



# New Mexico HIPAA Awareness & Preparedness Program



## Activity Packet

<u>Activity</u>	<u>Page</u>
Creating a Notice of Privacy Practices	2
When is an Authorization Necessary?	7
Who are your Business Associates?	8
Privacy Policies and Procedures Assessment	9
Security Policies and Procedures Assessment	13

# CREATING A NOTICE OF PRIVACY PRACTICES

Patients have the right to adequate notice of the uses and disclosures of PHI that may be made by your organization, and of their rights and your organization's legal duties with respect to PHI. The Notice of Privacy Practices is a public statement that documents a covered entity's policies and procedures relating to the use and disclosure of PHI.

This exercise will help to familiarize you with the requirements for the Notice of Privacy Practices. Following is a sample Notice of Privacy Practices. Read through this sample Notice, and fill in information specific to your organization in the blank spaces provided.

---

**[Organization Name: \_\_\_\_\_]**  
**Notice of Privacy Practices**

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.

If you have any questions about this Notice please contact: **[Name of Privacy Officer: \_\_\_\_\_]**

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" (PHI) is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice, at any time. The new notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with any revised Notice of Privacy Practices by **[accessing our website at: \_\_\_\_\_]**, calling the office and requesting that a revised copy be sent to you in the mail or asking for one at the time of your next appointment.

## **1. Uses and Disclosures of Protected Health Information**

### **Uses and Disclosures of Protected Health Information**

Your PHI may be used and disclosed by your physician, our office staff and others outside of our office that are involved in your care and treatment for the purpose of providing health care services to you. Your PHI may also be used and disclosed to pay your health care bills and to support the operation of the physician's practice.

Following are examples of the types of uses and disclosures of your PHI that we are permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

**Treatment:** We will use and disclose your PHI to provide, coordinate or manage your care and any related services. This includes the coordination or management of your health care with a third party that has already obtained your permission to have access to your PHI protected. For example, we would disclose your PHI, as necessary, to a home health agency that provides care to you. **(Applicable to your organization? \_\_Yes \_\_No)** We will also disclose PHI to other physicians who may be treating you. For example, your PHI may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you. **(Applicable to your organization? \_\_Yes \_\_No)** In addition, we may disclose your PHI from time-to-time to another physician or health care provider (e.g., a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your physician. **(Applicable to your organization? \_\_Yes \_\_No)**

**(Other Examples of uses/disclosures for TREATMENT:**

---

**Payment:** Your PHI will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you such as; making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant PHI be disclosed to the health plan to obtain approval for the hospital admission. **(Applicable to your organization? \_\_Yes \_\_No)**

**(Other Examples of uses/disclosures for PAYMENT:**

---

**Healthcare Operations:** We may use or disclose, as-needed, your PHI in order to support the business activities of your physician's practice. These activities include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, marketing and fundraising activities, and conducting or arranging for other business activities.

For example, we may disclose your PHI to medical school students that see patients at our office. **(Applicable to your organization? \_\_Yes \_\_No)** In addition, we may use a sign-in sheet at the registration desk where you will be asked to sign your name and indicate your physician. **(Applicable to your organization? \_\_Yes \_\_No)** We may also call you by name in the waiting room when your physician is ready to see you. **(Applicable to your organization? \_\_Yes \_\_No)** We may use or disclose your PHI, as necessary, to contact you to remind you of your appointment. **(Applicable to your organization? \_\_Yes \_\_No)**

We will share your PHI with third party business associates that perform various activities (e.g., billing, transcription services) for the practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your PHI, we will have a written contract that contains terms that will protect the privacy of your PHI.

We may use or disclose your demographic information and the dates that you received treatment from your physician, as necessary, in order to contact you for fundraising activities supported by our office. If you do not want to receive these materials, please contact our Privacy Contact and request that these fundraising materials not be sent to you. **(Applicable to your organization? \_\_Yes \_\_No)**

**(Other Examples of uses/disclosures for HEALTH CARE OPERATIONS:**

---

**Uses and Disclosures of Protected Health Information Based upon Your Written Authorization**

Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization, at any time, in writing, except to the extent that your physician or the physician's practice has taken an action in reliance on the use or disclosure indicated in the authorization.

**Other Permitted and Required Uses and Disclosures That May Be Made With Your Authorization or Opportunity to Object**

We may use and disclose your PHI in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree or object to the use or disclosure of the PHI, then your physician may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is relevant to your health care will be disclosed.

**Facility Directories:** Unless you object, we will use and disclose in our facility directory your name, the location at which you are receiving care, your condition (in general terms), and your religious affiliation. All of this

information, except religious affiliation, will be disclosed to people that ask for you by name. Members of the clergy will be told your religious affiliation. **(Applicable to your organization? \_\_Yes \_\_No)**

**Others Involved in Your Healthcare:** Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your PHI that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose PHI to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. Finally, we may use or disclose your PHI to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care. **(Applicable to your organization? \_\_Yes \_\_No)**

**Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Object**

We may use or disclose your PHI in the following situations without your authorization. These situations include:

**Required By Law:** We may use or disclose your PHI to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, as required by law, of any such uses or disclosures.

**Public Health:** We may disclose your PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury or disability. We may also disclose your PHI, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

**Communicable Diseases:** We may disclose your PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

**Health Oversight:** We may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

**Abuse or Neglect:** We may disclose your PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your PHI if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

**Food and Drug Administration:** We may disclose your PHI to a person or company required by the FDA to report adverse events, product defects or problems, biologic product deviations, track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

**Legal Proceedings:** We may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

**Law Enforcement:** We may also disclose PHI, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the practice, and (6) medical emergency (not on the Practice's premises) and it is likely that a crime has occurred.

**Coroners, Funeral Directors, and Organ Donation:** We may disclose PHI to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. PHI may be used and disclosed for cadaveric organ, eye or tissue donation purposes.

**Research:** We may disclose your PHI to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your PHI. . **(Applicable to your organization? \_\_Yes \_\_No)**

**Criminal Activity:** Consistent with applicable federal and state laws, we may disclose your PHI, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose PHI if it is necessary for law enforcement authorities to identify or apprehend an individual.

**Military Activity and National Security:** When the appropriate conditions apply, we may use or disclose PHI of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We may also disclose your PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

**Workers' Compensation:** Your PHI may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally-established programs.

**Inmates:** We may use or disclose your PHI if you are an inmate of a correctional facility and your physician created or received your protected health information in the course of providing care to you. **(Applicable to your organization? \_\_Yes \_\_No)**

**Required Uses and Disclosures:** Under the law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of Section 164.500 et. seq.

## **2. Your Rights**

Following is a statement of your rights with respect to your PHI and a brief description of how you may exercise these rights.

**You have the right to inspect and copy your protected health information.** You may inspect and obtain a copy of PHI about you that is contained in a designated record set for as long as we maintain the PHI. A designated record set contains medical and billing records and any other records that your physician and the practice uses for making decisions about you.

Under federal law, however, you may not inspect or copy the following records; psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding, and PHI that is subject to law that prohibits access to PHI. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact our Privacy Contact if you have questions about access to your medical record.

**You have the right to request a restriction of your protected health information.** This means you may ask us not to use or disclose any part of your PHI for the purposes of treatment, payment or healthcare operations. You may also request that any part of your PHI not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

Your physician is not required to agree to a restriction that you may request. If physician believes it is in your best interest to permit use and disclosure of your PHI, your PHI will not be restricted. If your physician does agree to the requested restriction, we may not use or disclose your PHI in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your physician. You may request a restriction by ***[describe how the patient may obtain a restriction: \_\_\_\_\_]***.

**You have the right to request to receive confidential communications from us by alternative means or at an alternative location.** We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Privacy Contact.

**You have the right to request amendments to your protected health information.** You may request an amendment of PHI about you in a designated record set for as long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Privacy Contact to determine if you have questions about amending your medical record.

**You have the right to receive an accounting of certain disclosures we have made of your protected health information.** This right applies to disclosures for purposes other than treatment, payment or healthcare operations as described in this Notice of Privacy Practices. It excludes disclosures we may have made to you, for a facility directory, to family members or friends involved in your care, or for notification purposes. Disclosures made pursuant to a signed authorization by you are also excluded from the accounting. You have the right to receive specific information regarding these disclosures that occurred after April 14, 2003. You may request a shorter timeframe. The right to receive this information is subject to certain exceptions, restrictions and limitations.

### **3. Complaints**

You may complain to us or to the Secretary of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our privacy contact of your complaint. We will not retaliate against you for filing a complaint.

You may contact our Privacy Contact, **[Name: \_\_\_\_\_]** at **[(505) \_\_\_\_\_]** or **[e-mail address: \_\_\_\_\_]** for further information about the complaint process.

**This notice was published and becomes effective on [date - no later than April 14, 2003].**

## **WHEN IS AN AUTHORIZATION FORM NECESSARY?**

To help you determine which uses and disclosures of patient information require an authorization form and which are covered under a consent form, fill out the following table. List all the instances you can think of in which someone has requested patient information from you or your facility that do **NOT** fall into the categories of treatment, payment or health care operations.

	<i>Who requests information?</i>	<i>Why is the information needed?</i>	<i>Is this information needed for payment, treatment, or internal health care operations?</i>	<i>Is an authorization necessary?</i>
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

## ***WHO ARE YOUR BUSINESS ASSOCIATES?***

In the table below, enter some of the relationships your organization has with outside organizations. Outside entities who have access to your organization's PHI and who provide *non-healthcare treatment related services* on your organization's behalf are classified as Business Associates under HIPAA, and you'll need to implement Business Associate Agreements with them.

In assessing who your Business Associates are, it's useful to determine what information they have access to, and whether that level of access is necessary for the services they provide. If you suspect they have access to more information than they need, you can start thinking about how to convey the minimum necessary information. If they don't need access to PHI at all but are constantly coming in contact with it, that's a sign that your privacy and security measures are weak and need to be improved.

	<b>Business Associate</b>	<b>What PHI they may come in contact with</b>	<b>How PHI is used in provision of service</b>
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

## **PRIVACY POLICIES AND PROCEDURES ASSESSMENT**

Does your organization currently have the following policies, procedures or plans in place?

<b>Requirements</b>	<b>Yes</b>	<b>No</b>
<p>1. <b><i>Minimum Necessary Use</i></b>            Has your organization identified the categories of employees that need access to PHI to carry out their duties?</p> <p>For each category of employee identified, have the associated categories or types of PHI to which access is needed been identified?</p> <p>Are there documented policies and procedures in place that limit the information staff members within the facility may have access to, based upon their job function within your organization?</p>		
<p>2. <b><i>Minimum Necessary Disclosures</i></b>            Are there documented policies and procedures in place which limit the information that may be disclosed to outside entities on a routine or recurring basis?</p> <p>Is there an auditing procedure in place for the above policies?</p> <p>Are there documented policies and procedures in place which include criteria for limitations on <i>non-routine</i> disclosures to outside entities?</p>		
<p>3. <b><i>Minimum Necessary Requests by Other Covered Entities</i></b>            Are there documented policies and procedures in place which state limits on information disclosures to other covered entities?</p> <p>Are there documented policies and procedures in place which state limits on the amount of information <i>your organization</i> requests from <i>other</i> covered entities?</p>		
<p>4. <b><i>De-identification of Health Information</i></b>            Are documented policies and procedures in place which indicate how identifying information must be removed from certain documents? (Only necessary if your organization intends to strip medical records or other health information of <i>all</i> identifiers before disclosing the information to a third party).</p>		
<p>5. <b><i>Patient Privacy Complaints</i></b>            Are documented procedures in place to allow patients to lodge complaints regarding the privacy and confidentiality of their PHI?</p> <p>Is there a documented process for responding to such complaints?</p>		

6.	<p><b>Workforce Training</b></p> <p>Are documented policies in place that detail when and how employees will be trained on your organization’s policies, procedures and practices regarding patient privacy and confidentiality?</p> <p>Do workforce training policies address when workforce “update” training will be required? (i.e. new hire, policy changes, etc.)</p> <p>Are there methods in place to record training attendance and participation?</p>		
7.	<p><b>Workforce Sanctions</b></p> <p>Are documented policies in place which determine the consequences of violations of policies and procedures relating to HIPAA Privacy?</p> <p>Are employees aware of these sanctions?</p>		
8.	<p><b>Marketing and Fundraising</b></p> <p>Are documented policies in place that address how PHI can and cannot be used for marketing and fundraising purposes?</p>		
9.	<p><b>Release of Information</b></p> <p>Are documented policies in place which address how, to whom and in what circumstances patient information may be released?</p>		
10.	<p><b>Patient requests for Amendments to Medical Records</b></p> <p>Does your organization have a documented procedure in place for patients to request corrections, amendments or additions to their health records?</p> <p>Are there policies in place for responding to those requests?</p> <p>If a request for amendment is to be denied, is there a documented policy for recording reasons for denial?</p>		
11.	<p><b>Patient Requests for Access and Copies of Medical Records</b></p> <p>Does a documented policy exist for patients to access their own medical records?</p> <p>Does the policy include fees charged for copying the records?</p> <p>Does the policy state which portions of a patient’s medical records are <i>not</i> accessible to the patient?</p> <p>Does the policy identify the circumstances in which a patient’s request to access or receive a copy of his/her medical record can be denied?</p>		

12.	<p><b>Accounting of Disclosures</b></p> <p>Does your organization have a documented procedure for documenting each disclosure made for purposes other than treatment, payment or health care operations?</p> <p>Does your organization have a documented procedure for responding to patient requests for a list of disclosures of their PHI for purposes other than treatment, payment or health care operations?</p>		
13.	<p><b>Patient Requests for Restrictions on the Use/Disclosure of PHI for T/P/O</b></p> <p>Does your organization have a documented policy in place for patients to request limitations on the uses and disclosures of their personal medical information?</p> <p>Is there a policy in place that documents the process of determining whether to honor patient requests for restrictions?</p>		
14.	<p><b>Notice of Privacy Practices</b></p> <p>Does your organization provide a notice to patients detailing how PHI may and may not be used?</p> <p>Does each patient receive at least one copy of this notice?</p> <p>Do you require each patient to provide written acknowledgement that he/she has received a copy of the Notice?</p> <p>If your organization has a Website, is the notice posted on that site?</p>		
15.	<p><b>Authorization Form</b></p> <p>Does the organization provide a specific document of disclosure for patient signature when disclosing PHI for purposes other than those specifically allowed in the rule (treatment, payment and healthcare operations; public and public policy-related purposes; public health; research; health oversight; law enforcement)?</p> <p>Is there a documented process for a patient to revoke a previous authorization?</p> <p>Does your organization currently have a method for documenting each disclosure and for providing that disclosure history to patients on request?</p>		

16.	<p><b><i>Business Associate Contract Termination</i></b></p> <p>Does your organization have policies in place to respond to activities or practices of business associates that constitute a breach or violation of the business associate’s obligation to protect your organization’s PHI?</p> <p>If the business associate fails to take reasonable steps to cure the breach or end the violation, does your organization have policies in place to terminate the contract, or to report the problem to the Secretary of the Department of Health and Human Services if termination of the contract is not feasible?</p>		
17.	<p><b><i>Privacy Officer</i></b></p> <p>Has your organization designated an individual who will be responsible for monitoring privacy practices, developing and maintain privacy policies and procedures and maintaining a training program?</p> <p>Has a documentation of job description and assignment been made?</p>		

## SECURITY POLICIES AND PROCEDURES CHECKLIST

Does your organization currently have the following policies, procedures or plans in place?

	<i>Requirements</i>	<i>Yes</i>	<i>No</i>
1.	<b><i>Information Access Control</i></b> Are there documented policies and procedures for granting different levels of access to systems that contain PHI?		
2.	<b><i>Personnel Clearances</i></b> Are there documented policies and procedures to ensure that personnel have appropriate clearances?		
3.	<b><i>Security Management Processes</i></b> Are there documented policies and procedures to ensure:  -The prevention of security breaches?  -The detection of security breaches?  -The containment of security breaches?  -The correction of security breaches?		
4.	<b><i>Workforce Sanctions</i></b> Are there documented policies and procedures for disciplinary actions for security breaches caused by:  -Employees?  -Agents of the organization?  -Contractors?		
5.	<b><i>Records Processing</i></b> Are there documented policies and procedures for:  -The receipt of PHI?  -The manipulation of PHI?  -The storage of PHI?  -The dissemination of PHI?  -The transmission of PHI?  -The disposal of PHI?		

6.	<p><b>Media Controls</b></p> <p>Are there documented policies and procedures for your organization’s receipt of electronically stored PHI?</p> <p>Are there documented policies and procedures for your organization’s removal of electronically stored PHI?</p> <p>Do policies and procedures address:</p> <ul style="list-style-type: none"> <li>-Controlled access to media?</li> <li>-Mechanisms for tracking?</li> <li>-Data backup and storage?</li> <li>-Disposal?</li> </ul>		
7.	<p><b>Physical Access Controls</b></p> <p>Are there documented policies and procedures for:</p> <ul style="list-style-type: none"> <li>-Limiting employee access to data?</li> <li>-Disaster and recovery?</li> <li>-Emergency mode operation?</li> <li>-Control of equipment moving in and out of the facility?</li> <li>-A facility security plan?</li> <li>-Verifying access authorizations before anyone can gain physical access?</li> </ul>		
8.	<p><b>Access Levels</b></p> <p>Do current documented policies and procedures address:</p> <ul style="list-style-type: none"> <li>-The level of access granted to employees who work with PHI based on what their job requires?</li> <li>- A procedure for emergency access?</li> </ul>		
9.	<p><b>Workstation Use</b></p> <p>Do current documented policies and procedures address:</p> <ul style="list-style-type: none"> <li>-Appropriate usage of computer workstations?</li> <li>-Appropriate security of computer workstations?</li> <li>-Maintenance of computer workstations?</li> </ul>		

10.	<p><b><i>Employee Termination Procedures</i></b>  Do current documented policies and procedures address formal procedures for termination of employment?</p> <p>Are there documented measures for revoking access, including:</p> <ul style="list-style-type: none"> <li>-Changing combination locks?</li> <li>-Removal from access lists?</li> <li>-Removal of user account(s)?</li> <li>-Turning in access devices (keys, cards, etc.)?</li> <li>-Deleting passwords?</li> </ul>		
11.	<p><b><i>Security Incident Procedures</i></b>  Do current documented procedures exist for the reporting of security breaches?</p> <p>Are policies in place that dictate response to those breaches?</p>		
12.	<p><b><i>Visitor Sign-In</i></b>  Do current documented policies require visitor sign-in?</p> <p>Are escorts required in areas that contain PHI?</p>		