

Explanation of Sample HIPAA Privacy Policy Number 2:  
Notice of Privacy Practices Policy

Under the privacy rule, a physician practice which is a covered entity pursuant to the HIPAA regulations must have a HIPAA Notice of Privacy Practices (“HIPAA Notice”). The HIPAA Notice is a document setting forth how patient information may be used and disclosed by the physician practice as well as setting forth patient rights under HIPAA and the practice’s legal duties under HIPAA.

It is important to note, however, that the HIPAA Notice only describes those uses and disclosures that are permitted by the HIPAA Privacy Rule. The practice cannot add uses and disclosures that would otherwise require patient authorization. In other words, the HIPAA Notice cannot be used to bypass the authorization process.

HIPAA Privacy Policy Number 2 is a sample policy discussing the provision of the HIPAA notice to a practice’s patients.

***Required Statements in a HIPAA Compliant Notice***

There are a number of detailed specific requirements that must be contained in the Notice including the following:

- **Mandatory Header:** The practice’s HIPAA Notice must include this specific language as a header or displayed in some other prominent manner: “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.”
- **Descriptions of Uses and Disclosures:** The practice’s HIPAA Notice must include a description (and at least one example) of the types of uses and disclosures that the practice is allowed to make under HIPAA for treatment of the patient, payment of the claim, and health care operations, taking into account any state law that is more stringent than HIPAA. The HIPAA Notice must also contain a description of all of the other purposes under HIPAA for which the practice can use and disclose patient information without the patient’s written authorization.
- **Description of Certain Uses and Disclosures that Require an Authorization:** The Notice must also specifically state that an authorization will be required for uses and disclosures related to marketing, unless the marketing is face-to-face by the covered entity or involves a promotional gift of nominal value. The Notice must also state that a sale of protected health information would require a signed authorization, as well as any other use or disclosure not described in the Notice.

- **Statement of Authorization Requirement for Psychotherapy Notes (if applicable):**  
If the practice creates or maintains psychotherapy notes (which are defined by HIPAA as notes kept by a mental health professional analyzing the contents of a counseling session and which re kept separate from the rest of the patient’s chart), the Notice must specifically state that authorization is required for disclosures of such psychotherapy notes.
- **Statement regarding Fundraising (if applicable):**  
Although not typically applicable to physician practices, if a covered entity intends to use the patient’s information to contact them for fundraising purposes (for the entity’s own fundraising), this must be stated in the notice of privacy practices as well as a statement that the patient will be given the right to opt-out of such communications.
- **Patient Rights:** The practice must also include in its HIPAA Notice a list of patient rights afforded by HIPAA along with a brief description of how the patient may exercise the following rights:
  - Right to request restrictions on certain uses and disclosures along with a statement that the practice is not required to agree to the restriction (except with regard to a request that information not be provided to a health plan where the services are paid out of pocket);
  - Right to receive confidential communications of patient information;
  - Right to inspect and copy patient records (including a right to receive electronic copies of information maintained in electronic format);
  - Right to request an amendment of patient information;
  - Right to receive an accounting by the practice of certain specific disclosures of patient information by the practice to outside parties; and
  - Right to receive a paper copy of the HIPAA Notice from the practice.
- **Practice’s Duties Under HIPAA:** The practice must also include within its HIPAA Notice statements of its duties, including the practice’s legal requirement to:
  - Provide a HIPAA Notice;
  - Maintain the privacy of patient information;
  - Notify a patient regarding a breach of unsecured protected health information;
  - Follow the terms of its Notice; and
  - Reserve the right to change the Notice by setting forth a statement in the Notice if it intends to do so.
- **Complaint Procedures:** The practice must include in its Notice a statement that patients have the right to complain to the practice and the Department of Health

and Human Services if they believe their privacy rights have been violated; a brief description of how the patient may file a complaint with the practice; and a statement that the patient will not be retaliated against by the practice for filing a complaint.

- **Contact Information:** Within its Notice, the practice must include a name or title and telephone number of a person or office to contact for further information relative to HIPAA (note this can be a title rather than an individual's name).
- **Effective Date:** The Notice must also contain the date on which the practice put the Notice in place, which cannot be earlier than the date on which the Notice is published.

### ***Delivery and Posting of the Notice***

A practice must provide the HIPAA Notice to patients, absent an emergency treatment situation, before or at the time of the patient's first visit with the practice. Once the patient has received a copy of the Notice of Privacy Practices, the patient does not have to receive a copy on subsequent visits (even if the Notice is revised) unless the patient asks for a new copy.

In addition to providing the Notice to the patient as set forth above, a physician office practice must:

- Have the Notice available at the office for patients and others to request to take home with them.
- Post the Notice in a location where patients can clearly see and read the Notice.

Also, if the practice maintains a website that contains information about its services, it must post the Notice on the site and make it available electronically through the site.

### ***Written Acknowledgement of Receipt of Notice***

When the practice provides the HIPAA Notice to a patient, the practice is also required to make a good faith effort to obtain a written acknowledgment from the patient that he/she received the Notice. If the practice is unable to obtain a written acknowledgment, it must document its efforts and the reason why it was unable to obtain the written acknowledgement. (e.g., patient refused to sign the acknowledgement).

The written acknowledgement process can take various forms, such as a signature on the bottom of a carbon copy of the Notice of Privacy Practices, a signature or initial on a form, or an initial on a sign in sheet or logbook.

The acknowledgement can be obtained from the patient's personal representative, where the patient representative has authority to act on behalf of the patient (as discussed in Privacy Policy Number 1).