Notice of Privacy Practices Checklist of Requirements

The HIPAA Privacy regulation creates the right for patients to receive written notice of the uses and disclosures of protected health information (PHI) that may be made by a provider, the individual's rights, and the provider's legal duties with respect to PHI.

Use this checklist for developing your own Notice of Privacy Practices or assessing how well other notices meet the HIPAA requirements.

Note: This checklist addresses only HIPAA requirements. State laws may impose additional or more stringent requirements.

CONTENT: The regulation establishes the following requirements for the content of the Notice of Privacy Practices.

The Notice of Privacy Practices must:

_____ Be in writing.
_____ Be in plain language.

The Notice of Privacy Practices must contain:

_____ The following statement as a header or otherwise prominently display:

"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."

_____ A description, including at least one example, of the types of uses and disclosures that the provider is permitted to make for each of the following purposes: treatment, payment, and healthcare operations. The description must include sufficient detail to place the individual on notice of such uses and disclosures.

_____ A description of each of the other purposes for which the provider is permitted or required to use or disclose PHI without the individual's written authorization. The description must include sufficient detail to place the individual on notice of such uses and disclosures.

Note: If a use or disclosure described above is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.
A statement that other uses and disclosures will be made only with the individual's written Authorization and that the individual may revoke such Authorization in writing unless the provider has taken action in reliance on it.

If the provider intends to do so, separate statements that the provider may contact the individual to:

- Provide appointment reminders;
- Provide information about treatment alternatives or other health-related services that may be of interest to the individual;
- Raise funds for the provider.

A statement of the individual's rights with respect to PHI and a brief description of how the individual may exercise these rights, as follows:

- The right to request restrictions on certain uses and disclosures of PHI, including a statement that the provider is not required to agree to a requested restriction;
- The right to receive confidential communications of PHI;
- The right to inspect and copy PHI;
- The right to receive an accounting of disclosures of PHI;
- The right to obtain a paper copy of the Notice.

A statement of the provider's duties, including the requirements to:

- Maintain the privacy of PHI;
- Provide individuals with notice of the provider's legal duties and privacy practices;
- Abide by the terms of the Notice currently in effect.

A statement that the provider reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all PHI that it maintains.

A description of how the provider will provide individuals with a revised Notice.

A statement that individuals may complain to the provider and to the Secretary of the Department of Health and Human Services if they believe their privacy rights have been violated.

A brief description of how the individual may file a complaint with the provider.

A statement that the individual will not be retaliated against for filing a complaint.

The name, or title, and telephone number of a person or office to contact for further information about the Notice.

The date on which the Notice is first in effect.

Note: This date may not be earlier than the date on which the Notice is printed or otherwise published.
The Notice of Privacy Practices may contain:

_____ If the provider elects to limit the uses and disclosures that it is permitted to make by the Privacy regulation, a description of the more limited uses and disclosures of PHI.

Note: A provider may not include a limitation affecting its right to make a use or disclosure that is required by law or is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

MAINTENANCE AND DISTRIBUTION: The regulation establishes the following requirements for the maintenance and distribution of the Notice of Privacy Practices.

The provider must:

_____ Make a good faith effort to obtain a written acknowledgment from the individual of receipt of the Notice and, if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained.

_____ If the provider has a direct treatment relationship with an individual (as defined in Section 164.501 of the Privacy regulations):

- Provide the Notice no later than the date of the first service delivery, including service delivered electronically;
- In an emergency situation, provide the notice as soon as reasonably practicable after the emergency treatment situation.

_____ If the provider maintains a physical service delivery site:

- Have the Notice available at the service delivery site for individuals to request to take with them;
- Post the Notice in a clear and prominent location;
- Whenever the Notice is revised, make it available upon request on or after the effective date of the revision.

_____ Promptly revise and distribute its Notice whenever there is a material change to:

- The uses and disclosures;
- The individual's rights;
- The provider's legal duties;
- Other privacy practices stated in the Notice.

_____ Make the Notice of Privacy Practices available on request to any person.
Retain copies of Notices issued and any written acknowledgments of receipt of Notices of documentation of good faith efforts to obtain such written acknowledgment for six years from the date they were last in effect.

**ELECTRONIC:** The regulations establish the following specific requirements for electronic Notice of Privacy Practices.

If the provider maintains a Web site that provides information about the provider’s services, it must prominently post the Notice on the Web site and make it available electronically through the Web site.

A provider may provide the Notice by e-mail, if the individual agrees to electronic notice. If the provider knows that the e-mail has failed, a paper copy of the Notice must be provided.

An individual who is a recipient of an electronic Notice retains the right to obtain a paper copy upon request.

If the first service delivery is delivered electronically, the provider must provide electronic Notice automatically and contemporaneously in response to a first request for service.

**Note:** Additional requirements apply to joint Notices of Privacy Practices for providers that participate in organized healthcare arrangements. See section 164.520 (d) of the Privacy regulations for details.