
# HIPAA Tool Kit

**2017**

# Contents

# P-1200 Staff Training

This section establishes the responsibility for development and updating of staff training programs and materials on privacy policies and procedures. It also establishes the responsibility of all staff members to complete privacy training.

## P-1210 Content of Privacy Training Program for Staff

The **[title of privacy official]** or a staff member designated by the **[title of privacy official]** will develop a privacy policy orientation and training program.

The purpose of this program is to make sure that all staff members are familiar with the privacy policies and procedures adopted by **[name of organization]**.

The training and orientation program will cover:

- The definition and identification of protected health information
- Providing the "Notice of Privacy Practices" to all patients and obtaining a written acknowledgment of receipt
- Using and disclosing protected health information for treatment, payment, and health care operations
- Obtaining authorization, when required, for use and disclosure of protected information
- Procedures for handling suspected violations of privacy policies and procedures
- Penalties for violations of privacy policies and procedures
- Documentation required by the policies and procedures manual

Staff members will:

- Receive a summary of the medical practice's privacy policies and procedures
- Have an opportunity to review the policies and procedures manual
- Have an opportunity to ask questions about the privacy policies and procedures of **[name of organization]**

### Regulation

**45 CFR 164.530(b)(1)**
Requires training of all staff members on privacy policies and procedures.

## P-1220 Initial Privacy Orientation and Training

All staff members must complete the privacy policy orientation and training program during their probationary period.

1. Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by the **[title of privacy official]** or the staff member who conducts the training.
2. Until staff members complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
3. Prior to the end of a staff member's probationary period, his or her supervisor should confirm that he or she has completed privacy training.

4. The probationary period of any new employee who has not completed the privacy policy orientation and training program will be extended, and the employee will be ineligible for benefits that would have become available upon completion of the probationary period. In some cases, an employee who does not complete the privacy orientation and training program prior to the end of his or her probationary period will be required to complete the program before resuming normal job duties.

### Regulation

**45 CFR 164.530(b)**
Establishes HIPAA requirements for staff training.

## P-1230 Revised Policies and Procedures Training

The **[title of privacy official]** or a staff member designated by the **[title of privacy official]** will develop training materials on new or revised privacy policies and procedures.

### Procedures

1. Staff whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within one month of their effective date.
2. Completion of training on revised policies and procedures will be documented in the employee's personnel file.

### Regulation

**45 CFR 164.530(b)(2)(ii)**
Requires documentation of training.

**IMPORTANT**

Note: The medical practice's legal counsel should review and approve any penalty that is proposed to be assessed for non-compliance with privacy policies and procedures.

# P-2300 Use and Disclosure of Information for Health Care Operations

This section addresses the uses and disclosures of information in the course of day-to-day operations that do not require specific authorization (see policy P-3300).

## Regulation

**45 CFR 164.506**
Establishes requirements for the use and disclosure of protected health information for the purposes of treatment, payment, and health care operations.

## P-2310 Definition of Health Care Operations

Use and disclosure of protected health information is permitted under this policy to conduct the following activities:

- Quality assessment and improvement
- Professional credentialing
- Medical and utilization review
- Legal services
- Auditing
- Business planning and market research
- Grievance procedures
- Due diligence analysis related to sales and acquisitions
- Creation of de-identified information and limited data sets
- Customer service
- Patient directories
- Compliance monitoring

**IMPORTANT**
Review by legal counsel is advised.

Before using or disclosing protected health information for any of the functions included in health care operations, a good-faith effort must be made to obtain the patient's written acknowledgment of having received the "Notice of Privacy Practices." Obtaining the written acknowledgment is the responsibility of the **[title of receptionist]**. If the patient's acknowledgment cannot be obtained, the reason the attempt to obtain an acknowledgment was unsuccessful must be documented in writing.

Procedures for obtaining an acknowledgment are established by policy P-3190.

# Conducting Internal HIPAA Audits

## Making the Case for HIPAA Auditing

The foundation of all good compliance programs—whether they address compliance with the government's rules on coding and billing or health information privacy and security—is auditing and monitoring. Any good audit program helps an entity maintain compliance with whatever area the auditor is examining.

Although there are no set guidelines for auditing an existing Health Insurance Portability and Accountability Act program, two standards within the security rule require some form of auditing. If an organization has a HIPAA program in place, these areas should already be an active part of their HIPAA processes.

- Section 164.308(a)(1)(ii)(d), *Information system activity review (Required): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
- Section 164.312(1)(b), *Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

Beginning in 2011 the Office for Civil Rights (OCR) established a pilot audit program to determine if covered entities (CE) and business associates (BA) had implemented HIPAA privacy, security, and breach notification programs as required by HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act and to assess if the guidelines and processes that were established by the CE comply with the rules. If the Department of Health and Human Services (HHS) and the OCR feel it is necessary to audit these programs, then so should covered entities.

Proof of the need for ongoing auditing and monitoring is evident in OCR's finding from the initial pilot audits conducted in 2012. At the joint OCR and National Institute of Standards in Technology (NIST) conference, "Safeguarding Health Information: Building Assurance Through HIPAA Security," held in September 2014, the OCR reported that "58 out of the 59 health care providers audited had at least one negative finding regarding security rule compliance, 56 percent became aware of additional HIPAA regulations that apply to their organizations, and two-thirds of all entities had no complete or accurate risk assessment program." Based on the less-than-flattering findings from these phase one audits, the OCR is likely to step up HIPAA enforcement.

According to the numbers posted on the HHS website, the number of complaints received in 2012 was 10,454, rising to 12,915 in 2013. Independent research conducted by the Ponemon Institute on the cost of a data breach over several industry sectors, including health care, "found the average cost of a data breach to be $5.5 million with average cost per compromised record around $200" after a loss or theft of protected personal information.

**IMPORTANT**

An entity relying on its own complaint/grievance process to catch instances of noncompliance could be missing processes that violate HIPAA rules.

**IMPORTANT**

Two-thirds of CEs audited did not perform a complete or accurate risk assessment. Remember, some standards are required and some are addressable. "Required" means the policies and/or procedures must be implemented. "Addressable" means the CE must assess if the standard is "reasonable and appropriate" for the environment. A risk assessment is a required element of the security rule and includes a risk analysis [*164.308(a)(1)(ii)(A)*] and risk management [*64.308(a)(1)(ii)(B)*].