

HIPAA Notice of Privacy Practices

Fast Facts

Purpose

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires health care providers and other covered entities to develop and distribute a notice of privacy practices outlining individuals' rights with respect to their protected health information (PHI) and how it may be used and disclosed by covered entities. Use the HIPAA Notice of Privacy Practices to meet your HIPAA obligations.

Relevant Law

The HIPAA Privacy Rule creates national standards to protect individuals' health information by accomplishing these general goals:

- Gives individuals more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- Holds violators accountable, with civil and criminal penalties that can be imposed if they violate individuals' privacy rights.
- Enables individuals to make informed choices regarding the use and dissemination of personal health information when seeking care and reimbursement for care.
- Enables individuals to find out how their information may be used, and about certain disclosures of their information that have been made.
- Limits release of information to the minimum reasonably needed for the purpose of the disclosure.

- Gives individuals the right to examine and obtain a copy of their own health records and request corrections.

To comply with the HIPAA Privacy Rule, covered entities generally must:

- Notify individuals about their privacy rights and how their information can be used.
- Adopt and implement privacy procedures for their own practice, hospital, or plan.
- Train their employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Secure individual records containing individually identifiable health information so that they are not readily available to those who do not need them.

Fast Facts continued on the back

Penalties

HIPAA imposes civil and criminal penalties for failing to comply with the Privacy Rule. Penalties begin at \$100 per violation, up to a maximum of \$50,000, with a calendar year cap of \$1.5 million. Criminal penalties apply for a deliberate offense, as in intent to sell protected health information, ranging from \$50,000 and one year in prison, up to \$250,000 and ten years. HIPAA also makes employers liable for violations of their business associates if the employer is aware of the wrongdoing.

Fast Facts *(continued)*

Required Content of the Notice of Privacy Practices

Covered entities are required to provide a notice in plain language that includes:

- The following language prominently: “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.”
- How the covered entity may use and disclose protected health information about an individual.
- The individual’s rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.
- The covered entity’s legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.
- Whom individuals can contact for further information about the covered entity’s privacy policies.

The notice must also include an effective date. You are required to promptly revise and distribute your notice whenever you make material changes to any of your privacy practices.

Providing the Notice

- A covered entity must make its notice available to any person who asks for it.
- A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.
- Health plans must also:
 - Provide the notice to new enrollees at the time of enrollment.

- Provide a revised notice to individuals then covered by the plan within 60 days of a material revision.
- Notify individuals of the availability of and how to obtain the notice at least once every three years.
- Health care providers must also:
 - Provide the notice to the individual no later than the first date of service 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 health care provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.
 - When first service to an individual is provided over the Internet, through e-mail, or otherwise electronically, the health care provider must send an electronic notice automatically in response to the individual’s first request for service. The health care provider must make a good-faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.
 - In an emergency treatment situation, provide the notice as soon as it is reasonably practicable to do so after the emergency situation has ended. In these situations, health care providers are not required to make a good-faith effort to obtain a written acknowledgment from individuals.
 - Make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the health care provider’s office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.
 - A covered entity may e-mail the notice to an individual if the individual agrees to receive an electronic notice.

Do’s & Don’ts

DO document compliance with HIPAA notice requirements by keeping copies of the Notice of Privacy Practices you provide to your patients and any written acknowledgments.

Don’t forget to check state laws. Some state laws are more stringent than the HIPAA Privacy Rule with respect to the use and disclosure of PHI.

DO treat all patient information as if you were the patient. Don’t be careless or negligent with PHI in any form, whether spoken, written or electronically stored.

We are the employer’s advocate, dedicated to helping you comply with regulations and protect your business. Our practical solutions make it easy to understand your obligations, delegate administrative tasks and share compliance responsibility with your staff.

Finally, employers have a resource for efficient and affordable solutions that bridge the gap between what the law requires and what makes sense for your business.

COMPLYRIGHT

This product is designed to provide accurate and authoritative information. However, it is not a substitute for legal advice and does not provide legal opinions on any specific facts or services. The information is provided with the understanding that any person or entity involved in creating, producing or distributing this product is not liable for any damages arising out of the use or inability to use this product. You are urged to consult an attorney concerning your particular situation and any specific questions or concerns you may have.

Important note: This is approved for use by the purchaser only. This form may not be shared publicly or with third parties.