

# HIPAA COMPLIANCE SYSTEM

Eagle Associates, Inc (800) 777-2337



2009 - 2010

## Quick Links

[Table of Contents](#)

[User's Introduction Section](#)

[Privacy Rule Policies](#)

[Security Standard Policies](#)

[HIPAA Forms](#)



# HIPAA Compliance Manual

for the healthcare practice setting

The information, guidelines and policies set forth within this manual were developed in accordance with regulations and guidelines established by the Department of Health and Human Services (DHHS) in the Standards and Rules for the Health Insurance Portability and Accountability Act (HIPAA). Because of the dynamic changing nature of federal, state and local regulations, it is impossible to guarantee absolute accuracy of the material contained in this manual. Compliance with HIPAA's Standards and Rules is dependent upon the practice's implementation and regular evaluation of the effectiveness of its policies and enforcement of its established policies and procedures. Eagle Associates, their employees, consultants and representatives cannot assume any responsibility for omissions, errors, misprinting or ambiguity contained within the manual and shall not be held liable in any degree for any loss, illness or injury caused by such omissions, errors, misprinting or ambiguity presented therein.

## **HIPAA Compliance Statement**

This Compliance Manual contains the guidelines and information necessary to provide for compliance with HIPAA Standards and Rules in the healthcare practice setting. Eagle Associates, Inc. provides this manual and a system of ongoing technical support (such as updates, toll-free technical support, training and educational materials) to assist the healthcare facility in maintaining an effective system of compliance with HIPAA Standards and Rules. It is ultimately a cooperative effort between the practice, its staff, and Eagle Associates that will determine the achieved level of regulatory compliance.

Compliance with HIPAA Standards and Rules is an ongoing process, requiring the attention of management and staff on a regular basis. The program requires training for all employees, effective communication, documentation and recordkeeping, maintenance of regulatory updates (provided by Eagle Associates), and the implementation of a complete assessment and evaluation program to verify compliance on an annual basis. The manual is designed to be a living document within the practice.

## 2009 HIPAA COMPLIANCE MANUAL

### Table of Contents

Section	Title
<b><u>1.00</u></b>	<b><u>GENERAL ADMINISTRATIVE POLICIES</u></b>
1.01	Organizational Structure
1.01a	Compliance Manager
1.01b	Privacy Manager
1.01c	Compliance Committee
1.01d	HIPAA Compliance Assignments
1.02	HIPAA Compliance Review Policy
1.03	Employee Training Policy
1.04	Compliance Meetings
1.04a	Compliance Committee Meetings
1.05	Notices and Forms
1.05a	Notice of Privacy Practices-Posting Requirement
1.05b	Forms
1.05c	Patient Complaints - Posting Requirement
1.05d	Supplementary Staff Training - Posting Requirement
1.06	Recordkeeping
1.07	Patient Complaint System
1.07a	Patient Privacy Complaint Form
1.08	Health Plan Sponsor
1.08a	Privacy Officer
1.09	Definitions
1.10	Use and Disclosure of Employee PHI
1.10a	Access to Employee PHI
1.10b	Non-Compliance Resolution
1.10c	Certification
1.11	Employee Rights
1.11a	Right to Inspect and Copy Employee PHI
1.11b	Right to Authorization
1.11c	Right to Request Amendments
1.11d	Accounting of Uses and Disclosures
1.12	Administrative Policies
1.12a	Documentation and Recordkeeping
1.12b	Business Associate Agreements
1.12c	Staff Training
1.13	Employee Notice of Privacy Practices
1.14	HIPAA Sanctions
1.14a	HIPAA Sanction Examples
<b><u>2.00</u></b>	<b><u>TRANSACTION POLICIES</u></b>
2.01	Transaction Extension/Model Compliance Plan (Discontinued)
2.02	Vendor Relationships
2.02a	Software Vendors
2.02b	Healthcare Clearing Houses
2.03	Staff Training
2.04	Healthcare Provider Taxonomy Codes
2.05	Situational Use

2.06	Taxonomy Code Maintenance
2.07	Obtaining Taxonomy Codes
2.08	Use of Taxonomy Codes
2.09	Transactions/Code Sets Complaint

### **3.00** PRIVACY POLICIES

3.01	Definitions
3.02	Privacy Manager
3.03	Staff Responsibility
3.03a	Staff Access to Protected Health Information
3.04	Use and Disclosure of Protected Health Information
3.05	Minimum Necessary Information
3.05a	Reasonable Safeguards
3.06	Routine Disclosures
3.07	Non-Routine Disclosures
3.08	Provider Responsibilities
3.08a	Direct Provider Relationships
3.08b	Indirect Provider Relationships
3.09	Individual (Patient) Rights
3.09a	Exceptions to Individual (Patient) Rights
3.09b	Personal Representatives
3.09c	Minor Children
3.09d	Family Members
3.10	Disclosure Accountability
3.10a	Fees for Disclosure Accountability
3.11	Notice of Privacy Practices
3.11a	Availability of the Notice of Privacy Practices
3.11b	Revisions to Notice of Privacy Practices
3.11c	Acknowledgment of Receipt
3.11d	Sample of Notice of Privacy Practices
3.11e	Documentation of Notices
3.12	Authorizations
3.12a	Authorization Process
3.12b	Documentation of Authorizations
3.12c	Samples of Authorizations
3.13	Restrictions to Protected Health Information
3.13a	Denial of Requested Restriction to Protected Health Information
3.13b	Termination of a Restriction
3.13c	Disagreement to Termination of a Restriction
3.13d	Documentation of Restrictions, Terminations and Disagreements
3.13e	Sample of Request for Restriction of Protected Health Information
3.14	Requested Amendments to Protected Health Information
3.14a	Amendment Process
3.14b	Acceptance of a Requested Amendment to PHI
3.14c	Amending Protected Health Information Received from Another Entity
3.14d	Denying a Request for Amendment
3.14e	Documentation of Requested Amendment, Denial
3.14f	Sample of Request for Amendment and Denial/Acceptance
3.15	Access to Protected Health Information
3.15a	Access Process
3.15b	Denial of Access Without Review
3.15c	Denial of Access with Review
3.15d	Copies of Protected Health Information

- 3.15e Documentation of Access
- 3.15f Sample Copies of Forms for Access
- 3.16 Privacy Security
  - 3.16a Operational Hours
  - 3.16b Non-Operational Hours
  - 3.16c Off-Site Transportation
- 3.17 Business Associates
  - 3.17a Minimum Disclosure
  - 3.17b Business Associate Agreements
  - 3.17c Elements of the Business Associate Agreement
  - 3.17d Renewal of Business Associate Agreements
  - 3.17e Termination of Business Associate Agreements

### **3.20 IDENTITY THEFT PROGRAM POLICIES**

- 3.21 Purpose and Applicability
  - 3.21a Program Responsibility
  - 3.21b Definitions
- 3.22 Identification of Relevant Red Flags
  - 3.22a Covered Accounts
  - 3.22b Establishment of Covered Accounts
  - 3.22c Access for Covered Accounts
  - 3.22d Previous Identity Theft Experiences
- 3.23 Detecting Red Flags
- 3.24 Red Flag Responses
- 3.25 Annual Assessment
- 3.26 Board Approval
- 3.27 Annual Assessment

### **4.00 SECURITY POLICIES**

- 4.01 Applicability
- 4.02 Definitions
- 4.03 General Rules
  - 4.03a Policies, Interpretations and Procedures
- 4.04 Implementation Specifications
- 4.05 Administrative Safeguards
- 4.06 Security Management Process
  - 4.06a Risk Analysis
  - 4.06b Risk Management
  - 4.06c Sanction Policy
  - 4.06d Information System Activity Review
- 4.07 Assigned Security Responsibility
- 4.08 Workforce Security
  - 4.08a Authorization and/or Supervision
  - 4.08b Workforce Clearance Procedure
  - 4.08c Termination Procedure
- 4.09 Information Access Management
  - 4.09a Isolating Clearinghouse Functions
  - 4.09b Access Authorization
  - 4.09c Access Establishment and Modification
- 4.10 Security Awareness and Training
  - 4.10a Security Reminders
  - 4.10b Protection from Malicious Software
  - 4.10c Log-in Monitoring
  - 4.10d Password Management

4.11	Security Incident Procedures
4.11a	Response and Reporting
4.12	Contingency Plan
4.12a	Data Backup Plan
4.12b	Disaster Recovery Plan
4.12c	Emergency Mode Operation Plan
4.12d	Testing and Revision Process
4.12e	Applications and Data Criticality Analysis
4.13	Evaluation
4.14	Business Associate Agreements, Written Contracts and Other Arrangements
4.15	Physical Safeguards
4.16	Facility Access Controls
4.16a	Contingency Operations
4.16b	Facility Security Plan
4.16c	Access Control and Validation
4.16d	Maintenance Records
4.17	Workstation Use and Security
4.18	Device and Media Controls
4.18a	Disposal
4.18b	Media Re-Use
4.18c	Accountability
4.18d	Data Backup and Storage
4.19	Technical Safeguards
4.20	Access Control
4.20a	Unique User Identification
4.20b	Emergency Access Procedure
4.20c	Automatic Logoff
4.20d	Encryption and Decryption
4.21	Audit Controls
4.22	Integrity
4.22a	Mechanism to Authenticate EPHI
4.23	Person or Entity Authentication
4.24	Transmission Security
4.24a	Integrity Controls
4.24b	Encryption
4.25	Policies, Procedures and Documentation
4.26*	_____
4.27*	_____
4.28*	_____
4.29*	_____
4.30	Security Incidents
4.30a	Security Incident Examples

\* Policies 4.26 through 4.29 have been left blank intentionally. You may use these sections for supplemental policies and procedures that are necessary for your unique practice setting.

## **5.00** **FEDERAL IDENTIFIERS**

- 5.01 Effective Date and Compliance Date
- 5.02 National Provider Identifier (NPI)
- 5.03 Implementation Specification
- 5.04 National Provider Identifier Designations
- 5.05 National Plan and Provider Enumeration System (NPPES)
- 5.06 Implementation of NPI for Non-Electronic Providers

## **6.00** **ENFORCEMENT RULE**

- 6.01 Overview
- 6.02 Enforcement Guidance
  - "Civil Money Penalties: Procedures for Investigation, Imposition of Penalties, and Hearings" Federal Register, April 17, 2003
  - "HIPAA Administrative Simplification: Enforcement (Final Rule)" Federal Register, February 16, 2006

## **7.00** **HIPAA FORMS INDEX**

- 7.10 Confidentiality Statement
- 7.11 Employee Notice of Privacy Practices
- 7.12 Vendor Confidentiality Statement
- 7.20 Notice of Privacy Practices (Short Version)
  - Notice of Privacy Practices - Brochure Format
  - Notice of Privacy Practices - Posting Format
- 7.22 Business Associate Agreement
  - 7.22a Business Associate Agreement - Attachment A
- 7.30 Patient Authorization for Personal Representative
- 7.31 Patient Authorization for Disclosure of PHI
- 7.32 Patient Authorization for Disclosure to Designated Provider
- 7.33 Provider Request for Disclosure from another Covered Entity
- 7.34 Patient Authorization for Disclosure of PHI via E-Mail
- 7.40 Patient Privacy Complaint Form
- 7.60 Request for Access to PHI
- 7.70 Patient Request for Restriction of PHI
- 7.71 Acceptance/Denial of Requested Restriction
- 7.72 Termination of Patient Restriction
- 7.80 Patient Request for Amendment of PHI
- 7.81 Acceptance/Denial of Requested Amendment
- 7.90 Disclosure Accountability Request

## **8.00** **RESOURCE GUIDE**

- 8.01 Organization
- 8.02 Transaction Standard Index
- 8.03 Transaction Standard Questions and Answers
- 8.04 Privacy Rule Index
- 8.05 Privacy Rule Questions and Answers