Contents

Acknowledgments xi
Introduction xiii

CHAPTER 1
Welcome to HIPAA  1
   I. Title I  2
   II. Title II  3
   III. Title III  6
   IV. Title IV  9
   V. Title V  9
   VI. Overview of Title II  10
       A. Privacy Rule  10
       B. Security Rule  11
       C. Enforcement Rule  13
   VII. Conclusion  14

CHAPTER 2
The Basics  15
   I. Fundamentals  15
       A. Who Needs to Comply?  15
       B. What Information Is Subject to HIPAA?  23
       C. General Rules for Disclosure  27
       D. What If Other Laws Conflict with HIPAA?  29
   II. Conclusion  30
CHAPTER 3
Authorizations for Release of Protected Health Information 33

I. Consent versus Authorization: What’s the Difference? 33
   A. Consent 34
   B. Authorization 34

II. Authorizations 35
   A. Core Elements 35
   B. Required Statements in Authorizations 44
   C. Other Requirements for Authorizations 45
   D. Other Considerations for Authorizations 46

III. Federal Trade Commission Act 48

IV. State Law Requirements 50
   A. HIPAA Preempts State Laws 50
   B. Elements of Authorizations under State Law 52
   C. Psychiatric Records under State Law 52

V. Conclusion 53

CHAPTER 4
Disclosures without Authorizations 55

I. Treatment, Payment, or Health Care Operations 56
   A. Treatment 56
   B. Payment 57
   C. Health Care Operations 59

II. Averting a Serious Threat to Health or Safety 68

III. Providing Access to Individuals via a Third Party 69

IV. Law Enforcement 69

V. Public Health Activities 71

VI. Victims of Abuse, Neglect, or Domestic Violence 72

VII. Lawful Oversight Activities 74

VIII. Judicial and Administrative Proceedings 75

IX. Informational and Promotional Disclosures 78
   A. Facility Directories 78
   B. Friends and Relatives 79
CHAPTER 5
Administrative Requirements for Covered Entities and Business Associates 87

I. Administrative Requirements 88
   A. Notice of Privacy Practices 89
   B. Accounting for Disclosures 95
   C. Disclosures to Public Health Officials 98

II. Administrative Safeguards 100
    A. Covered Entity Obligations 101
    B. Business Associates 103

III. Conclusion 104

CHAPTER 6
Summary of the HIPAA Security Rule 107

I. Purpose and Scope of the Security Rule 107

II. Who Needs to Comply? 110

III. Administrative, Physical, and Technical Safeguards 110
    A. Administrative Safeguards 111
    B. Physical Safeguards 119
    C. Technical Safeguards 119

IV. Organizational Requirements 121
    A. Business Associate Agreements 121
    B. Policies and Procedures 122

V. Conclusion 122
CHAPTER 7
The HITECH Act 123

I. Requirements for Business Associates 124
   A. Compliance Requirements for Business Associates 124
   B. Special Business Associate Considerations 128
   C. Business Associate Agreements 131

II. HIPAA Breaches 133
   A. Risk Assessments 134
   B. Breach Response 135

III. Other HITECH Act Provisions 135

IV. Conclusion 136

CHAPTER 7 APPENDIX:
HIPAA Business Associate Agreement 137

CHAPTER 8
Responding to a Security Incident or Breach: Mechanics of Incident Response and Breach Notification 151

I. Definition of a Security Incident under HIPAA 151

II. Response and Notification Requirements for a Security Incident under HIPAA 152

III. Definition of a Breach under HIPAA 153

IV. Analysis of the HIPAA Breach Notification Rule 154
   A. Has a Breach Occurred? 155
   B. Who to Notify? 157

V. Steps to Take after the Breach 162

VI. Conclusion 162
# Table of Contents

## I. GENERAL INFORMATION APPLICABLE TO ALL PRIVACY AND SECURITY POLICIES
- Policy Statement
- Scope of These Privacy and Security Policies
- Applicability of These Policies
- Defined Terms

## II. WHEN THE PROVIDER MAY MAKE DISCLOSURES OF PHI WITHOUT AUTHORIZATION
- Purpose of Policy
- Policy Detail

## III. NOTIFICATION OF PRIVACY OR SECURITY BREACHES
- Purpose of Policy
- Policy Detail

## IV. NOTICE OF PRIVACY PRACTICES PROCEDURES
- PURPOSE OF POLICY
- POLICY DETAIL
- WHO IS AFFECTED

## V. MINIMUM NECESSARY STANDARD
- Purpose of Policy
- Policy Detail

## VI. INDIVIDUAL'S REQUEST TO RESTRICT USES AND DISCLOSURES OF PHI
- Purpose of Policy
- Policy Detail
VII. INDIVIDUAL’S REQUEST FOR CONFIDENTIAL COMMUNICATIONS 203
   Purpose of Policy 203
   Policy Detail 203

VIII. INDIVIDUAL’S RIGHT OF ACCESS TO PHI 204
   Purpose of Policy 204
   Policy Detail 204

IX. INDIVIDUAL’S REQUEST TO AMEND PHI 212
   Purpose of Policy 212
   Policy Detail 212
   Amendment or Correction: 216

X. INDIVIDUAL’S REQUEST FOR AN ACCOUNTING OF DISCLOSURES 217
   Purpose of Policy 217
   Policy Detail 217

XI. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS 222
   Purpose of Policy 222
   Policy Detail 222

XII. WAIVER OF RIGHTS 222
   Purpose of Policy 222
   Policy Detail 222

XIII. DOCUMENTATION REQUIREMENTS AND RETENTION OF RECORDS 223
   Purpose of Policy 223
   Policy Detail 223

XIV. TRAINING ON HIPAA PRIVACY AND SECURITY POLICIES 225
   Policy Statement 225
   Scope of this Policy 226
   Purpose of Policy 226
   Policy Detail 226
XV. DISCIPLINARY SANCTIONS FOR NONCOMPLIANCE WITH PROVIDER’S PRIVACY AND SECURITY POLICIES 227
    Purpose of Policy 227
    Policy Detail 227

XVI. REPORTING AND MITIGATING INADVERTENT OR IMPROPER DISCLOSURES OF PHI OR SECURITY INCIDENTS 228
    Purpose of Policy 228
    Policy Detail 228

XVII. ADMINISTRATIVE, TECHNICAL, AND PHYSICAL PRIVACY AND SECURITY SAFEGUARDS 230
    Purpose of Policy 230
    Policy Detail 231

XVIII. VERIFICATION OF PERSONS REQUESTING PHI 241
    Purpose of Policy 241
    Policy Details 241

XIX. AUTHORIZATIONS 244
    Purpose of Policy 244
    Policy Details 244

XX. REQUESTS FOR DISCLOSURES OF AN INDIVIDUAL’S PHI FROM SPOUSES, OTHER FAMILY MEMBERS, AND FRIENDS/FACILITY DIRECTORIES 246
    Purpose of Policy 246
    Policy Details 246

XXI. DISCLOSURES TO BUSINESS ASSOCIATES 248
    Purpose of Policy 248
    Policy Details 248

XXII. DE-IDENTIFIED INFORMATION, SUMMARY HEALTH INFORMATION, AND LIMITED DATA SETS 249
    Purpose of Policy 249
    Policy Details 249
XXIII. COMPLAINTS 251
Purpose of Policy 251
Policy Details 251

XXIV. DESIGNATED RECORD SETS 252
Purpose of Policy 252
Policy Details 253

XXV. DESIGNATED PERSONNEL/ACCESS PROFILES 254
Purpose of Policy 254
Policy Detail 254

XXVI. STATE LAW COMPLIANCE 255
Purpose of Policy 255
Policy Detail 255
Procedural Guidance 256

XXVII. USING AND DISCLOSING PSYCHOTHERAPY NOTES 256
Background 256
Policy 257

XXVIII. WORKFORCE EMPLOYEE SCREENING 257

XXIX. FUNDRAISING 257
Purpose of Policy 257
Policy Detail 257

XXX. SALE OF PROTECTED HEALTH INFORMATION 259
Purpose of Policy 259
Policy Detail 259

APPENDIX B
HIPAA Business Associate Agreement (Favorable to Data Source) 261

About the Authors 281
Table of Cases 283
Index 000