

# The HIPAA Compliance Manual

## Table of Contents

<b>I.</b>	<b>HIPAA Privacy/Security Overview</b> .....	<b>1</b>
	Virtually All Medical Practices Are Covered by HIPAA .....	2
	What is Covered Under HIPAA? .....	2
	Be Careful Where You Get HIPAA Information .....	3
	Frequently Asked Questions .....	5
	Basic Requirements Under HIPAA Privacy/Security Provisions .....	8
	Summary of Privacy Forms .....	13
	Standardization of Transactions and Code Sets .....	14
	The Security Rule .....	18
<b>II.</b>	<b>Some HIPAA Myths</b> .....	<b>20</b>
	Reasonable Safeguards .....	20
	Incidental Uses and Disclosures .....	21
<b>III.</b>	<b>Legislative Background</b> .....	<b>25</b>
	HIPAA Regulations .....	26
	The Rule Making Process for Admin Simplification: What’s Taking So Long? .....	27
<b>IV.</b>	<b>Virtually All Medical Practices are covered by HIPAA</b> .....	<b>42</b>
<b>V.</b>	<b>What Is HIPAA Supposed to Protect?</b> .....	<b>44</b>
	Does HIPAA’s Privacy Protection Apply Only to Electronic Information? .....	45
<b>VI.</b>	<b>Enforcement, Fines and Penalties</b> .....	<b>51</b>
	Filing HIPAA Complaints .....	64
<b>VII.</b>	<b>General Rules for Disclosure of Protected Information</b> .....	<b>67</b>
<b>VIII.</b>	<b>Disclosures for Treatment, Payment, and Operations</b> .....	<b>71</b>
	Frequently Asked Questions .....	74
	Consent for Use and Disclosure of Health Information (Optional) .....	78
	Definition of Treatment, Payment and Health Operations .....	79
	Treatment .....	79
	Payment .....	80
	Health Care Operations .....	82
<b>IX.</b>	<b>Uses/Disclosures that Require a Patient’s Authorization</b> .....	<b>96</b>
	Exceptions to General Rules on Authorizations .....	97
	Sample Authorization Form for Use/Release of Health Information .....	100
	Designing a Valid Medical Practice HIPAA Authorization Form .....	101
	Regulations .....	103
	Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required. ....	121
	Workers’ Compensation .....	127
	Public Health Disclosures .....	129
	Frequently Asked Questions .....	130
	Transition – Consents/Authorizations Before April 2003 .....	133

# The HIPAA Compliance Manual

<b>X.</b>	<b>Disclosing the <i>Minimum Necessary</i></b> . . . . .	<b>135</b>
	Frequently Asked Questions . . . . .	137
	Final Regulations for <i>Minimum Necessary</i> : . . . . .	144
<b>XI.</b>	<b>Accounting for Authorized/Required Disclosures</b> . . . . .	<b>147</b>
	Do You Have to Document Oral Communications? . . . . .	148
	You Have Time to Respond (up to 90 days) . . . . .	149
	Regulations . . . . .	150
<b>XII.</b>	<b>Patients Are Entitled to a Copy of Medical Records And Have the Right to Request Amended Records</b> . . . . .	<b>159</b>
	Regulations . . . . .	166
	Patients May Amend Information In Medical Records . . . . .	168
<b>XIII.</b>	<b>Verification of Authorizations</b> . . . . .	<b>176</b>
<b>XIV.</b>	<b>Disclosing Patient Information to Family and Others</b> . . . . .	<b>181</b>
<b>XV.</b>	<b>Access to Minor’s Health Information by Parents and Personal Representatives</b> . . . . .	<b>187</b>
<b>XVI.</b>	<b>Research</b> . . . . .	<b>200</b>
	De-Identification of Protected Health Information . . . . .	203
	Frequently Asked Questions . . . . .	205
<b>XVII.</b>	<b>Marketing</b> . . . . .	<b>209</b>
<b>XVIII.</b>	<b>Notice of Privacy Practices</b> . . . . .	<b>226</b>
	Frequently Asked Questions . . . . .	228
	Notice of Privacy Practices – Example . . . . .	232
	Before Printing, Medical Practices Should Make Sure Their Notice: . . . . .	240
	Acknowledgment of Receipt of Notice . . . . .	241
<b>XIX.</b>	<b>Business Associates</b> . . . . .	<b>261</b>
	Frequently Asked Questions . . . . .	264
	Business Associate Contractual Language . . . . .	273
	Pertinent Business Associate Regulations . . . . .	277
<b>XX.</b>	<b>HIPAA and State Law</b> . . . . .	<b>280</b>
<b>XXI.</b>	<b>Does HIPAA Keep an Employer from Getting Copies of Employee’s Records</b> . . . . .	<b>282</b>
<b>XXII</b>	<b>Privacy Officer And Contact Person for Complaints/Questions</b> . . . . .	<b>284</b>
	Privacy Officer/Contact’s Responsibilities . . . . .	284
	Privacy Officer(s) in Affiliated Entities . . . . .	286

# The HIPAA Compliance Manual

<b>XXIII.</b>	<b>HIPAA Training</b> .....	<b>287</b>
	Acknowledgment Form Privacy/Security Training .....	288
<b>XXIV.</b>	<b>Written Policies and Procedures</b> .....	<b>289</b>
	An Illustration of A Policy/Procedure For A Typical Medical Practice .....	294
	General Rules and Reminders .....	296
	Job Descriptions .....	298
	Destruction of Records .....	300
	Transmission of Records .....	301
	Confidentiality Notice (fax, email) .....	301
	Verify Addresses, Fax Numbers, Email Addresses .....	301
	Disciplinary Actions .....	302
	Notice of Privacy Practices .....	302
	Complaints About Privacy/Security .....	303
	Duty to Mitigate .....	303
	Maintenance of Documentation Related to This Policy/Procedure .....	304
	Privacy Officer And Contact Person for Complaints/Questions .....	304
	Privacy Officer/Contact's Responsibilities .....	304
	Training .....	305
	Disclosures for Treatment, Payment, and Operations .....	307
	Release of Medical Records to the Patient or Subject to Patient's Authorization . . . .	310
	Patient Authorization for Release of Records to Third Parties .....	312
	Verification of Patient's Signature or Representations of Representative or Public Officials .....	313
	If a Patient Requests An Amendment or Correction to Their Records .....	315
	Accounting for Authorized/Required Disclosures .....	315
	Disclosing No More than the Minimum Necessary .....	316
	Right to Receive Confidential Communications .....	318
	Special Situations .....	319
	Access to Minor's Health Information by Parents .....	319
	Disclosures to Family Members and Others Involved .....	320
	Release of Psychotherapy Records .....	322
	Request for Psychiatric Records by the Patient .....	323
	Release of AIDS/HIV Records .....	323
	Request for Medical Records of Deceased Patient .....	323
	Mandatory Release/Reporting .....	324
	Disclosure of Records in Research .....	324
	Marketing .....	326
<b>XXV.</b>	<b>Security Rule</b> .....	<b>328</b>
	General Rules .....	335
	Required vs. Addressable Specifications .....	335
	Security Standards Matrix .....	341
	Security for the Small Group Practice .....	343
<b>XXVI.</b>	<b>Transaction and Code Set Standards</b> .....	<b>362</b>
	<b>Appendix</b> .....	<b>384</b>
	<b>CD-ROM – Law, Regs, Clarifications, User Modifiable Forms, etc. . . . .</b>	<b>Included With Manual</b>