

HIPAA COMPLIANCE MANUAL OUTLINE

The HIPAA regulations require all covered entities to maintain records of policies, procedures, actions, activities and designations required by the HIPAA Administrative Simplification provisions. To facilitate this requirement covered entities should maintain a printed HIPAA compliance manual. This manual should contain all documentation developed or utilized during the HIPAA compliance project. This outline will assist a covered entity in the development of a HIPAA compliance manual.

HIPAA POLICY HANDBOOK

The HIPAA standards for privacy and security require the development and adoption of policies and procedures to facilitate compliance with the HIPAA requirements. The sample policy handbook that is included with HIPAA Rx Forms Creator software contains model policies and procedures that address the HIPAA privacy and security requirements for covered entities. The HIPAA Rx Forms Creator includes a 96-page policy and procedure handbook.

HIPAA PROJECT PLAN TEMPLATE

The HIPAA Project Plan template should list each individual task associated with HIPAA compliance. The HIPAA Project Plan template already includes a model for a HIPAA project. The template will allow you to track the amount of time to complete each compliance step and assign tasks to other members of the project team (if applicable).

BUSINESS ASSOCIATE CONTRACT

As defined in the HIPAA regulations, a business associate is any entity that creates, receives, maintains or transmits health information on behalf of a covered entity. The HIPAA privacy and security standards require covered entities to have business contracts in place with these entities. It also requires business associates to provide written assurances, in the form of business associate contracts, that they will appropriately safeguard protected health information. The objective of this contract is to require the business associate to comply with the organization's privacy practices and to implement safeguards for any protected health information that it receives from the organization.

NOTICE OF PRIVACY PRACTICES

Covered entities must make available to each individual a "Notice of Privacy Practices." The Notice of Privacy Practices must inform the individual of the uses and disclosures of protected health information that may be made by the organization, and of the individual's rights and the practice's legal duties with respect to protected health information.

MODEL CONTINGENCY PLAN

Each covered entity must have a written contingency plan that includes provisions for data backup, disaster recovery and emergency mode operations. HIPAA requires such a plan to ensure that the organization has a formally developed plan in the event of an emergency or other occurrence. This outline will assist covered entities in creating their contingency plan.

WORKFORCE CONFIDENTIALITY AGREEMENT

Members of the workforce, which may include employees, contractors, students, and volunteers, must understand the importance of confidentiality within the covered entity, and

agree to uphold the standards established by the privacy and security officials. This agreement lists the workforce member's responsibilities as it relates to maintaining the confidentiality of information within the organization. This should be used in tandem with a workforce member's signed acceptance of the organizations HIPAA policies for privacy and security.

MODEL JOB DESCRIPTION FOR PRIVACY OFFICER

The HIPAA privacy standards require that covered entity identify an individual responsible for the development and implementation of the policies and procedures of the organization. In addition, the privacy standards require that the organization designate an individual who is responsible for receiving complaints. To understand the job requirements of this individual, the sample job description should be reviewed, customized and then maintained along with the covered entities documentation.

MODEL JOB DESCRIPTION FOR SECURITY OFFICER

The HIPAA security standards require that the covered entity identify individuals responsible for the development and implementation of the policies and procedures of the covered entity. To understand the job requirements of this individual, the sample job description should be reviewed, customized and then maintained along with the covered entities documentation.

PROJECT TEAM WORKSHEET

The HIPAA Project Team Worksheet is used to designate individuals that will be working on the HIPAA project. These individuals will become intimately familiar with HIPAA's requirements and will assist the Privacy and Security Officers with the assessment, documentation development and implementation.

REGISTRATION FORM FOR NEW PATIENTS

To reduce the amount of paperwork, new patients should complete a registration form that collects all relevant information regarding the individual and allows the individual to provide written acknowledgement that he/she has received the Notice of Privacy Practices.

INFORMATIONAL HIPAA BROCHURE FOR PATIENTS

HIPAA's Health Insurance Reform provisions greatly affect the portability and continuity of patients' health insurance, while its privacy standards affect access to their health information. The Patient Brochures provide an excellent introduction to HIPAA and its effects on a covered entity's patients.

HIPAA COMPLIANT SIGN-IN SHEET

The covered entity must ensure that its existing process for patient sign-in does not disclose any information that is individually identifiable to a patient. Sign-in sheet information should be limited to name, date and time. The included sign-in sheet meets these requirements.

AUTHORIZATION FORM FOR USING AND DISCLOSING PHI

Covered entities must obtain a signed "authorization" to use or disclose information for purposes other than treatment, payment and health care operations (except as required by law). The authorization form must contain the following core elements: description of

information to be used or disclosed, name of the person(s) authorized to use or disclose the information, name of the person(s) requesting the information, expiration date or event that relates to the information use or disclosure, statement of the individual's right to revoke the authorization and the exceptions to this right, statement that the authorized information may be subject to re-disclosure by the recipient, and signature of the individual.

REQUEST FORM FOR HEALTH RECORD AMENDMENT

The HIPAA privacy standards provide individuals with the right to request an amendment to their health information if they believe it to be inaccurate. Individuals should utilize this form when they are requesting an amendment to their health information. Utilize the Policy for Health Record Amendment (located in the HIPAA policy manual) as a guideline for establishing internal process for reviewing amendment requests.

REQUEST FORM FOR ACCOUNTING OF DISCLOSURES

Covered entities must maintain a detailed accounting of all disclosures of protected health information. Patients are entitled to one (1) free accounting per every twelve month period. This form will provide a mechanism for documenting requests from patients. The covered entity must act on the individual's request for an accounting no later than 60 days after receipt of such a request.

REQUEST FORM FOR INSPECTING PHI

An individual has the right to inspect and obtain a copy of protected health information about the individual in a designated record set. The healthcare organization must have a mechanism for documenting patients' requests to inspect their health information. The organization must act on a request for access no later than 30 days after receipt of the request.

REQUEST FORM FOR RESTRICTING USES OF PHI

Covered entities must permit an individual to request that the organization restrict uses or disclosures of protected health information. The organization, however, is not required to agree with the restrictions if it interferes with treatment, payment or operations.

PATIENT FORM FOR FILING COMPLAINTS

If a patient believes that the covered entity has violated his/her rights under HIPAA, or if they disagree with a decision made by the covered entity, the patient has the right to complain. If the patient still does not believe the incident has been rectified, they may submit a complaint to the U.S. Department of Health and Human Services.

FORM FOR ACCOUNTING OF PHI DISCLOSURES

The covered entity must maintain a detailed accounting of all disclosures of protected health information. This form will provide a mechanism for the organization to record and document disclosures. The form should be included in the individual's record.

FORM FOR DOCUMENTING SYSTEM INVENTORY

The covered entity should complete a full documentation of all hardware and software used for operations. This is used for disaster recovery purposes and to identify security vulnerabilities. This template will assist in recording the organization's assets.

MODEL FAX COVER SHEET

All faxes submitted by the covered entity should include a cover sheet with a detailed privacy disclosure. All fax recipients should be contacted by telephone to ensure they received the transmitted information. This template includes a disclosure regarding the confidentiality of health information.

NEW EMPLOYEE CHECKLIST

New employees should go through a standard training and orientation process for privacy and security. Use this template as a guideline for developing internal practice for orienting new employees.

EMPLOYEE TERMINATION CHECKLIST

Appropriate measure must be taken to ensure that keys, computer access codes and office property are returned to the organization upon termination. This customizable checklist provides guidelines for employee termination.

HIPAA PROJECT PROPOSAL

The purpose of the project proposal is to outline for management, and/or the principals of the organization, the compliance steps, timeline for implementation, and cost of the HIPAA project.

NETWORK DOCUMENTATION CHECKLIST

The purpose of this template is to provide you with a list of documentation that should be maintained for the covered entity's information systems network. By having a well-documented information systems network the covered entity is able to maintain the integrity of their data and identify security vulnerabilities.