MEDICAL OFFICE

COMPLIANCE TOOLKIT

The Complete Medical Practice Compliance Resource

HIPAA | HITECH | OSHA | CLIA

AAPC
PHYSICIAN SERVICES
Compliant and Profitable Practices

MEDICAL OFFICE COMPLIANCE TOOLKIT

The Complete Medical Practice Compliance Resource

HIPAA | HITECH | OSHA | CLIA

2011

AAPC
PHYSICIAN SERVICES
Compliant and Profitable Practices

Copyright 2011 by AAPC Physician Services

Parts of content copyright HCP—Used by permission

2500 South 3850 West, Suite B

Salt Lake City, Utah 84120

All rights reserved

MEDICAL OFFICE COMPLIANCE TOOLKIT

Hardcopy Table of Contents

HIPAA Privacy Information Reference	**Page 1**
HIPAA Privacy Forms	
HIPAA Security Information Reference	**Page 71**
HIPAA Security Forms	
OSHA Information Reference	**Page 179**
OSHA Forms	
CLIA Information Reference	**Page 261**
CLIA Forms	
ARRA and HITECH Information Reference	**Page 267**

This Compliance Toolkit includes over 75 online forms and documents that can be downloaded and customized to meet the needs of your practice. To access your online forms:

1. Login to your AAPC Member Account on the AAPC Web site (www.aapc.com)
2. In the left column, "View All" next to "Purchases"
3. Under the "Courses" tab, find the "Medical Office Compliance Toolkit"
4. Click that link to access your electronic forms and policy documents

ONLINE FORMS & POLICIES INDEX

- General Billing Audit Form
- General Employee Compliance Training Log
- General Medical Record Audit Form
- General Training Attendance Sheet
- HIPAA Privacy Business Associate Letter
- HIPAA Privacy Data Use Agreement
- HIPAA privacy Employee Confidentiality Agreement
- HIPAA Privacy Employee Disciplinary Action
- HIPAA Privacy Fax and Email Disclaimers
- HIPAA Privacy Fax Transmission Log
- HIPAA Privacy General Safeguards Checklist

- HIPAA Privacy Handling of Patient HIPAA Complaints
- HIPAA Privacy HHS Privacy Complaint Form
- HIPAA Privacy HIPAA Incident & Resolution Form
- HIPAA Privacy Notice of Privacy Practices
- HIPAA Privacy Patient Complaint Form
- HIPAA Privacy PHI Use and Disclosure Authorization
- HIPAA Privacy Privacy Audit Form
- HIPAA Privacy Privacy Officer Job Description
- HIPAA Privacy Psychotherapy Use and Disclosure Authorization
- HIPAA Privacy Report of PHI Disclosures
- HIPAA Privacy Request for Accounting of Disclosure of PHI
- HIPAA Privacy Request for Confidential Communications
- HIPAA Privacy Request for Restriction of Disclosure of PHI
- HIPAA Privacy Request Inspect or Copy Deseased PHI
- HIPAA Privacy Request to Amend Patient Records
- HIPAA Privacy Request to Copy or Inspect PHI
- HIPAA Privacy Response to Request for Confidential Communication
- HIPAA Privacy Response to Request Resctrictions of PHI
- HIPAA Privacy Response to Requests to Amend Patient Records
- HIPAA Privacy Response to Requests to Inspect PHI
- HIPAA Privacy Review of Denial to Inspect PHI
- HIPAA Privacy Revokation of Authorization to Use PHI
- HIPAA Privacy TCS Checklist
- HIPAA Security Breach Notification Checklist
- HIPAA Security Breach Notification to HHS
- HIPAA Security Breach Notification to Media
- HIPAA Security Breach Notification to Patient
- HIPAA Security Business Associate Agreement
- HIPAA Security Business Associate Checklist
- HIPAA Security Contingency Plan Template
- HIPAA Security Employee IT Access List
- HIPAA Security Employee Termination Checklist
- HIPAA Security Environmental Risk Analysis Samples
- HIPAA Security Equipment & Information Technology Inventory
- HIPAA Security Facility Maintenance Record
- HIPAA Security Facility Risk Analysis Samples
- HIPAA Security Hardware and Software Risk Analysis Samples
- HIPAA Security HIPAA Incident Summary Log
- HIPAA Security Incident Report
- HIPAA Security IT Access Change Request
- HIPAA Security IT system Activity Review Log
- HIPAA Security Sanctions Policy
- HIPAA Security Security Officer Job Description

- OSHA Bloodborne Exposure Incident Report
- OSHA Bloodborne Pathogens Exposure Control Chart
- OSHA Checklist Bloodborne Pathogens
- OSHA Checklist General Safety
- OSHA Checklist Hazard Communications
- OSHA Checklist Regulated Waste
- OSHA Confidential Employee Medical Record
- OSHA Consent To Draw And Test Blood
- OSHA Evaluation of Safety Syringes Safety Devices
- OSHA Exposure Control Plan Review
- OSHA Exposure Management Checklist
- OSHA Eyewash Testing Log
- OSHA Fire Extinguisher Inspection Log
- OSHA HBV Employee Exposure Determination
- OSHA Hepatitis B Vaccination Verification
- OSHA Housekeeping Checklist
- OSHA Housekeeping Cleaning Form
- OSHA Informed Refusal of Hepatitis B Vaccination
- OSHA Informed Refusal of Post Exposure Evaluation
- OSHA List of Regulated Substances
- OSHA Location PPE and Other Safety Equipment
- OSHA Minimum PPE
- OSHA NFPA Labeling System
- OSHA Qualitative Fit Test Form
- OSHA Request for Release of Exposure_Medical Record Information
- OSHA Request MSDS Sample Letter
- OSHA Safer Sharps Evaluation Log
- OSHA Sample MSDS
- OSHA Sharps Injury Log
- OSHA Sharps Injury Report
- OSHA Workplace Chemical Inventory
- Compliance Checklist HIPAA Privacy
- Compliance Checklist HIPAA Security and HITECH
- Compliance Checklist OSHA
- HIPAA Policies Procedures
- HIPAA Security PP
- OSHA Policies and Procedures
- EMR ROI Tool

Contents

HIPAA Privacy Reference Guide 1

Section 1: Introduction to HIPAA Privacy 1
- What is HIPAA? 1
- Who is Affected? 1
- Who Must Comply? 1
- HIPAA's Objective 2
- Key Components of HIPAA 2
- Acronyms 3
- HIPAA Privacy Compliance Officer Responsibilities 3

Section 2: Common Uses and Disclosures 9
- Health Care Operations 9
- Payment 9
- Required Uses and Disclosures of PHI 10
- Authorization 10
- Restriction for Use and Disclosure of PHI 11
- Uses and Disclosures Without Authorization 11
- Disclosure of an Entire Medical Record 12
- Minimum Necessary Standard 12
- Reasonable Reliance 13
- Incidental Uses and Disclosures 13
- Accounting for Uses and Disclosures 13
- Accidental Disclosures 14
- Mitigation 14
- Photographs 15
- Faxes and E-Mails 15

Section 3: Other Uses and Disclosures 17
- Marketing 17
- Research 17
- De-identified Health Information 18
- Research Use/Disclosure with Individual Authorization 18
- Limited Data Sets 18
- Data Use Agreement 19
- Research Use/Disclosure Without Individual Authorization 19
- Fundraising 20

Consumer Credit Reporting Agencies 20
Debt Collection Agencies 21
Public Health 21
Psychotherapy Notes 21
Authorization Required 21

Section 4: Safeguards 23
Sign–in Sheets 23
Call Verification 23
Phone Messages and Appointment Reminders 23
Reasonable Safeguards 24
Oral Communication 25
Unauthorized Visitors 25
Handling EOBs 25
Auditing 26

Section 5: Patient Access 27
Patient's Right of Access 27
Denial of Access 27
Destruction of Medical Records 29
Patient Access to the Entire "Designated Record Set" 29
Fees for Copying 29
Amending Patient Records 30
Patient's Right to Request Confidential Communication 30
Personal Representative 30
Immunization Records 31
Emergency Medical Care 31

Section 6: Legal Issues 33
Disclosures to Law Enforcement 33
Disclosures Allowed Without an Authorization 33
The Government's Role 40
State Law Preemption 40
Social Security Numbers 40

Section 7: Workforce Members 43
Training 43
Workforce Members 43
Medical Students And Other Medical Trainees 43
Employment Records 43
Sanctions 43

Section 8: Transactions and Code Sets 45
EDI Transactions 45
Code Sets 45
Implementation Guides 46
Companion Guides 46
Implementation of the EDI Standards 47

Section 9: National Identifiers. 49
National Employer Identifier (NEI) 49
National Provider Identifier (NPI) 50
National Health Plan Identifier 50
National Identifier for Individuals 50

Section 10: Enforcement and Complaints 51
Enforcement of the National Standards 51
Enforcement and Civil Money Penalties (CMP). 51
Privacy Complaints 51
Office for Civil Rights (OCR) Investigations 52
Transaction and Code Sets Complaints 52

HIPAA
Privacy Forms

BUSINESS ASSOCIATE LETTER

Dear _____,
("Business Associate")

As you are aware, The Health Insurance Portability and Accountability Act of 1996 (HIPAA) encompasses significant instructions and requirements regarding the control and care of protected health information (PHI). The prevailing sections of the act are commonly known as the HIPAA "Privacy Rule." The rule mandates that numerous precautions be taken and safeguards put in place to protect our patients' protected health information from unwanted disclosure and possible unauthorized use.

As a result, we are sending you our "Business Associate Privacy Agreement." This agreement protects our patients, our practice, and you as a business associate with whom we might have occasion and necessity to share pertinent protected health information in order to effect proper treatment.

Our practice requires that all those with whom we do business comply with the law and always use their best efforts to serve our patients. Together, we can assure our patients that their treatment is superior and their confidence is well placed.

To this end, please sign and return the enclosed agreement.

Sincerely,

Employee Non-Disclosure / Confidentiality Agreement

I have read and understand [**clinic name**] policies regarding the privacy of individually identifiable health information (or protected health information ("PHI")), pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In addition, I acknowledge that I have received training concerning the use, disclosure, storage and destruction of PHI as required by HIPAA, and that I have read and understand the material set forth in the HIPAA Training Handbook(s) provided by [clinic name]. I further understand that, through my affiliation with [clinic name], I will be exposed to privileged, intimate and personal information in addition PHI (such information and PHI shall collectively be referred to as "PHI" herein).

I understand that HIPAA requires many of [**clinic name**] clients to have detailed policies and procedures in place that dictate how employees can use patient information, when they can disclose it, and how they should dispose of it.

In consideration of my employment with and/or compensation from [clinic name], I hereby agree that I will not at any time—either during or after my employment or affiliation with (a) [**clinic name**] or (b) its clients—use, access or disclose PHI in any manner to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities with [clinic name] or its clients, and as permitted under their privacy policies and procedures as adopted and amended from time to time or as permitted under HIPAA. I understand that this prohibition includes, but is not limited to, disclosing any information about the identity of the patients with whom I work or any information about them, including their medical and other personal information, to family, friends, other patients, other clients, or co-workers, unless such person is lawfully authorized to receive such information. I agree to document uses and disclosure of PHI as required by the clients and/or HIPAA and to return or destroy all PHI associated with the clients upon the termination of my services. I agree that I immediately will report to [clinic name] and to the client with which I am placed any impermissible PHI use or disclosure.

I understand that my person access code, user ID, access key, password and similar access information will be kept confidential at all times. I understand that I will not remove from [**clinic name**] any devices or media unless instructed or authorized to do so. I agree to return all means of access to PHI upon termination of my employment with [clinic name].

I understand and acknowledge my responsibility to apply the policies and procedures of [clinic name]. I understand that unauthorized use or disclosure of PHI will result in disciplinary action, up to and including the termination of employment or affiliation with [clinic name] and its clients and could result in the imposition of civil and criminal penalties under applicable laws, as well as professional disciplinary action.

I understand that my obligations will survive the termination of my employment or end of my affiliation with [clinic name] and its clients, regardless of the reason for such termination. I understand that my obligations extend to any PHI that I may acquire during the course of my employment or affiliation with [**clinic name**] or its clients, whether in oral, written or electronic form and regardless of the manner in which access was obtained. I understand that I should contact an administrative officer of [**clinic name**] if I have any questions, comments or concerns about the training I received or my obligations under this agreement.

Signature of employee: _____ Date:_____

Print Your Name:_____

Contents

HIPAA Security Reference Guide 71

Section 1: Introduction to the Security Rule 71
Overview of the Security Rule 71
Security Controls 72
Security Rule Principles 72
The HIPAA Security Officer 74
Definitions 75

Section 2: Understanding the Security Rule 77
What Does the Rule Do? 77
Where Do I Start? 77
Documentation Requirements 79
Understand Your Information Systems 80
Security Rule Safeguards 80
Physical Safeguards 82
Technical Safeguards 84
Seven Steps to Security Compliance 85

Section 3: Administrative Safeguards 87
Standard #1: Assigned Security Responsibilities (Required) 87
Standard #2: Security Management Process 87
Standard #3: Workforce Security 96
Standard #4: Information Access Management 101
Standard #5: Security Awareness and Training 104
Standard #6: Security Incident Procedures 110
Standard #7: Contingency Plan 114
Standard #8: Evaluation (Required) 120
Standard #9: Business Associate Contracts (Required) 121

Section 4: Physical Safeguards 123
Standard #1: Facility Access Controls 123
Standard #2: Workstation Use (Required) 128
Standard #3: Workstation Security (Required) 129
Standard #4: Device and Media Controls 130

Section 5: Technical Safeguards 137
Standard #1: Access Control 137
Standard #2: Audit Controls (Required) 141

Standard #3: Integrity 144
Standard #4: Person or Entity Authentication (Required) 146
Standard #5: Transmission Security 147

Section 6: Organizational Requirements 151
Standard #1: Documentation (Required) 151
Standard #2: Policies and Procedures (Required) 151

HIPAA
Security Forms

Employee Termination Checklist

(Practice Name)

_____ _____

Employee Name Termination Date

- ☐ All building keys or badges have been returned to Security Officer.
- ☐ Email access has been eliminated. Account has been forwarded to Security Officer.
- ☐ Voicemail access has been eliminated. Account has been forwarded to appropriate staff.
- ☐ Intranet / System passwords have been terminated
- ☐ Employee IT Access List has been updated.
- ☐ Employee directory has been updated (website, phone lists etc.)
- ☐ Personal Computer / Laptop has been returned
- ☐ PDA's, pager, cell phone has been returned
- ☐ Unused vacation / sick time credited for last pay check
- ☐ Termination letter outlining benefits status and end dates has been provided
- ☐ Confidentiality agreements that were signed have been reviewed with employee
- ☐ Final timesheet and expenses submitted
- ☐ Exit interview conducted

_____ Date: _____

Administrator / HR Signature

Contents

OSHA Reference Guide 179

Introduction to OSHA Regulations for Health Care 180
What Is OSHA? 180
Your OSHA Compliance Officer 181

Standard #1: General Safety Compliance 185
Poster 185
Fire Safety 185
Building Safety 186
Workplace Safety 188

Standard #2: Blood Borne Pathogens Standard 197
Blood borne Pathogen Exposure Control Plan 197
Occupational Exposure Determination 197
Protection Against Blood Borne Diseases in the Health Care Environment 198
Universal Precautions 201
Work Practice Controls 201
Safer Sharps Evaluation 202
Engineering Controls 202
Personal Protective Equipment 203
Laundry 204
Housekeeping 204
Disinfection and Sterilization 205
Communication of Hazards to Employees 206
Exposure Incidents: Post-Exposure Evaluations and Follow Up 207
Steps to Take in Case of an Exposure Incident 208
Recordkeeping 209
Emergency Procedures/Contingency Plans 211
Work Areas and Non-Work Areas 212
Training Requirements 212
Exposure Control Plan Checklist 214

Standard #3: Hazard Communications Standard 217
Hazard Risk Assessment 217
Hazard Communications Policy 217
Master List of Hazardous Chemicals 217
Material Safety Data Sheets (MSDS) 217

Hazardous Chemical Labeling 219
Training 220

Standard #4: Regulated Waste Management 223
Biomedical Waste Plan 223
Training 225

OSHA Forms

Request for Release of Exposure / Medical Record Information

(Name of Practice)

Patient Name: _____

Date of Birth: _____

Patient Address: _____
Street City, State Zip

Requested patient information
Please describe the information that you would like us to provide a copy of:

_____

_____

_____

We will review your request to determine if the information can be made available to you. In some cases, we may be legally prohibited from disclosing certain information. For further details please refer to our Notice of Privacy Practice.

We will complete our review of your request within the next 15 days and contact you either by phone or writing to arrange for you to pick up a copy of your records. First time requests for information is provided free of charge. If you need additional copies, an administrative fee of $_____ will be charged for copying the requested material.

If we are unable to accommodate or deny your request, we will notify you in writing.

_____ _____
Patient Signature or Personal Representative Date

Office Use Only

Request was received by: _____ Date:_____
(Name and title of staff receiving / processing this request)

- ❑ **We hereby accept this request.**
- ❑ **We hereby deny this request.**

_____
Practice Representative (Type/Print)

_____
Practice Representative Signature

_____
Date

Contents

CLIA Compliance 261

Section 1: Overview and History 261
CLIA Certificate Types 261
Application for CLIA Certification 262
Expectations for Compliance with CLIA 263

CLIA Forms 265