



Piedmont Behavioral Healthcare

HIPAA PRIVACY PRIORITY CHECKLIST

This checklist was developed to guide providers in prioritizing business practices to implement HIPAA's Privacy standards. Given that resources (i.e., time, money, personnel) may be limited, providers may find it beneficial to review the classifications and apply the checklist items to their own practices. Place a check next to the business practice specified once it is completely implemented. Business practices are classified as either:

CRITICAL - These business practices are critical for compliance with HIPAA's Privacy standards.

IMPORTANT - These business practices are important for compliance with HIPAA's Privacy standards.

FUNDAMENTAL – These business practices are fundamental for compliance with HIPAA's Privacy standards.

PHI = Protected Health Information

CRITICAL

Policies and Procedures:

Are your privacy policy and procedures (including processing complaints and employee training) in accordance with HIPAA's Privacy standards?

Designated Privacy Person:

Do you have a designated person (or system) responsible for:

- Privacy policy and procedure development and implementation?
- Processing privacy complaints and questions?
- Accounting and tracking PHI disclosures?
- Processing requests related to individual rights?

Employee Training:

Do you:

- Provide privacy training to each new employee?
- Have a policy for procedures to undertake when employees leave or are terminated?

Notices:

- Do you have a *Notice of Privacy Practices* prepared and displayed in accordance with HIPAA's Privacy standards?
- Have you distributed the *Notice* to patients?

Do you have a policy with procedures for:

- Distributing the *Notice* no later than the patient's first appointment?
- Maintaining the patient's acknowledgement of receipt of the *Notice*?

IMPORTANT

Policies and Procedures:

Do your privacy policies and procedures allow for:

- Permissive uses and disclosures of PHI for the following categories:
 - To the individual or the individual's personal representative
 - For treatment, payment, or health care operations
 - Situations in which the individual is given an opportunity to agree or object (e.g., facility directories)
 - For public priorities (e.g., public health, health oversight, required by law)
 - As authorized by the individual
- Assessing the authorization process to identify transition issues, which may result from the continued use or disclosure of PHI pursuant to a legal permission obtained prior to the regulations' effective date?
- Providing a copy of an individual's written request for disclosure of the individual or as required by law, public health, etc, in lieu of the accounting?
- Working with business associates to ensure individual rights are maintained?

Documentation requirements of:

- An individual's agreement or objection to the release of PHI?
- PHI requests, complaints, consents, authorizations, etc.?

Obtaining authorization prior to the use or disclosure of:

- Psychotherapy notes?
- PHI for purposes other than treatment, payment, or health care operations (e.g., marketing)?

Review and revision of the authorization form for:

- Compliance with privacy standards?
- Compliance with privacy standards if the form is combined with other documents to create a compound authorization (other than for research or psychotherapy notes)?

An individual to:

- Request restrictions to the uses and disclosures of their PHI and to address how to terminate an agreed upon restriction?
- Request to receive confidential communications by alternative means or at an alternative address?
- Revoke an authorization (and actions to take in the event the individual revokes the authorization)?
- Access, inspect and/or obtain a copy these records been reviewed and/or revised to comply with HIPAA requirements?
- Amend PHI in the designated record sets?
- Request an accounting of disclosures?

Safeguards:

Have you:

- Inventoried the types of individually identifiable information (e.g., medical records, client or case files, prior authorization requests, consents, preventive health assessments, health status questionnaires, encounter information, claims or claim records, enrollment, or other) handled, processed, accessed, or stored within your office/facility?

- Assessed access to PHI by your employees' job responsibilities (and under what conditions, and the nature of the business)?
- Identified all external disclosures of PHI?
- Reviewed all of your employees' communication methods (e.g., face-to-face, telephone, fax, email, EDI) for exchange (send or received) of PHI?
- Implemented administrative, technical, and physical safeguards to protect PHI from intentional, unintentional or incidental use or disclosure?

Business Associates:

- Have you identified all business associates (with their contract renewal dates) that perform services on your behalf?

Other:

- If you act as a health plan and disclose PHI to a plan sponsor, does your plan Documents contain appropriate PHI restrictions?

FUNDAMENTAL

Policies and Procedures:

- Do your policies and procedures receive periodic management review?

Do you have policies that prohibit:

- Requiring an individual to waive their right to privacy in order to be provided treatment?
- Retaliating, intimidating, or threatening employees filing complaints, opposing acts believed to be unlawful under the privacy law, or participating in investigations?

Do you have procedures for:

- De-identification and re-identification by the organization, if applicable.
- Mitigating any known harmful effect following a use or disclosure of PHI in violation of the privacy standards?
- Employees to make complaints about PHI policies or procedures?

___ Requiring employees to agree to confidentiality requirements? Is the agreement in writing?

___ Sanctioning business associates or limiting data set recipients for known violations?

___ Identifying when a limited data set agreement is necessary?

Do your policies and procedures allow for:

___ Use and disclosure of data stored in limited data sets?

___ Auditing employees' compliance with privacy practices?

___ Sanctioning employees for violations of privacy policies and procedures?

___ Reviewing records retention compliance with privacy standards?

___ Governing privacy practices with respect to business associates and mitigation for known privacy violations?

Employee Training:

___ Are your employees re-trained when material changes affect their functions?

Business Associates:

___ Have your contracts or written agreements with entities that perform services on your behalf (e.g., billing agents) been updated to include all Business Associate provisions as mandated by the Privacy rule?

Have you:

___ Developed a Limited Data Set Agreement with all required provisions, if applicable?

___ Reviewed all releases of data to determine if a Limited Data Set agreement is required?