (**NPP**) describing how health information may be used or disclosed by the PMC. The **NPP** should also include a description of the instances in which advance authorization for use or disclosure may or may not be sought and a description of the steps that the patient may exercise with respect to her own health information.

5. Written authorization will be obtained from each patient for any use or disclosure of health information for which such prior authorization is warranted as described above. See Form: *Authorization for Release of Health Information*.

6. Any outside disclosure of health information will be limited only to the minimum amount of information that is reasonably necessary to accomplish the specific purpose(s).

7. For each patient, an accounting will be made of each outside disclosure of health information and those records will be kept for at least 7 years after the last disclosure. The Privacy Officer shall prepare such accounting.

8. Each patient will be notified that she may inspect and copy her health information, that she may request restrictions on the use or disclosure of her health information, that she may request amendments to her health information and that she may find out what disclosures have been made to outside persons. Requests for inspection and copying shall be responded to within 30 days. Requests for restrictions on use and disclosure or requests for amendments of health information shall be responded to within 60 days. In the event of denial of any requests to restrict the usage or disclosure of health information or the denial of any requests to amend health information, the patient will be given a written notice of such denial and an explanation of the reasons. The Privacy Officer shall handle all such requests.

9. Privacy and security of **PHI** shall be promoted by the following:

* Making sure no **PHI** is viewable or accessible by other patients or 3rd parties;
* Speaking quietly when discussing or talking with a patient in the reception area, a waiting room, hallway or other public area;
* Posting signs to remind staff/volunteers to protect patient confidentiality;
* Isolating or locking file cabinets or records rooms and limiting access to same;
* Providing additional security, such as passwords, on computers/networks maintaining **PHI** and having staff turn their computers off when away from their desks.
* Limiting whom within the entity has access to **PHI**, based on who needs access to perform their job duties. Only doctors, nurses, or others involved in treatment may have access to the entire medical record, as needed.
* Only authorized personnel shall have access to the online database and the database must be password protected.
* Maintaining a secure firewall and routinely reviewing information system activity in order to detect any breach in the firewall.
* Not allowing **PHI** on laptop computers or other portable electronic devices.
* If questioned about a patient’s record and there is no existing written authorization, the correct response is: “Due to confidentiality, I cannot verify the patient has ever been seen or treated at the PMC, nor can I tell you that the requested records are on file.”

10. The PMC and its Business Associates shall not offer **PHI** for sale or use it to fundraise or market. In the event the PMC wants to use a patient’s story for promotional material, a signed Release must be obtained from the patient and all identifying information removed prior to publication. See Form: *Patient Permission To Use Images and Medical Information In Publications and Promotional Materials*

11. If the PMC’s copier is a digital copier, the security features on the copier must be used to protect **PHI**. At least monthly and before all service calls, the Privacy Officer shall securely overwrite the entire hard drive. If a copier has a hard drive, it shall be removed prior to selling and/or returning to another party.

12. When upgrading systems and software, the Privacy Officer must perform an appropriate technical evaluation to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the internet.

13. Patients will be given an opportunity on the intake sheet to indicate how the PMC may contact them, via, phone, text, email, or mail. The patient has a right to request to receive confidential communications by alternative means or at alternative locations.

14. Ultrasound reports sent off-site, whether electronically or physically, to a Physician to review shall have all **PHI** removed and a code provided in place of the patient’s name.

15. All Clinic employees and volunteers will be trained concerning these procedures.

**PATIENT PERMISSION TO USE IMAGES AND**

**MEDICAL INFORMATION IN PUBLICATIONS**

**AND PROMOTIONAL MATERIALS**

The Pregnancy Medical Clinic (PMC) is committed to protecting the privacy of our patients’ medical information. We must obtain your written consent before we can photograph you and your baby or reveal details about your care for use in publications or promotional materials. Please review the form and be assured your questions are fully answered by a PMC staff member before signing this form. You are entitled to receive a signed copy.

Only you and your team of medical caregivers may provide details about your case for promotional purposes, such as advertising, brochures, web pages, publications or news stories. Once stories, photos, audio and videotape enter the public domain, it’s important to understand that other outlets are free to use them. We cannot guarantee that other organizations will not display your publicized images or information.

Signing this form is your choice and will have no effect upon your medical care, fees or insurance benefits. You may cancel or revoke your authorization at any time by writing to PMC, address… ; however, if we have already used the information and disclosed it as provided by the authorization, we will not be able to revoke your authorization.

Please list specific information you do **NOT** want disclosed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please initial if you want us to use a fictitious name and not your real name: \_\_\_\_\_\_\_

You agree to the use of photos of you and your baby and the publication of your story, including medical information/ultrasound photographs by PMC for brochures, publications, websites, promotional material in newspaper, television, radio, magazines and online publications and marketing/advertising by PMC. You agree to waive any and all rights, claims, actions that you or your baby may have against PMC arising from the publication and use of your story and photographs.

-----------------------------------------------------------------------------------------------------------

I have read this form, and all of my questions have been answered. My signature confirms that I understand and accept all of the above conditions, and approve the use of my and my baby’s images, stories and private health information by PMC.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Signature (Patient or Guardian) Print Patient Name Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Relationship to Patient Email Address Phone(s)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mailing Address

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Print PMC Rep’s Name Signature Date

**POLICY: Notice of Privacy Practices**

Pursuant to the Health Insurance Portability and Accountability Act (**HIPAA)**, the Pregnancy Medical Clinic (PMC) has developed a notice for patients, which provides a clear explanation of privacy rights and practices as it relates to private health information.

**PROCEDURE:**

 1. A **Notice of Privacy Practices (NPP),** that describes how the PMC may use or disclose protected health information and an individual’s rights with respect to the privacy of that information, shall be prepared by the Privacy Officer for use at the PMC. The notice must include an effective date.

 See Sample: ***Notice of Privacy Practices*.**

 2. The Privacy Officer shall promptly revise and distribute this notice whenever there are material changes to any privacy practices.

 3. The PMC shall post the **NPP** in a clear and prominent location at the facility and make a copy available to patients.

 4. The PMC shall prominently post and make available the **NPP** on any website it maintains that provides information about its customer services or benefits.

 5. The PMC shall provide the notice to each patient no later than the date of first service delivery and, except in an emergency treatment situation, make a good faith effort to obtain the individual’s written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained. The Acknowledgement Form shall be placed in the patient’s file. See Form: *Notice of Privacy Practices Acknowledgement.*

 6. When first service delivery to an individual is provided over the internet, through email, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the individual’s first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice. The receipt shall be placed in the patient’s file.

 7. The PMC shall make the **NPP** available at the provider’s office or facility for individuals to request to take with them.

 8. The PMC may email the notice to an individual if the individual agrees to receive an electronic notice.

**(On PMC Letterhead)**

**Privacy Officer Name and Contact Information:**

**Effective Date of Notice:**

NOTICE OF PRIVACY PRACTICES[[1]](#footnote-1)

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

# **Your Rights**

You have the right to:

* Get a copy of your paper or electronic medical record
* Correct your paper or electronic medical record
* Request confidential communication
* Ask us to limit the information we share
* Get a list of those with whom we’ve shared your information
* Get a copy of this privacy notice
* Choose someone to act for you
* File a complaint if you believe your privacy rights have been violated

# Your Choices

You have some choices in the way that we use and share information as we:

* Tell family and friends about your condition
* Provide disaster relief
* Provide mental health care
* Market our services and sell your information
* Raise funds

# Our Uses and Disclosures

We may use and share your information as we:

|  |
| --- |
| * Treat you
* Run our organization
* Bill for your services
* Help with public health and safety issues
* Do research
* Comply with the law
* Respond to organ and tissue donation requests
* Work with a medical examiner or funeral director
* Address workers’ compensation, law enforcement, and other government requests
* Respond to lawsuits and legal actions
 |

# Your Rights

**When it comes to your health information, you have certain rights.** This section explains your rights and some of our responsibilities to help you. **Get an electronic or paper copy of your medical record.**

* You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
* We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

**Ask us to correct your medical record**

* You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
* We may say “no” to your request, but we’ll tell you why in writing within 60 days.

**Request confidential communications**

* You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
* We will say “yes” to all reasonable requests.

**Ask us to limit what we use or share**

* You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say “no” if it would affect your care.
* If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health provider. We will say “yes” unless a law requires us to share that information.

**Get a list of those with whom we’ve shared information**

* You can ask for a list (accounting) of the times we’ve shared your health information for six years prior to the date you ask, who we shared it with, and why.
* We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We’ll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

**Get a copy of this privacy notice**

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

**Choose someone to act for you**

* If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
* We will make sure the person has this authority and can act for you before we take any action.

**File a complaint if you feel your rights are violated**

* You can complain if you feel we have violated your rights by contacting us using the information on page 1.
* You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting [**www.hhs.gov/ocr/privacy/hipaa/complaints/**](http://www.hhs.gov/ocr/privacy/hipaa/complaints/)**.**
* We will not retaliate against you for filing a complaint.

# Your Choices

**For certain health information, you can tell us your choices about what we share.** If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

* Share information with your family, close friends, or others involved in your care
* Share information in a disaster relief situation
* Include your information in a hospital directory

*If you are not able to tell us your preference, for example if you are unconscious, we may share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*

In these cases, we never share your information unless you give us written permission:

* Marketing purposes
* Sale of your information
* Most sharing of psychotherapy notes

In the case of fundraising:

* We may contact you for fundraising efforts, but you can tell us not to contact you again.

# Our Uses and Disclosures

## How do we typically use or share your health information?

We use or share your health information in the following ways:

**Treat you**

We use your health information and share it with other professionals who are treating you.

*Example: A doctor treating you for an injury asks another doctor about your overall health condition.*

**Run our organization**

We use and share your health information to run our practice, improve your care, and contact you when necessary.

*Example: We use health information about you to manage your treatment and services.*

**Bill for your services**

We can use and share your health information to bill and get payment from health plans or other entities.

*Example: We give information about you to your health insurance plan so it will pay for your services.*

## **How else can we use or share your health information?**

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information, see: [www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html).

**Help with public health and safety issues**

We can share health information about you for certain situations such as:

* Preventing disease
* Helping with product recalls
* Reporting adverse reactions to medications
* Reporting suspected abuse, neglect, or domestic violence
* Preventing or reducing a serious threat to anyone’s health or safety

**Do research**

We can use or share your information for health research.

**Comply with the law**

We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we’re complying with federal privacy law.

**Respond to organ and tissue donation requests**

We can share health information about you with organ procurement organizations.

**Work with a medical examiner or funeral director**

We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

**Address workers’ compensation, law enforcement, and other government requests**

We can use or share health information about you:

* For workers’ compensation claims
* For law enforcement purposes or with a law enforcement official
* With health oversight agencies for activities authorized by law
* For special government functions such as military, national security, and presidential protective services

**Respond to lawsuits and legal actions**

We can share health information about you in response to a court or administrative order, or in response to a subpoena.

# Our Responsibilities:

* We are required by law to maintain the privacy and security of your protected health information.
* We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
* We must follow the duties and privacy practices described in this notice and give you a copy of it.
* We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information: [www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html).

# **Changes to the Terms of this Notice**

# We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our website.

**(On PMC Letterhead)**

 **Notice of Privacy Practices Acknowledgement**

 **Notice of Privacy Practices (NPP)** is provided to all patients. This **Notice of Privacy Practices** identifies: 1) how medical information about you may be used or disclosed; 2) your rights to access your medical information, amend your medical information, request an accounting of disclosures of your medical information, and request additional restrictions on our uses and disclosures of that information; 3) your rights to complain if you believe your privacy rights have been violated; and 4) our responsibilities for maintaining the privacy of your medical information.

 The undersigned certifies that he/she has read the foregoing, received a copy of the **Notice of Privacy Practices** and is the patient, or the patient’s personal representative.

Name of Patient Signature of Patient

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

Name of Patient’s Personal Representative Signature of Representative

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

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 *FOR INTERNAL USE ONLY*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Employee Signature of Employee

If applicable, reason patient’s written acknowledgement could not be obtained:

\_\_Patient was unable to sign.

\_\_Patient refused to sign

\_\_Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Policy: Release of Health Information**

 Patient health information will be made available to patients upon their request.

**Procedures:**

**Releasing to Patient:**

1. A patient who requests her medical records will be required to come to the office during regular business hours, provide proof of identity, and sign an *Authorization to Release Health Information* Form.

2. Medical records will only be released in person to the patient upon proof of identity, except in emergency situations.

3. The medical record may be stored in the same file as the advocacy record, or may be kept completely separate. The advocacy record is not to be included in the medical record given to the patient unless she initiates the request for same. The medical record should not be included in the same file as the Earn While You Learn or other parenting type file.

**Release to Third Parties:**

1. All patient files are confidential. Information therein shall be released to third parties only upon written authorization from the patient. The patient must sign an *Authorization to Release Health Information* Form and clearly identify the designated 3rd party to receive the record. The written authorization will be time limited and not exceed 90 days from the date of signature. A staff person will witness the written authorization and the patient will need to show proof of identity.

2. If patient records are subpoenaed, the Nurse/Clinic Director should immediately contact legal counsel as there may be patient-doctor privileges that would prohibit complying with the subpoena.

3. No medical records will be released to other practitioners unless an *Authorization to Release Health Information* is on file with the Pregnancy Medical Clinic (PMC). Faxed authorizations from other offices will not suffice. The only exception is if the patient is facing an emergency and the records are needed by another medical professional immediately.

**Timing and Fees:**

A request for medical records must be responded to within 30 days (*check state law*), except in emergency situations and a reasonable fee to cover costs of copying may be charged the patient.

**AUTHORIZATION FOR RELEASE OF**

**HEALTH INFORMATION**

I request that health information regarding my care and treatment be released as set forth on this form and in accordance with the ***Health Insurance Portability and Accountability Act of 1996 (HIPAA).***

I understand that:

1. I hereby authorize release of my information by the Pregnancy Medical Clinic (PMC) in a secure manner.

2. I have the right to revoke this authorization at any time in writing to the PMC. I understand that I may revoke this authorization except to the extent that action has already been taken based on this authorization.

3. I understand that signing this authorization is voluntary.

4. I understand the information to be released or disclosed may include information relating to sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV), and alcohol and drug abuse. I authorize the release or disclosure of this type of information.

5. Name and address of agencies to which you are authorized to release information:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Specific information to be released:

\_\_ Medical Records from \_\_\_ / \_\_\_ / \_\_\_\_\_\_ to \_\_\_ / \_\_\_ / \_\_\_\_\_\_

\_\_ Entire Medical Record, including patient histories, nursing notes (not psychotherapy notes), test results, radiology studies, films, referrals, consults, billing records, insurance records, and records sent to you by other healthcare providers.

 \_\_ Ultrasound Report

 \_\_ Verification of Positive Pregnancy Test

 \_\_ Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. This authorization will expire in thirty (30) days unless otherwise noted: \_\_\_\_\_\_\_

All items on this form have been completed and my questions about this form have been answered. In addition, I have been provided a copy of this form.

Patient’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date of Birth: \_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Patient or Legally Authorized Representative Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and Relationship of Legally Authorized Representative to Patient

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 **For Internal Use Only**

**\_\_\_\_Photo ID obtained \_\_\_\_Copy Attached Staff Initial:\_\_\_\_\_\_\_**

**Policy: Business Associate Agreements**

 The Pregnancy Medical Clinic (PMC) will allow its business associates to create, receive, maintain, or transmit Protected Health Information (**PHI**) on its behalf, only if the PMC obtains satisfactory written assurance that the business associate will appropriately maintain the privacy and security of the **PHI** and fulfill the Health Insurance Portability and Accountability Act (**HIPAA)** business associate obligations. The PMC shall have Business Associate Agreements (**BAA**) signed by each business associate.

**Procedure:**

1. The Privacy Officer will identify all business associates who have non-incidental access to **PHI**. Other than a member of the workforce of the PMC, business associates include anyone who provides a service on behalf of the PMC, which involves the use or disclosure of **PHI**. Also included are businesses pertaining to claims processing, data analysis, processing for administration, utilization review, quality assurance, billing, benefit management, practice management; or a person who provides legal, actuarial, accounting, consulting, data aggregation, research, management, administrative, accreditation or financial services to the organization and has access to **PHI**.

2. The Business Associate must enter into a Business Associate Agreement with the PMC (See Form: *Business Associate Agreement*.) and also ensure that their subcontractors comply with the Business Associate Agreement as well.

3. Examples of vendors that are likely to be deemed Business Associates:

* Providers of data transmission services, to the extent they require “routine access” to the **PHI**;
* Data storage or document storage vendors – whether or not they view the **PHI** they maintain;
* Operators of portals or other interfaces created on behalf of covered entities that allow patients to share their data with the covered entity; and
* Entities that provide oversight and governance for electronic health information exchanges.

4. Examples of vendors who are not Business Associates:

* Other health care providers to whom the PMC transmits the patient’s medical chart for treatment purposes.
* A laboratory that does the testing of PMC’s patients.
* Janitorial service whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.
* A person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.
* Plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician’s office, so they do not meet the definition of a “business associate”.

**Business Associate Agreement**\*

\*Modified from Sample provided by U.S. Department of Health and Human Services:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>

This Agreement is effective as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ by and between:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (“Pregnancy Medical Clinic”) and

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Business Associate”)

to set forth the terms and conditions under which “protected health information” (**PHI**), as defined by the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) and Regulations enacted hereunder, created or received by (“Business Associate”) on behalf of (“Pregnancy Medical Clinic”) may be used or disclosed.

**RECITALS**

WHEREAS, Pregnancy Medical Clinic (PMC) has engaged Business Associate to perform services or provide goods, or both;

WHEREAS, Pregnancy Medical Clinic possesses Protected Health Information that is protected under Health Insurance Portability and Accountability Act (**HIPAA)** and the **HIPAA** Regulations, and is permitted to use or disclose such information only in accordance with **HIPAA** and the **HIPAA** Regulations;

WHEREAS, Business Associate may receive such information from Pregnancy Medical Clinic, or create and receive such information on behalf of Pregnancy Medical Clinic, in order to perform certain of the services or provide certain of the goods, or both; and

WHEREAS, Pregnancy Medical Clinic wishes to ensure that Business Associate will appropriately safeguard Protected Health Information;

NOW THEREFORE, Pregnancy Medical Clinic and Business Associate agree as follows:

1. Definitions

The terms used in this Agreement shall have the same meaning as those terms in the **HIPAA**  Rules.  “**HIPAA** Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations and Activities of Business Associate. Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Immediately report to Pregnancy Medical Clinic any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the Pregnancy Medical Clinic as necessary to satisfy Pregnancy Medical Clinic’s obligations under 45 CFR 164.524;

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Pregnancy Medical Clinic pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Pregnancy Medical Clinic’s obligations under 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to the Pregnancy Medical Clinic as necessary to satisfy Pregnancy Medical Clinic’s obligations under 45 CFR 164.528;

(h)  To the extent the business associate is to carry out one or more of Pregnancy Medical Clinic's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Pregnancy Medical Clinic in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the **HIPAA** Rules.

3.   Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information as necessary to perform the services set forth in Service Agreement and to de-identify the information in accordance with 45 CFR 164.514(a)-(c) if requested by the Pregnancy Medical Clinic.

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information consistent with Pregnancy Medical Clinic’s minimum necessary policies and procedures.

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Pregnancy Medical Clinic

(e) Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) Business associate may provide data aggregation services relating to the health care operations of the Pregnancy Medical Clinic.

4. Inform Business Associate of Privacy Practices and Restrictions

(a) Pregnancy Medical Clinic shall notify business associate of any limitation(s) in the notice of privacy practices of Pregnancy Medical Clinic under 45 CFR 164.520, to the extent that such limitation may affect business associate’s use or disclosure of protected health information.

(b) Pregnancy Medical Clinic shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate’s use or disclosure of protected health information.

(c) Pregnancy Medical Clinic shall notify business associate of any restriction on the use or disclosure of protected health information that Pregnancy Medical Clinic has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate’s use or disclosure of protected health information.

5. Term and Termination

(a) Term: The Term of this Agreement shall be effective as of the date above and shall terminate upon conclusion of services between the parties or on the date Pregnancy Medical Clinic terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause: Business associate authorizes termination of this Agreement by Pregnancy Medical Clinic, if Pregnancy Medical Clinic determines business associate has violated a material term of the Agreement and business associate has not cured the breach or ended the violation within the time specified by Pregnancy Medical Clinic.

(c) Obligations of Business Associate upon Termination:

Upon termination of this Agreement for any reason, business associate shall return to Pregnancy Medical Clinic all protected health information received from Pregnancy Medical Clinic, or created, maintained, or received by business associate on behalf of Pregnancy Medical Clinic that the business associate still maintains in any form.  Business associate shall retain no copies of the protected health information.

(d) Survival:  The obligations of business associate under this Section shall survive the termination of this Agreement.

6. Indemnification.

Business Associate shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless Pregnancy Medical Clinic and his/her respective employees, directors, and agents from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney fees, including at trial and on appeal) asserted or imposed against any them arising out of the acts or omissions of Business Associate or any of Business Associate’s employees, directors, or agents related to the performance or nonperformance of this Agreement.

7. Miscellaneous

(a) Regulatory References: A reference in this Agreement to a section in the **HIPAA** Rules means the section as in effect or as amended.

(b) Amendment: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the **HIPAA** Rules and any other applicable law.

(c) Interpretation: Any ambiguity in this Agreement shall be interpreted to permit compliance with the **HIPAA** Rules.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Pregnancy Medical Clinic Name of Business Associate

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Authorized Representative Signature of Authorized Representative

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name/Title of Authorized Representative Name/Title of Authorized Representative

**Policy: Contact by Telephone, Email, Fax or Text**

The Pregnancy Medical Clinic (PMC) will ensure that disclosures of Protected Health Information (**PHI**) by telephone, fax, text or email are relayed in a confidential and secure manner and are restricted to the minimum necessary to achieve the business purpose.

**Procedure:**

1.Staff and volunteers caring for patients must be aware of the patient-approved methods of communication designated on the patient’s intake sheet as well as any documented restrictions (e.g. requests for confidential communications) on the release of patient information.

2. After verifying the acceptable method(s) of communication and the identity and authority of the recipient, staff and volunteers must follow the applicable procedures below to ensure the security of **PHI**.

Telephone Disclosures:

* Only speak directly with the patient, verifying identity with exchange of information.
* If approved by patient, messages left on answering machines should be limited to the caller’s first name, who she/he is calling, and a number to return the call.
* If approved by the patient, appointment reminders may be left on a patient’s voicemail, but only the minimum amount of information necessary.

 Email Disclosures:

* Obtain written permission to communicate via email as part of the patient intake process. Do not communicate by email without the patient’s written permission.
* Always double-check the email recipient prior to sending and limit recipient list to the minimum necessary.
* Avoid emailing **PHI** when possible and always use secure email.
* Utilize the following language on the bottom of all emails: *This message is intended only for the addressee and may contain information that is confidential or privileged. Unauthorized use is strictly prohibited and may be unlawful. If you are not the addressee, you should not read, copy, disclose or otherwise use this message, except for the purpose of delivery to the addressee. If this email is incomplete or illegible, or has been received in error, please call the PMC Privacy Officer at (\_\_\_) \_\_\_-\_\_\_\_.*

Fax Disclosures:

* Only fax **PHI** to 3rd parties with proper Authorization signed by patient.
* Always use the PMC fax cover sheet when sending **PHI** by fax.
* The cover sheet shall include a confidentiality statement instructing anyone who receives the fax in error to destroy the fax and contact the sender: *This message is intended only for the addressee and may contain information that is confidential or privileged. Unauthorized use is strictly prohibited and may be unlawful. If you are not the addressee, you should not read, copy, disclose or otherwise use this message, except for the purpose of delivery to the addressee. If this fax is incomplete or illegible, or has been received in error, please call the PMC Privacy Officer at (\_\_\_) \_\_\_-\_\_\_\_.*
* Do not include any type of **PHI** on the cover sheet.
* If possible, do not fax highly sensitive **PHI**, such as **PHI** about a patient’s drug or alcohol treatment, mental illness, sexually transmitted diseases, or HIV/AIDS status. If it is necessary to fax highly sensitive **PHI**, notify the recipient when sending the fax so that he or she can wait beside the machine to retrieve the fax when it arrives.
* Always double check the fax number prior to sending the fax. Review fax confirmations to validate faxing of the information to the intended recipient.
* Routinely monitor fax machines to ensure any incoming fax containing **PHI** is not left on the machine for an extended period of time.

Text Disclosures:

* The PMC will use a secure and encrypted text messaging service and never transmit **PHI** via text.
* The PMC must obtain the patient's written authorization to receive text messages from the PMC. They should indicate their consent on the space provided on the PMC intake form.
* When texting, do not deliver any identifying information. Do not send any medical information. Simple messages like “please call” or “member2morrow” are preferred. You may even allow the patient to choose her own message for you to send to remind her of her appointment or to call the office.
* Note the patient’s chart that a text was sent and any response received. Print a record of the texts and place in patient’s chart if possible.

**Policy: Breach Assessment and Notification.**

 In the event of a breach in security of Protected Health Information (**PHI)**, the Privacy Officer will conduct a risk assessment and make appropriate notifications if required. A breach is an impermissible acquisition, access, or use or disclosure of **PHI** unless the PMC or its business associate “demonstrates that there is a low probability that the **PHI** has been compromised based on a risk assessment.” Examples of breaches include: unauthorized access to a computers containing **PHI**; theft or loss of a computer, laptop or other portable device containing **PHI**; misplacement of medical records.

**Procedure:**

1. If an impermissible use or disclosure of any **PHI** occurred, the Privacy Officer shall perform a risk assessment and must consider at least:

* The nature and extent of the **PHI** involved (i.e., types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity);
* The type of unauthorized person who used the **PHI** or to whom the data was disclosed;
* Whether the **PHI** was actually acquired or viewed; and
* The extent to which risk to the **PHI** has been mitigated.

2. The Privacy Officer shall determine whether one of the existing exceptions to the definition of the breach applies (i.e., unintentional good faith acquisition, access, or use of **PHI** by a workforce member; inadvertent disclosure between two individuals who are otherwise authorized to access the **PHI**; or disclosure to an unauthorized person who would not reasonably have been able to retain such information).

3. If the Privacy Officer determines after assessment that a breach has occurred, the patient(s) will be notified in writing by first class mail, or notification may be provided orally or by telephone or email, in limited circumstances, where the individual has requested to only receive communication in this manner.  If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside.  If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of writing, telephone, or other means.   These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.  Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

4. Notification to the Media. If the breach affects more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, the Pregnancy Medical Clinic (PMC) is required to provide notice to prominent media outlets serving the State or jurisdiction. The PMC shall issue a press release to appropriate media outlets serving the affected area.  Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

5. Notification to the Secretary of HHS. The PMC must notify the Secretary of all breaches of unsecured **PHI** affecting fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches were discovered. If the breach involves 500 or more individuals, the PMC shall notify the Secretary contemporaneously with its notice to the affected individuals. The PMC will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form

6. Notification by a Business Associate. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the PMC following the discovery of the breach.  A business associate must provide notice to the PMC without unreasonable delay and no later than 60 days from the discovery of the breach.  To the extent possible, the business associate should provide the PMC with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

7. The Privacy Officer must train employees on these breach policies and procedures, and the PMC will apply appropriate sanctions against workforce members who do not comply with all the privacy and security policies and procedures, including termination of employment, if appropriate.

**Policy: HIPAA Training**

All staff/volunteers will receive regular Health Insurance Portability and Accountability Act (**HIPAA)** training, and new staff/volunteers will complete **HIPAA** training prior to commencing any responsibilities that involve Protected Health Information (**PHI**).

**Procedure:**

1. The Privacy Officer shall be responsible for training all staff and volunteers on **HIPAA** and related state guidelines. Training shall occur on a regular basis as needed. The initial training shall review all Policies & Procedures (P&P) related to privacy and security of **PHI**. All new staff/volunteers shall receive this training prior to commencing duties that involve **PHI**.

2. The training shall thoroughly review all the Pregnancy Medical Clinic’s (PMC’s) P&Ps related to **HIPAA**, i.e. confidentiality and privacy, including a general overview of what **HIPAA** is and how it applies to the PMC.

3. The Privacy Officer shall keep a log of trainings and attendees and shall also complete a ***HIPAA*** *Training Verification* form with each staff/volunteer member that will be placed in their personnel file. This form shall include the date of the training.

4. The Privacy Officer may use educational resources to assist in the training, such as those provided by the Office of Civil Rights (**OCR**), which has educational programs for health care providers on compliance with various aspects of the **HIPAA** Privacy and Security Rules. Each of these programs is available with free Continuing Medical Education (**CME**) credits for physicians and Continuing Education (**CE**) credits for health care professionals. They are available at Medscape.org:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html>

There are also Consumer Videos available at <http://www.youtube.com/USGovHHSOCR> that may be of assistance in trainings as well.

**HIPAA TRAINING VERIFICATION FORM**

I have received the Health Insurance Portability and Accountability Act (**HIPAA**) training or information. The training was conducted or the information was give to me on \_\_\_\_\_\_\_\_\_\_\_\_ (date).

I understand that Protected Health Information (**PHI**) is confidential and that authorization from the patient must be obtained to use or disclose **PHI** that is requested for reasons other than treatment, payment or operations, or in order to comply with the law.

I understand that violation of **HIPAA** Privacy Rule may result in disciplinary action up to and including termination of employment.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Privacy Officer Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. HHS Model Form, <http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html> [↑](#footnote-ref-1)