

HIPAA Privacy Rule Compliance Checklist for Health Plans

Penny Wofford of the [Edwards Ballard Law Firm](#) in Spartanburg prepared this checklist. Questions may be directed to Penny at (864) 542-8612.

Implementing administrative requirements:

1. Designate a privacy officer.
2. Develop privacy policies and procedures.
3. Provide training to all employees with access to protected health information.
4. Develop and distribute a privacy notice.
5. Post privacy notice on website *(if health plan maintains a website)*.
6. Prepare or amend Business Associate contracts.
7. Create authorization form.
8. Amend health plan documents.

Drafting policies and procedures:

A covered entity's policies and procedures should be specific to the operations of the covered entity and appropriate to the size and scope of the covered entity's activities. In general, a covered entity's policies and procedures should include:

- A. Rules for uses and disclosures of Protected Health Information (PHI) including minimum necessity requirements, including:
 - The identity of the classes of employees who need access to PHI to perform job duties;
 - The categories and types of PHI needed; and
 - The conditions upon which such access is allowed.
- B. Rules for safeguarding protected health information
- C. Procedures for verifying the identity of persons seeking disclosure of protected health information
- D. Rules for disclosing PHI to family and friends of patients
- E. A detailed complaint procedure

- F. Rules regarding the appropriate application of sanctions for workforce violations
- G. Procedures regarding the training requirements
- H. Procedures and time requirements for implementing individual rights and responding to requests for information, including:
 - Right to copies
 - Right to amend records
 - Right to an accounting
 - Right to request restrictions
 - Right to file a complaint
- I. Procedures for obtaining authorizations
- J. Procedures for distribution of the privacy notice
- K. Rules for implementing business associate agreements and responding to business associate violations
- L. Procedures for retention of records and documentation requirements