A Look Inside MyHIPAA Guide

From: Diane Evans, PUBLISHER, MyHIPAA Guide

Email Diane Evans: devans@medmediamart.com
Phone: 1-877-438-1386

MyHIPAA GUIDE.COM

http://MyHIPAAGuide.com

The MyHIPAA Guide Process for HIPAA Compliance

1. Build a foundation

MyHIPAA Guide's Compliance Charter template sets the fundamental ethical principles for HIPAA compliance. The Charter:

~Defines the Compliance Officer (CO) role as that of creating and managing the compliance program
~Places responsibility for compliance on all in the organization
~Setting forth direct-line authority for the CO across the organization
~Protects the CO retaliation/personal liability

2. Take action

MyHIPAA Guide takes organizations through a 10-step compliance plan, and provides the resources for what's needed for critical tasks such as:
~Risk assessment
~Policies and procedures
~Business associate agreements
~Privacy notices
~Staff training
~Breach reporting and investigating

3. Stay compliant

Ultimately, the Charter is carried out through an annual Work Plan that spreads responsibility and holds individuals responsible for assigned tasks.

4. Pay special attention to social media abuses

MyHIPAA Guide has available:

~Social media guidelines
~Online courses for staff training
~On-site training

~Whistle-blower web page for confidential/anonymous reporting of potential abuses

MyHIPAA Guide Resources:

Appendix A: Sample page from Compliance Charter
Appendix B: Inventory of 50+ resources on MyHIPAA Guide
Appendix C: Sample page from annual Work Plan

Appendix A: Sample page from Compliance Charter template

This Charter sets out the fundamental ethical principles applicable to _____ and underlines the commitment of the Organization to a policy of integrity in the performance of its mission.

The observance of the compliance and integrity program constitutes an essential element of the reputation and of the image of _____. Adherence by the members of the organization to the principles contained in this Charter contributes to maintaining and safeguarding public confidence in the management and in the activities of _____ in the wider context of the communities we serve.

Implementation of these fundamental principles is a responsibility that falls individually on each member of the staff of the Organization and on each member of the relevant decision-making and management bodies. Committed to ensuring that the conduct of its activities conforms to this Charter, the Organization establishes a Compliance Officer and appoints _____as the Corporate Compliance Officer, with full, direct-line authority over compliance matters applicable to this Organization.

The Code of Conduct adopted by each member of the Organization establishes the guiding principles of this integrity program, fleshes out, and constitutes a key element of the Organization's governance.

Principles of Integrity and of Professional Ethics

Members of the staff and of the managing and management bodies of the Organization will carry out their tasks in compliance with the legislative and regulatory framework within which the Organization operates, as well as in compliance with generally accepted standards of good financial and administrative practice which shall include:

- Observance of the laws, rules and regulations applicable to _____ and to its activities;
- Observance of fairness, confidentiality and discretion in dealings with consumers and in all professional contacts;
- Loyalty, reliability and objectivity toward the member of the Organization which employs them;

Appendix B: Inventory of 50+ Cataloged Resources, organized by steps in the compliance process

Step 1:

- Overview of who's covered under HIPAA
- Link to submit inquiries to US Office for Civil Rights

Step 2:

- Overview of Compliance Officer responsibilities
- Compliance charter template to set CO job responsibilities and create a foundation for compliance
- 7-page overview titled *HIPAA Basics for Providers,* issued in 2015, includes:
  ~Examples of Records to Retain
  ~Breach notification timelines and resources
- 62-page *Guide to Privacy and Security of Electronic Information,* issued by HHS in April 2015, includes sections on:
  ~Understanding an individual's health information
  ~Breach notification, HIPAA enforcement, and civil and criminal penalties
  ~Chart with examples of potential information security risks with different types of EHR hosts
  ~List titled "Low-Cost, Highly Effective Safeguards"
  ~Table on examples of risks and how to mitigate them
  ~Links to games and videos for training workforce

Step 3:

- Overview of HIPAA documentation requirements
- Security Policy Template, which includes:
  ~Fill-in-the blank policies and procedures (mandates are color-coded in red)
  ~4 forms for reporting, investigating, logging and assessing a security breach
  ~Forms for logging approved vendors and software
  ~Confidentiality form
  ~Network access request form

Step 5:

- Explanation of security risk assessment
- Fact sheet on Top 10 Myths about risk analysis
- 4 videos to educate staff on risk assessment and contingency planning'
- Interactive security risk assessment tutorial with promptings on:
  ~What to consider in assessing risks
  ~Potential threats and vulnerabilities
  ~Examples of safeguards
  ~Boxes where you can document answers, comments, and risk remediation plans, and save them in PDF, Excel or in charts
- Listing of recent examples of breaches and settlements

Step 6:

- Introduction to 5 broad categories of potential risk
- 11-page federal information sheet on taking precautions with electronic health information
- 4-page federal *Safeguards* report that addresses emailing of health information with individuals and with other providers for treatment purposes
- The HHS-published *Security Standards Series*, which includes handy checklists and sample questions to consider relating to safe practices.
- Comprehensive tool kit, developed by the National Institute of Standards and Technology (NIST), to help organizations take the right actions for:
  ~basic security practices
  ~responding to security failures
  ~risk management
  ~dealing with personnel issues
- Federally produced guides, in the form fillable PDFs with checklists, to self-assessment of safety relating to:
  ~High Priority Safety Practices
  ~Organization Responsibilities
  ~Contingency Planning
  ~System Configuration
  ~System Interfaces
  ~Patient Identification
  ~Computerized Provider Order Entry
  ~Test Results Reporting and Follow Up

~Clinician Communication

Step 6:

- Overview on implementation of safeguards
- Annual Work Plan template to maintain accountability

Step 7:

- Overview of breach notification process
- Social media guidelines to help prevent breaches
- Breach notification procedures
- Link to the feds' portal for breach reporting

Step 8:

- Overview of heightened patient rights and corresponding obligations of provider organizations
- Templates for privacy notices in English and Spanish
- Report titled *Health Care Professionals' Privacy Guide* on HIPAA updates relating to communications
- Education materials that organizations can customize for staff training relating to communications

Step 9:

- Overview of who is a Business Association (BA)
- Sample terms for Business Associate Agreements
- Summary of June 2016 clarification from the feds on holding BAs accountable

Appendix C: Sample page from annual Work Plan

Compliance & Integrity Program

Annual Work Plan

Privacy & Security Program Work Plan					
Plan Area	**Program Goal**	**Actions**	**Deliverables**	**Due By**	**Resource**
New Employee & Annual Training	Provide all employees (as part of the Annual Integrity & Compliance Training) awareness and understanding of the Privacy & Security Programs and respons bility of employees	• Review/update employee training materials and based on the documented curriculum make sure they are current and address key messages • Resource annual training delivered in person, ad-hoc or through the LMS • Receive regular reports to track completion of annual training throughout the year with follow-up with department leaders	Resource all 28 NEO courses	Ongoing	Various
Security Training	Ensure employees and vendors with responsibilities for security & equipment whose job responsibilities require further knowledge and understanding of security protocols are provided ongoing training opportunities specific to their roles	• Implement a formal security awareness program targeted for information technology, vendor, and users • Assure all employees will receive the security training annually • For users issued portable devices, implement mandatory training upon receiving such equipment • All employees will acknowledge at least annually that they have read and understood the Information Acceptable Use Agreement • Individual training completion records will be kept for a defined time period • Training content will inform trainees of their responsibility to report all suspected information security incidents, system weaknesses, and violations of Acceptable Use • Vendors & Business Associates will also receive information annually on organizations standards	All Employees & Vendors receive Security Standards & Training	Ongoing	John Doe
Incident Management					
Security & Privacy Incident Response Process	Lead and manage operations of the PMHS standard Security & Privacy Incident Response Process	• Establish and maintain the incident management program to prepare for, detect, analyze, contain, eradicate, document, report, and recover from information security and privacy incidents/breaches • Document reporting & investigation procedures for: – Privacy Rights Violation/Issue – Identity Theft/Fraud – Improper destruction or disposal of PHI/PII – Inappropriate use of Authorized Access Privileges – Misdirected Fax – Theft/loss of documents – Theft/loss of mobile device – Unauthorized electronic disclosure of PHI/PII – Unauthorized use of PHI/PII – Unauthorized verbal disclosure of PHI/PII – Unauthorized Written Disclosure of PHI • Respond to all incidents involving PHI/PII and assure that established procedures to be followed upon notice of an incident, officials will provide notification to the Integrity & Compliance Officer and in-house or assigned legal	SBPIR procedures are documented for 11 types of incidents All incidents are recorded & reported through AEM	Ongoing	Jane Doe