

HIPAA PRIVACY CHECKLIST

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets forth standards for the protection of certain health information. The Privacy Rule standards under HIPAA have been established to address the use and disclosure of individual's health information by organizations such as medical practices and also define the patient's privacy rights to understand and control how their information is used.

Each standard is a requirement that the covered entity must comply with respect to an individual's protected health information. Within each standard are implementation specifications that outline details regarding how the standard is to be implemented by the covered entity.

How to Use the HIPAA Privacy Checklist

The checklist provides a detailed review of each of the compliance requirements under the HIPAA Privacy Rule. The check list has been designed to help practices easily understand what is required of them and evaluate if they are compliant. Each section includes:

- Review of required standards
- Implementation specifications under each standard
- Guidance and easy to understand explanations
- Assessment guidelines to ensure appropriate compliance
- Reference for applicable forms. The complete AAPC Physician Service Compliance Toolkit contains over 100 forms that are ready to use or can be customized for your specific medical practice. Forms referenced in the checklist correspond to the applicable forms provided in the Compliance Toolkit.

Legal Notice

The HIPAA Compliance Checklist does not constitute legal advice, and we are not acting as your attorney. The materials being provided are for informational purposes only and should not be used as a substitute for the advice of competent legal counsel.

Use and Disclosure of PHI Requiring Patient Authorization HIPAA Regulation: 164.508	Practices are required to obtain a signed authorization to release protected health information for uses other than treatment, payment, healthcare operations, or as required by law.
---	---

Implementation Specification	Guidance	Assessment	Y / N	Comments
Elements required to be included in an authorization form 164.508 (c) <u>Applicable Forms:</u> PHI Use and Disclosure Authorization Psychotherapy Use and Disclosure Authorization Revocation of Authorization to Use PHI	Authorizations must be documented on a form that includes specific elements required by HIPAA. Elements required to be on an authorization form include: <ul style="list-style-type: none"> • A description of PHI authorized for release • Name of the clinic or individuals authorized to release the PHI • Name of the clinic or individual authorized to receive the PHI • Purpose of releasing the PHI • Indication the patient may revoke the authorization • Indication that treatment is not conditional on signing the authorization (except for research participation or if approval is needed prior to providing insurance coverage) • Patient signature and date • Expiration dates of authorization 	The practice uses an authorization form to obtain approval to use or disclose PHI for all non-TPO related purposes.		
	Providing copies to patients 164.508 (C)(3), (4) Copies of any authorization document are required to be provided to the patient.	Patients are provided copies of their signed authorizations forms.		
	Revoking an authorization 164.508(b)(5) Patients are allowed to revoke their authorization at any time. This must be done in writing.	The practice uses a revocation of authorization form to document any patient requests to revoke authorization to use or disclose PHI.		
	Psychotherapy notes 164.508 (a)(2)	A practice must obtain authorization to use or disclose Psychotherapy Notes unless they are used for treatment by the originator of the notes, for training purposes, or for defense in legal cases. Authorization for psychotherapy notes must be obtained in writing using a separate form from any other authorizations.	Authorizations for psychotherapy notes are obtained in writing using a unique form.	
Marketing 164.508 (a)(3)	Marketing is defined as communication about a product or service that encourages the recipient to buy something. Authorization is required for any use or disclosure of PHI related to market efforts. Some marketing activities do not require authorization. These include: <ul style="list-style-type: none"> • Face-to-face communication with the patient • Reminders of prescription refills • General health promotional things such as (but not limited to) annual mammogram reminders, cholesterol screening etc. 	Appropriate authorization is obtained from the patient in writing prior to using PHI for marketing efforts.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Fundraising activities 164.514 (f)	Practices must obtain authorization before using PHI for any fundraising related activities. An exception to this is granted for practices conducting fundraising activities on their own behalf, as long as the information is limited to demographic information and the practice notifies the patient that they may opt out of any such solicitations.	Appropriate authorization is obtained from the patient in writing prior to using PHI for any fundraising efforts.		

Use and Disclosure of PHI Requiring an Opportunity to Agree or Object HIPAA Regulation: 164.510	HIPAA Privacy Rules allows a medical practice to make certain uses or disclosures of PHI without obtaining a written authorization, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or object to the use. Agreement can be communicated verbally.
---	--

Implementation Specification	Guidance	Assessment	Y / N	Comments
Facility directories 164.510 (a)	A practice may use patient information to maintain an inpatient directory. The only information that is allowed to be disclosed in the facility's directory is the patient name, general condition, religious affiliation and physical location. <i>This standard typically applies to inpatient settings</i>	The patient directory (if applicable) only lists appropriate information allowed under HIPAA Privacy.		
Disclosing PHI to family members and friends 164.510 (b)	A practice is allowed to share PHI with family members, relatives, close friends or any other person identified by the patient to the extent the information is necessary for the patients care or payment related to services. Providers and clinical staff should not assume that PHI can be disclosed because the person(s) came with the patient for appointment. It's best practice to ask the patient's permission prior to exam. Patient PHI may also be used in order to help identify, locate or notify family members or their care taker to inform them of the patient's location, general condition or death.	Providers only share patient PHI with family members, relatives or close friends after receiving appropriate consent from the patient.		
Disaster relief efforts 164.510 (b)(4)	PHI may also be disclosed to public or private organizations which are authorized to assist in disaster relief efforts. Information is only to be used for the purposes of locating family members or person's responsible for care of the individual. The only information that is allowed to be disclosed is the patient name, general condition, religious affiliation and physical location.	Patient PHI disclosed for purposes of disaster relief efforts is limited to only what is allowed under HIPAA Privacy.		
Limitations on information that can be shared when the patient is not present. 164.510(b)(3)	In situations where a patient is not able to agree or object (e.g. the patient is not present, incapacitated or in an emergency) the provider is allowed to disclose PHI, but it must be based on their professional judgment to determine if disclosing PHI is appropriate and in the best interest of the patient.	Information shared under circumstance where the patient is not present is based on the physician's judgment and strictly limited to information relevant to the other person's involvement with the patient.		

Practice Safeguards	The HIPAA Privacy Rule requires practices to ensure the safeguard of Protected Health Information (PHI). Practices are expected to make "good faith, reasonable and appropriate" effort to establish the necessary safeguards to comply with the Privacy Rule requirements. The following section outlines safeguards that a practice should have in place to help maintain compliance and ensure protection of patient information.
----------------------------	--

Implementation Specification	Guidance	Assessment	Y / N	Comments
Patient Sign In Sheets	Sign in sheets are permitted under HIPAA as long as they have limited information about the patient and do not have any identifying information, other than the patient name.	Patient Sign-in sheets are limited to patient name, appointment time, and time of arrival.		
Verifying Patient Identities 164.514 (h)	<p>The practice is required to verify the identity of any patient requesting his/her own protected health information. Examples of information that can be used to identify a patient includes, but is not limited to:</p> <ul style="list-style-type: none"> • Date of birth • Zip code • Address • Mother's maiden name • Last 4 digits of social security number • Driver license 	Patients who call over the phone are required to provide 2 identifying pieces of information.		
Phone Message and Appointment Reminders	Appointment reminders can still be mailed to patients, but any information should be limited to the patient's name and date / time of the appointment. No other information should be used.	Appointment reminder cards contain only the patient name and date and time of an appointment.		
	The practice may leave phone messages with patients regarding test results, appointment reminders or to schedule an appointment. Information left on a phone message should be limited to the patient's name, their doctor's name and phone number and date / time of the appointment.	Phone messages left by the clinic are limited to the patient's name, physician contact information and date/time for an appointment.		
Patient Privacy	A practice should make reasonable precautions to prevent inadvertent disclosure of PHI. These safeguards are not specifically mandatory, but should be considered when evaluating if they are reasonable to implement.	Exam rooms or clinic doors are closed before engaging in any discussion of PHI.		
		Fax and telephone answering machines are place in a secure area where patients can not readily access them.		
		If possible, use cubicles or dividers to help promote confidentiality when registering or checking out patients.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
		When sending EOBs (explanation of benefits) to secondary carriers, any PHI that is not applicable to the claim is blacked out.		
Photographs	<p>The use of photographs of patients is permitted by HIPAA as long as these are kept away from public view or appropriate patient authorization has been obtained.</p> <p>OB providers may hang new baby photos in a specific area, but must have written consent by their parents. Baby names should be removed from all pictures prior to displaying for public view.</p>	The practice maintains any pictures of patients in a secure file, not accessible to the public.		
Faxes <u>Applicable Forms:</u> Fax and Email Disclaimer Statement Fax Transmission Log	<p>Faxes and emails are allowed to contain PHI for treatment, payment and healthcare operation (TPO) purposes. Practices are required to be able to account for where PHI has been faxed. In addition, fax cover sheets are required to have a privacy disclaimer on them.</p> <p><i>Tip: Best practice is to use a fax confirmation sheet that is maintained in the patient record that shows the front page with the faxed to information.</i></p>	<p>All faxes containing PHI have a privacy disclaimer on the cover sheet.</p> <p>The practice maintains a fax log which is used to track / document faxes containing PHI.</p>		
Emails <u>Applicable Forms:</u> Fax and Email Disclaimer Statement		A confidentiality disclaimer is included at the bottom of all emails sent by the practice.		