

The ADA Practical Guide to **HIPAA Compliance**

Privacy and Security Manual

Table of Contents

CD-ROM Users Guide	i
---------------------------------	----------

Introduction/Getting Started	iii/v
---	--------------

Chapter 1: The 2013 Final Rule

Introduction	1
HIPAA History	2
Summary of the Changes in the 2013 Final Rule	4
A. Notice of Privacy Practices	4
B. Breach Notification	6
C. Business Associates and Subcontractors	8
D. Restricted Disclosure to a Health Plan	12
E. Patient Request to See and Get Copies of Records ("Access")	17
F. Subsidized Marketing Communications	21
G. Sale of Patient Information	25
H. Decedents	27
I. Enforcement	30
J. Penalties	31
K. Fundraising	33
L. Immunization Records	35
M. Genetic Information	37
N. Research	38
Government Resources	39

Chapter 1: Appendices

1-1 Definitions of Key Terms (Plain Language)	41
1-2 Definitions of Key Terms (Regulatory Language)	53

Chapter 2: 25 Steps Toward Privacy and Breach Notification Compliance

Step 1: Privacy Official	3
Step 2: Privacy Policies and Procedures	8
Step 3: Notice of Privacy Practices (“Notice” or “NPP”).....	11
Step 4: Designated Record Sets	18
Step 5: Minimum Necessary	21
Step 6: Verify Identity	26
Step 7: Required Disclosures	30
Step 8: Permitted Use and Disclosures	31
Step 9: Patient Authorization Forms	43
Step 10: Subsidized Marketing Communications	49
Step 11: Sale of Patient Information	57
Step 12: Mitigate Harm	58
Step 13: Business Associates.....	60
Step 14: Patient Rights and Requests	71
Step 15: Training	100
Step 16: Disciplinary Action (“Sanctions”)	103
Step 17: Retaliation and Intimidation.....	104
Step 18: Waiver of HIPAA Rights.....	106
Step 19: Documentation of HIPAA Compliance.....	107
Step 20: Safeguard Patient Information.....	109
Step 21: De-identification.....	112
Step 22: Breach Notification	115
Step 23: Complaints.....	135
Step 24: Fundraising.....	138
Step 25: Review and Revise	140

Chapter 2: Appendices

2.1.1 Sample Designation of Privacy Official.....	5
2.1.2 Sample Privacy Official Job Description	6
2.2 Sample Acknowledgement of Receipt of HIPAA Policies and Procedures	10
2.3.1 Sample Notice of Privacy Practices.....	14
2.3.2 Sample Acknowledgement of Receipt of Notice of Privacy Practices	17
2.4 Sample List of Designated Record Sets	20
2.5.1 Sample Workforce Access to Patient Information.....	24
2.5.2 Sample Routine Disclosures and Requests	25
2.6 Sample Verification of Identity	29
2.8 Sample Decision Tree: Decedent PHI.....	42
2.9 Sample Authorization Form for Use or Disclosure of Patient Information.....	47

2.10.1	Sample Patient Authorization for Marketing – All Products and Services	51
2.10.2	Sample Patient Authorization for Marketing – Single Product or Service	53
2.10.3	Sample Patient Authorization for Marketing – Single Company.....	55
2.13	Sample Business Associate Agreement	65
2.14.1	Sample Request for Access.....	77
2.14.2.1	Sample Request for Amendment	83
2.14.2.2	Sample Denial of Request to Amend	84
2.14.2.3	Sample Amendment Request Log	85
2.14.3.1	Sample Log of Disclosures of Patient Information.....	90
2.14.3.2	Sample Request for Accounting of Disclosures	91
2.14.4	Sample Request for Confidential Communications	94
2.14.5	Sample Request for Restricted Use or Disclosure	98
2.15	Sample HIPAA Training Sign-in Sheet.....	102
2.22.1	Sample Breach Assessment Form	125
2.22.2	Sample Breach Log	129
2.22.3	Sample Agreement to Receive Electronic Communication	132
2.22.4	Full Disk Encryption Q&A	133
2.23	Sample Complaint Log.....	137

Chapter 3: Protected Health Information

Chapter 4: Administrative Safeguard Standards: HIPAA Security Rule

Administrative Standards and Implementation Specifications.....	2
Security Management Process	3
Risk Analysis	4
Sanction Policy	7
Information System Activity Review.....	8
Assigned Security Responsibility	9
Workforce Security	11
Authorization and/or Supervision	12
Workforce Clearance Procedure	13
Termination Procedures.....	14
Information Access Management	16
Isolating Health Care Clearinghouse Functions	18
Access Authorization.....	19
Access Establishment and Modification.....	20
Security Awareness and Training.....	21
Security Reminders	22
Protection from Malicious Software.....	23
Log-in Monitoring	24
Password Management	25

Security Incident Procedures	27
Response and Reporting.....	28
Contingency Plan	29
Data Backup Plan.....	31
Disaster Recovery Plan.....	32
Emergency Mode Operation Plan.....	33
Testing and Revision Procedures.....	35
Applications and Data Criticality Analysis.....	36
Evaluation	37
Business Associate Contracts and Other Arrangements	39
Written Contract or Other Arrangement.....	41

Chapter 4: Appendices

Appendix 4-1: NIST Activities and Sample Questions Regarding Administrative Safeguards.....	43
Appendix 4-2: Sample HIPAA Security Risk Assessment For A Small Dental Practice.....	63
Appendix 4-3: NIST Appendix E: Risk Assessment Guidelines.....	81
Appendix 4-4: Sample Acknowledgement of Responsibilities Regarding Access to Practice’s Electronic Systems Containing Electronic Protected Health Information.....	89
Appendix 4-5: Sample Consequences of Unauthorized Access to the Practice’s Electronic Protected Health Information.....	90
Appendix 4-6: Sample Workforce Member Exit Interview Checklist.....	91
Appendix 4-7: Sample Workforce Member Acknowledgement of Awareness and Understanding of Practice’s Exit Interview.....	92
Appendix 4-8: Sample Security Incident Report.....	93
Appendix 4-9: Sample Security Incident Log.....	94

Chapter 5: Technical Safeguard Standards: HIPAA Security Rule

Fundamentals About Technical Safeguards	2
Access Control	5
Unique User Identification.....	6
Emergency Access Procedure.....	7
Automatic Logoff.....	8
Encryption and Decryption.....	9
Audit Controls	10
Integrity	11
Mechanism to Authenticate Electronic Protected Health Information.....	12
Person or Entity Authentication	13
Transmission Security	14
Integrity Control.....	16
Encryption.....	17
Chapter Summary	18

Chapter 5: Appendices

Appendix 5-1: HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information	19
Appendix 5-2: NIST Activities and Sample Questions Regarding Technical Safeguards.....	27
Appendix 5-3: Emergency Access Log	36

Chapter 6: Physical Safeguards Standards: HIPAA Security Rule

Facility Access Controls	4
Contingency Operations.....	5
Facility Security Plan.....	6
Access Control and Validation Procedures.....	8
Maintenance Records.....	9
Workstation Use	10
Workstation Security	12
Device and Media Controls	14
Disposal	17
Media Re-Use.....	18
Accountability.....	19
Data Backup and Storage.....	20

Chapter 6: Appendices

Appendix 6-1: NIST Activities and Sample Questions Regarding Physical Safeguards.....	21
Appendix 6-2: Sample Maintenance Repair Log	27
Appendix 6-3: Sample Electronic Media and Hardware Movement Log	28

Chapter 7: Training is the Key to Compliance..... 1

HIPA Training Overview.....	1
What You're Required to Do	1
Sample Training Update Topics	3

Chapter 7: Appendices..... 9

Appendix 7.1: Sample 12-Month Security Refresher Training Sessions.....	9
---	---

Chapter 8: 12 Key Things to Remember: HIPAA Privacy, Security, and Breach Notification

Web Resources