

# HIPAA Portability, Privacy & Security

## Table of Contents

[See also the Table of Contents behind each Appendix Tab]

About the Authors .....	i
How to Use This Manual .....	ii
Current Developments .....	see the Current Developments Tab
Statutes, Regulations, Sample Documents, and Other Items .....	see the Appendix Tabs

### Outline Table of Contents

<p><b>PART 1 OF 5</b> <b>INTRODUCTION</b></p>
---

<b>I. Overview of This Manual .....</b>	<b>1</b>
A. <i>What This Manual Covers</i> .....	1
1. Part 1—Introduction .....	1
2. Part 2—Portability Rules .....	1
3. Part 3—Insurance Market Rules .....	2
4. Part 4—Administrative Simplification Rules .....	2
5. Part 5—Additional HIPAA Rules Affecting Group Health Plans .....	2
B. <i>Provisions in HIPAA That This Manual Does Not Cover</i> .....	2
C. <i>Other EBIA Manuals Provide Guidance for Group Health Plans</i> .....	2
<b>II. HIPAA Portability, Privacy &amp; Security: A Short Course .....</b>	<b>31</b>
A. <i>This Short Course Is for You</i> .....	31
B. <i>What You Will Learn in the Short Course</i> .....	32
C. <i>HIPAA Applies to Most Group Health Plans</i> .....	32
D. <i>Consequences of Failing to Comply With HIPAA</i> .....	33
E. <i>Limitations on Preexisting Condition Exclusions</i> .....	33
1. Restrictions on PCEs .....	33
2. Preexisting Conditions Cannot Be Applied to Certain Individuals .....	34
3. Creditable Coverage Reduces PCE Period .....	35
4. Notice Requirements to Impose a PCE .....	36
5. Plan or Issuer Must Issue Certificate of Creditable Coverage .....	36
6. New Plan Must Review Information and Issue PCE Determination Notice .....	36
F. <i>Special Enrollment Rights</i> .....	36
1. Loss of Other Coverage .....	36
2. Becoming Eligible for State Premium Assistance Subsidy .....	37
3. Acquisition of New Dependent .....	37

4.	Notice Requirements .....	38
5.	COBRA Qualified Beneficiaries Have Special Enrollment Rights.....	38
G.	<i>Nondiscrimination Rules</i> .....	38
1.	What Is a Health Status-Related Factor? .....	38
2.	Prohibited Discrimination in Eligibility, Premiums, and Contributions.....	38
3.	Nondiscrimination Rules for Benefits.....	39
4.	Wellness Incentives .....	39
5.	Discrimination in Favor of Individuals With Adverse Health Conditions .....	40
6.	The Genetic Information Nondiscrimination Act (GINA).....	40
H.	<i>Prohibitions on Dollar Limits and Rescissions</i> .....	40
1.	Lifetime and Annual Dollar Limits .....	40
2.	Prohibition on Rescissions .....	41
I.	<i>HIPAA’s Portability Rules in Practice—Amy’s &amp; Bob’s Stories</i> .....	41
1.	Amy Starts Work .....	41
2.	Bob Starts Work .....	42
3.	Amy and Bob Get Married (But Not to Each Other, Of Course).....	42
4.	Amy’s Husband Loses Health Coverage .....	42
5.	Bob Has a Child.....	43
6.	Amy and Bob Are Laid Off.....	43
J.	<i>Compliance Checklist for HIPAA’s Portability Requirements</i> .....	43
1.	Plan Design Issues .....	43
2.	Plan Document .....	44
3.	Summary Plan Descriptions (SPDs).....	46
4.	Other Communications to Participants.....	46
5.	Administrative Procedures .....	47
K.	<i>HIPAA’s Insurance Market Rules</i> .....	47
L.	<i>Overview of HIPAA’s Administrative Simplification Requirements</i> .....	47
1.	Which Entities Must Comply? .....	48
2.	What Information Is Covered?.....	48
M.	<i>How the Privacy &amp; Security Rules Affect Group Health Plans and Plan Sponsors</i> .....	49
1.	How Do the Privacy & Security Rules Apply to Group Health Plan Sponsors? .....	49
2.	Sharing Group Health Plan PHI With the Plan Sponsor.....	49
3.	Requirements for Business Associates.....	51
4.	Breach Notification Requirements .....	51
N.	<i>Core Privacy Requirements</i> .....	51
1.	Core Requirement #1: Use and Disclosure Rules .....	51
2.	Core Requirement #2: Individual Rights & Privacy Notice .....	52
3.	Core Requirement #3: Administrative Requirements .....	53
O.	<i>HIPAA Privacy Rule in Practice: Three Plan Sponsors</i> .....	54
1.	Fully Insured Group Health Plan: Plan and Employer Are “Hands-Off” PHI .....	54
2.	Fully Insured Group Health Plan: Plan and Sponsor Are “Hands-On” PHI.....	54
3.	Self-Funded Group Health Plans and Their Sponsors.....	54
P.	<i>Core Security Requirements</i> .....	55
1.	Entities Subject to the Security Rule .....	56

2. Relationship Between the Privacy Rule and the Security Rule .....	56
3. Security Standards and Implementation Specifications .....	56
4. Documenting HIPAA Security Rule Compliance.....	57
Q. EDI Standards .....	57
R. Privacy and Security Compliance Checklist.....	57
1. General Health Plan Activities .....	58
2. Determine Privacy Requirements for Each Health Plan.....	58
3. Determine Security Requirements for Each Health Plan .....	58
4. Breach Notification Requirements .....	59
5. Other HIPAA Compliance Concerns .....	59
S. Conclusion .....	59
<b>III. [Reserved].....</b>	<b>111</b>
<p><b>PART 2 OF 5</b></p> <p><b>HIPAA’S PORTABILITY, SPECIAL ENROLLMENT AND NONDISCRIMINATION RULES</b></p>	
<b>IV. Portability: Sources of Governing Law .....</b>	<b>111</b>
A. Statutes .....	111
1. HIPAA .....	111
2. GINA Amended HIPAA Provision .....	112
3. Children’s Health Insurance Program Reauthorization Act of 2009 Amended HIPAA Provision.....	112
4. Health Care Reform Significantly Impacts HIPAA Provisions.....	112
B. Legislative History .....	112
C. Regulations.....	112
1. Jointly Issued Interim Regulations .....	112
2. Jointly Issued “Clarification” of Interim Regulations.....	112
3. Interim Final Regulations on Nondiscrimination and Proposed Rules on Wellness Programs.....	113
4. Jointly Issued Final Regulations .....	113
5. Jointly Issued Final Regulations on Nondiscrimination and Wellness Programs .....	113
6. Jointly Issued Interim Final Regulations on Nondiscrimination Based on Genetic Information.....	113
7. Jointly Issued Interim Final Regulations on PCEs, Coverage Limits, and Rescissions .....	113
D. EBSA/DOL Publications .....	113
E. Other Agency Notices and Publications .....	113
F. IRS Notice 98-12 .....	113
G. Some State-Law Requirements May Apply to Insured Plans .....	114
1. The General Rule With Regard to Laws Affecting HIPAA’s PCE and Special Enrollment Provisions .....	114
2. Is a State Law Affecting HIPAA’s PCE Requirements That Is More Beneficial Than HIPAA in Some (but Not All) Ways Saved From Preemption?.....	115
3. Scope of HIPAA Preemption With Regard to Nondiscrimination Requirements .....	117
4. Which State’s Laws Apply? .....	117
<b>V. How Are HIPAA’s Portability Requirements Enforced? .....</b>	<b>151</b>
A. Both Employers and Issuers Are Responsible for HIPAA Portability Compliance .....	151
1. What Is a HIPAA Group Health Plan?.....	152
2. What Is a HIPAA Health Insurance Issuer? .....	152

B. Much of HIPAA Is Jointly Enforced by the DOL, IRS, and HHS .....	152
C. IRS Excise Taxes for HIPAA Violations.....	153
D. HIPAA Enforcement by the DOL.....	154
1. Overview of the DOL’s Enforcement Authority .....	154
2. DOL Audits of Health Plans .....	154
E. HIPAA Enforcement by HHS.....	155
1. Overview of CMS Enforcement Authority .....	155
2. CMS Enforcement When States Fail to Enforce HIPAA Requirements .....	155
3. Noncompliance and Penalties .....	155
F. Penalties for Violation of Genetic Information Nondiscrimination Act.....	157
1. DOL, HHS, and IRS Penalties Under Title I of GINA.....	157
2. Amount of Penalty .....	157
3. Exceptions and Limitations .....	157
4. EEOC Enforcement Under Title II of GINA .....	157
G. Private Lawsuits .....	158
<b>VI. What Plans Are Subject to HIPAA’s Portability Requirements? .....</b>	<b>191</b>
A. Overview .....	191
B. Table: Which Plans and Benefits Are Subject to HIPAA Portability?.....	192
C. What Is a Group Health Plan?.....	193
1. Group Health Plan Definitions .....	193
2. Under ERISA and PHSA Definitions, a Group Health Plan Must Be an ERISA Employee Welfare Benefit Plan .....	194
3. Plans Covering Partners, Sole Proprietors, and Independent Contractors .....	195
4. Individual Health Insurance Policies Can Be Subject to HIPAA’s Group Rules .....	196
D. What Is a Health Insurance Issuer? .....	199
1. Health Insurance Issuer .....	199
2. Group Health Insurance Coverage .....	199
3. Individual Health Insurance Coverage.....	200
4. Stop-Loss Coverage Probably Is Not Subject to HIPAA’s Portability Rules .....	200
E. Small Group Health Plans, Including Retiree-Only Plans .....	201
1. Plans Covering Less Than Two Participants as Current Employees .....	201
2. Retiree-Only Medical Plans .....	201
F. Excepted Benefits: Certain Health FSAs, Dental, Vision, and Others.....	202
1. Health Flexible Spending Accounts Meeting Certain Conditions .....	202
2. Certain Benefit Types .....	206
3. Limited-Scope Benefits (Including Dental and Vision) .....	206
4. Certain Independent, Noncoordinated Benefits .....	208
5. Certain Supplemental Benefits.....	209
G. Wellness Programs.....	212
1. Stand-Alone Wellness Programs .....	213
2. Wellness Programs That Relate to Group Health Plans .....	213
H. Governmental Group Health Plans.....	213
1. Group Health Plans of State and Local Governmental Employers .....	213
2. Group Health Plans of Tribal Government Employers .....	215

3. Medicare, Certain Other Federal Government Programs, and Certain Tribal Programs .....	216
<i>I. Church Group Health Plans</i> .....	216
1. Generally .....	216
2. Limited Exception From Nondiscrimination Rules .....	216
<i>J. Health Savings Accounts (HSAs) and Archer Medical Savings Accounts (MSAs)</i> .....	217
1. Most HSAs Will Not Qualify as Group Health Plans .....	217
2. Archer MSAs as Group Health Plans .....	218
<i>K. Health Reimbursement Arrangements (HRAs)</i> .....	218
1. HRAs Are Group Health Plans .....	218
2. What Exceptions Might Apply to HRAs? .....	218
<b>VII. HIPAA's Restrictions on Preexisting Condition Exclusions</b> .....	<b>241</b>
<i>A. Overview—Preexisting Condition Exclusions, Creditable Coverage, and Other Limitations</i> .....	241
<i>B. Flowchart: Operation of HIPAA's PCE Provisions</i> .....	244A
<i>C. HIPAA's Limitations on Preexisting Condition Exclusions</i> .....	244B
1. What Is a Preexisting Condition? .....	244C
2. What Preexisting Conditions May Be Excluded From Group Health Plan Coverage? .....	244C
3. Maximum Duration: The 12-Month Look-Forward Rule (18 Months for Late Enrollees) .....	247
4. Enrollment Date Triggers the 6-Month Look-Back and 12-Month Look-Forward Periods— Important to Take into Account the “Waiting Period” .....	248
5. Using Creditable Coverage to Offset the Maximum Duration .....	250
6. Affiliation Periods .....	250
<i>D. Applying the PCE</i> .....	251
1. Medical Advice, Diagnosis, Care, or Treatment Must Have Been Recommended or Received During the 6-Month Look-Back Period .....	251
2. Subsequent Sickness or Injury Must Be Directly Attributable to the Preexisting Condition .....	255
3. Provider of Care Must Be Licensed .....	255
4. Conditions First Discovered During a Waiting Period Are Not Preexisting Conditions .....	256
5. Does a Benefit-Specific Waiting Period Operate as a PCE? .....	256
<i>E. Illustrations of the 6-Month Look-Back and 12-Month Look-Forward Rules</i> .....	257
<i>F. The Creditable Coverage Rules</i> .....	257
1. Group Health Plan Coverage .....	258
2. Health Insurance Coverage .....	259
3. Medicaid and Other Coverage .....	259
4. Excepted Benefits Do Not Count as Creditable Coverage .....	260
<i>G. Specifics of the PCE 12-Month Look-Forward Rule With Offsets for Creditable Coverage</i> .....	261
1. Overview .....	261
2. Coverage Before a 63-Day Break Generally Is Not Counted as Creditable Coverage .....	261
3. Creditable Coverage Before a 63-Day Break Is Counted for Certain Individuals Under the Trade Act of 2002 .....	263
4. Creditable Coverage Before a 63-Day Break is Counted for Certain Individuals For Purposes of COBRA Premium Assistance .....	264
5. Waiting Periods Generally Do Not Count as a Break in Coverage .....	265
6. Impact of Overlap Between Waiting Period and Creditable Coverage .....	266
7. Illustrations of How the Creditable Coverage Rules Work .....	267
8. Options for Determining Creditable Coverage .....	267

9. HMO Affiliation Period as Alternative .....	270
H. Notice Requirements to Impose a PCE .....	270
1. The Initial (General) PCE Notice Requirement.....	270
2. Individual PCE Determination Notice .....	273
I. Application of PCEs to Alternate Recipients Under QMCSOs.....	275
1. May a PCE Be Applied to an Alternate Recipient?.....	275
2. If the Plan Applies a PCE, What Is the Length of the Exclusionary Period?.....	276
J. Plan Designs and Strategies.....	276
<b>VIII. HIPAA Certificate of Creditable Coverage: Obligation to Furnish .....</b>	<b>291</b>
A. Overview .....	291
B. Who Must Furnish the HIPAA Certificate? .....	292
1. Self-Funded Plans .....	292
2. Insured Plans.....	292A
3. Employee Changing Coverage Options Under a Single Plan .....	293
4. Employer Changes Insurance Carriers .....	294
C. To Whom Must a HIPAA Certificate Be Issued?.....	294
1. When Is an Employer Deemed to Know About a Dependent’s Cessation of Coverage? .....	294
2. Must a Certificate Be Provided to a Domestic Partner Who Loses Coverage? .....	295
D. What Triggers the Requirement to Issue a HIPAA Certificate?.....	295
1. Certificate Must Be Automatically Provided Upon a Loss of Coverage .....	295
2. Upon Request.....	297
3. May the New Employer Request a Certificate From the Prior Plan?.....	298
4. Does HIPAA Require That Certificates Be Provided to Persons Who Have Not Lost Coverage? .....	298
5. Must a Certificate Be Issued to an Individual Who Terminates During the Waiting Period?.....	298
6. Must a Certificate Be Issued to a Newborn Whose Expenses Are Covered by Mom’s Coverage? .....	298
7. Must a Certificate Be Issued to Retiring Employees Who Will Immediately Qualify for Retiree Medical Coverage?.....	298A
8. HIPAA Certificates and FMLA Leave.....	298A
9. Caution for Employers With Multiple Plans .....	299
E. Content of the HIPAA Certificate.....	300
1. General Information Must Be Included on All HIPAA Certificates.....	300
2. Coverage Details—Depends on Length of Coverage .....	300
3. Special Content Rule When Participant Requests Certificate.....	301
4. Coordinating HIPAA Certificate With COBRA Election Notice .....	301
5. Certificates May Be Required Even When There Is No COBRA Qualifying Event .....	302
F. Method of Delivery of HIPAA Certificate.....	302
1. First-Class Mail to Last-Known Address.....	302
2. Electronic Disclosure of HIPAA Certificate .....	302
G. Procedures for Requesting Certificates .....	303
H. HIPAA Certificate Obligation: Mergers & Acquisitions.....	304
1. Stock Acquisition.....	304
2. Asset Acquisition .....	304
3. “COBRA Plus” Rules of Thumb for Merger & Acquisition Certifications .....	304

<b>IX. HIPAA Certificate of Creditable Coverage: Obligations Upon Receipt .....</b>	<b>331</b>
A. Overview .....	331
B. Individual Notice of Determination.....	331
C. When Should a HIPAA Certificate Be Processed? .....	333
D. How to Handle Claims or Inquiries Received Before a Determination Is Made .....	334
E. Modifying an Individual Notice .....	334
F. Consequences of Relying Upon an Erroneous or Fraudulent Certificate .....	334
G. Limiting Exposure Relating to the Receipt of a HIPAA Certificate.....	335
H. Demonstrating Creditable Coverage Without a HIPAA Certificate.....	335
<b>X. Special Enrollment Rights .....</b>	<b>371</b>
A. Overview .....	371
B. Individuals Who Lose Coverage .....	371
1. Employee or Dependent Must Have Had Coverage When Coverage Was Previously Offered .....	372
2. The Coverage That's Lost Must Have Been Under a Group Health Plan or Health Insurance .....	373
3. Coverage Must Be Lost as a Result of a Statutorily Prescribed Event .....	375
4. Plan May Impose Requirement to State in Writing Why Coverage Is Declined .....	380
5. Employee Usually Must Request Enrollment Within Specified Timeframes.....	382
6. Who Has Special Enrollment Rights as a Result of Loss of Other Coverage?.....	383
7. Recommendation That Special Enrollees Sign Special Enrollment Form .....	384
8. Effective Date of Special Enrollment .....	384
9. All Benefit Packages Must Be Available at Special Enrollment .....	384
C. Individuals Who Become Eligible for State Premium Assistance Subsidy.....	385
1. Who Can Enroll.....	385
2. Length of Special Enrollment Period.....	385
3. Effective Date of Enrollment .....	386
4. Benefit Packages Available at Special Enrollment .....	386
D. Acquisition of a New Dependent.....	386
1. Who Can Enroll? .....	386
2. Length of Special Enrollment Period.....	388
3. Effective Date of Enrollment .....	389
4. All Benefit Packages Must Be Available at Special Enrollment .....	390
E. Who Qualifies as a Dependent for Special Enrollment?.....	391
F. Disclosure Requirements for Special Enrollment Rights .....	393
1. Notice of Special Enrollment Rights .....	393
2. Summary Plan Description (SPD) .....	396
3. Additional Notice and Disclosure Relating to State Premium Assistance Subsidy.....	396
G. COBRA Qualified Beneficiaries Have Special Enrollment Rights.....	398
1. Qualified Beneficiaries on COBRA May Add Family Members Under the Special Enrollment Rules .....	398
2. But Qualified Beneficiaries Must Be Receiving COBRA Coverage to Have Special Enrollment Rights .....	398A
H. Cafeteria Plan Issues.....	399
1. Cafeteria Plan Election Changes Permitted If They Correspond With HIPAA Special Enrollment.....	399
2. Do Special Enrollment Rights Apply to Health FSAs? .....	399

3. The “Tag-Along” Rule .....	399
4. Retroactive Changes .....	401
5. Prospective Election Changes Outside of HIPAA’s Minimum Special Enrollment Window .....	401
6. Loss of Medicare, Medicaid or CHIP Entitlement; Eligibility for Medicaid or CHIP .....	402
<i>I. Retirees and Special Enrollment</i> .....	402
1. Retiree Medical Plans, Long-Term Disability Continuees, and Survivors .....	402
<i>J. Other Issues Involving Special Enrollment Rights</i> .....	403
1. HIPAA Special Enrollments and QMCSOs .....	403
2. Plans Can Go Beyond What HIPAA Requires .....	403
3. Special Enrollment and Preexisting Condition Exclusion Periods .....	403
4. Are Other Eligibility Requirements Measured as of Date of Triggering Event or Date When Special Enrollment Is Requested? .....	404
5. May a Plan Enforce a Waiver of Special Enrollment Rights? .....	404
<i>K. Action Items—Children’s Health Insurance Program Reauthorization Act</i> .....	405
<i>L. Special Enrollment Rights Under Health Care Reform (Transition Rules)</i> .....	406
1. Coverage for Certain Adult Children .....	406
2. Reinstating Individuals Who Previously Exhausted a Plan’s Lifetime Limit .....	406
<b>XI. Health Status and Genetic Information Nondiscrimination Rules</b> .....	<b>421</b>
<i>A. Overview and Sources of Rules</i> .....	421
<i>B. What Is a Health Status-Related Factor?</i> .....	421
<i>C. Nondiscrimination Rules for Eligibility and Benefits</i> .....	423
1. Nondiscrimination Rules for Eligibility—In General .....	423
2. Some PCE Limitations and Exclusions Are Permissible (Until 2014) .....	424
3. Eligibility Rules and Benefit Restrictions That Apply to All Similarly Situated Individuals Are Permissible .....	425
4. HRAs and HIPAA Nondiscrimination Rules .....	428
5. Benefit-Specific Waiting Periods Raise Additional Issues .....	429
6. Special Rules Apply to Source-of-Injury Exclusions or Limitations .....	430
<i>D. No Discrimination in Individual Premiums or Contributions</i> .....	431
<i>E. Defining Groups of “Similarly Situated Individuals”</i> .....	432
1. Groups of Participants Based on Bona Fide Employment Classifications .....	433
2. Differences Permitted Between Participants and Beneficiaries .....	433
3. Differences Permitted Among Beneficiaries .....	434
4. Differences Directed at Specific Individuals Not Allowed .....	434
<i>F. Nonconfinement Provisions, Traditional Actively-at-Work and Continuous-Service Clauses Not Allowed</i> .....	434
1. Traditional Actively-at-Work or Continuous-Service Requirements Violate HIPAA .....	436
2. Limited Actively-at-Work or Continuous-Service Provision Permissible .....	436
3. First-Day-of-Work Rule Permissible .....	437
4. Plan May Terminate Coverage When Eligibility Criteria Are No Longer Satisfied .....	437
5. Making Sense of the Actively-at-Work Prohibition .....	438
<i>G. Plans May Discriminate in Favor of Individuals Who Have Adverse Health Conditions</i> .....	439
<i>H. No Discrimination on the Basis of Genetic Information</i> .....	440
1. Key Terminology .....	440
2. GINA’s Prohibitions and Limitations .....	442

3. Wellness Programs Offered Outside Group Health Plans May Also Raise Issues Under GINA .....	448
4. GINA’s Proposed Modifications to HIPAA’s Privacy Regulations .....	450
5. Enforcement Under GINA .....	451
<i>I. Wellness Programs Must Meet Specific Requirements.....</i>	<i>451</i>
1. What Is a Wellness Program? .....	452
2. Health Risk Assessments .....	452
3. Participation-Only Programs: Wellness Programs That Do Not Reward Participants Based on a Health Factor .....	453
4. Standard-Based Programs: Requirements for Wellness Programs That Provide Rewards Based on a Health Factor .....	453
5. Examples of Standard-Based Wellness Programs That Meet HIPAA’s Requirements .....	457
6. Examples of Standard-Based Wellness Programs That Do Not Meet HIPAA’s Requirements.....	459
7. Wellness Program Checklist.....	459
8. ADA Considerations.....	460
9. Cafeteria Plan Issues.....	463
10. State-Law Issues .....	464
<i>J. Steps to Reduce Adverse Selection .....</i>	<i>464</i>
<i>K. Transition Rule for Governmental Plans Opting Into HIPAA Coverage.....</i>	<i>465</i>
<i>L. Limited Exception for Certain Grandfathered Church Plans .....</i>	<i>465</i>
<b>XII. Lifetime and Annual Dollar Limits; Prohibition on Rescissions .....</b>	<b>481</b>
<i>A. Lifetime and Annual Dollar Limits .....</i>	<i>481</i>
1. Overview .....	481
2. What Are “Essential Health Benefits” for Purposes of Complying With the Lifetime and Annual Dollar Limits? .....	481
3. Who Must Comply? .....	482
4. Prohibition on Lifetime Limits.....	483
5. Prohibition on Annual Limits .....	485
<i>B. Prohibition on Rescissions .....</i>	<i>490A</i>
1. Who Must Comply? .....	491
2. What Constitutes a Rescission?.....	491
3. Rescission Requires Advance Written Notice .....	491
4. Certain Retroactive Terminations of Coverage Are Permissible .....	492
5. Application of Rescission Rules.....	492
<b>XIII. HIPAA in the SPD .....</b>	<b>501</b>
<i>A. ERISA Requires Group Health Plans to Furnish SPD .....</i>	<i>501</i>
<i>B. ERISA Requires SPD Disclosures About Benefits and Loss of Benefits .....</i>	<i>501</i>
<i>C. HIPAA Portability Requirements in the SPD .....</i>	<i>501</i>
1. Preexisting Condition Exclusions (PCEs).....	501
2. Special Enrollment Periods .....	502
3. Nondiscrimination Rules .....	503
4. Prohibition on Lifetime and Annual Dollar Limits .....	504
5. Prohibition on Rescissions of Coverage .....	504
6. Claims Procedures .....	504
7. Disclosure of Interaction Between HIPAA and COBRA .....	504

D. HIPAA Privacy and Security in the SPD .....	505
E. SPD Disclosures About Other Federal Mandates .....	505
<b>XIV. HIPAA Portability Checklists.....</b>	<b>541</b>
A. Overview .....	541
B. Plan Design Issues .....	541
C. Plan Document.....	542
1. Preexisting Condition Exclusions (PCEs).....	542
2. Special Enrollment Periods .....	542
3. Nondiscrimination Rules .....	543
4. Prohibitions on Dollar Limits and Rescissions .....	543
5. Claims Procedures .....	544
D. Summary Plan Descriptions (SPDs).....	544
E. Other Disclosures to Participants.....	544
F. Administrative Procedures .....	545
<b>XV. Mistakes Happen: Correcting HIPAA Portability and Nondiscrimination Compliance Problems.....</b>	<b>581</b>
A. Overview .....	581
1. Consequences of Failing to Satisfy HIPAA’s Portability and Nondiscrimination Requirements .....	581
2. Self-Correction May Help to Minimize Consequences of Noncompliance .....	581
3. Importance of Plan’s Claims Procedure and Limitations Periods.....	582
B. Chart: Possible Corrective Action.....	582
C. PCE Limitation and Notice Violations.....	584
1. Failure to Provide Initial Notice of PCE.....	585
2. Incorrect Determination That Specific Individual or Condition Was Subject to PCE .....	585
3. Incorrect Determination of Duration of PCE Limitation Period.....	585
D. HIPAA Certificate Violations.....	586
1. The Requirement .....	586
2. Failure to Issue HIPAA Certificates: The Correction .....	586
3. Failure to Properly Track Coverage Under Multiple Coverage Options Within a Single Plan: The Correction .....	586
E. HIPAA Special Enrollment Violations .....	586
1. The Requirement .....	586
2. Failure to Provide Notice: The Correction .....	587
3. Failure to Allow Required Special Enrollment: The Correction .....	587
4. Imposing a Longer PCE period on Special Enrollees: The Correction .....	587
F. HIPAA Nondiscrimination Violations.....	587
1. The Requirement .....	587
2. Eligibility Denied: The Correction.....	587
3. Impermissible Contribution Rate or Benefits Exclusion: The Correction .....	588
4. Failure to Offer a Reasonable Alternative Standard (or Waiver) Under a Wellness Program: The Correction .....	588
5. Failure to Adequately Disclose That an Alternative Standard (or Waiver) Is Available Under a Wellness Program: The Correction .....	588
G. GINA Violations.....	588
1. The Requirement .....	588

2. Health Risk Assessment Contained Impermissible Family Medical History Questions: The Correction .....	588
3. Inadvertent Collection of Genetic Information: The Correction .....	589
<i>H. Lifetime and Annual Limit Violations</i> .....	589
1. The Requirement .....	589
2. Impermissible Imposition of Lifetime Dollar Limit: The Correction .....	589
3. Impermissible Imposition of Annual Dollar Limit: The Correction .....	589
<i>I. Rescission of Coverage Violations</i> .....	589
1. The Requirement .....	589
2. Impermissible Rescission of Coverage: The Correction .....	590

<b>PART 3 OF 5</b> <b>INSURANCE MARKET RULES</b>
---

<b>XVI.-XVII. [Reserved]</b> .....	<b>691</b>
<b>XVIII. Group Insurance Market Requirements</b> .....	<b>693</b>
<i>A. Overview—Group Insurance Market Rules</i> .....	693
1. What Is a Health Insurance Issuer That Is Subject to the Group Insurance Rules? .....	694
2. When Is an Issuer Offering Insurance in the Small Group Market? .....	695
3. Potential Applicability of Group Market Rules to Individual Coverage .....	699
<i>B. Guaranteed-Renewability Rules Applicable to All Group Insurance</i> .....	700
1. Product Withdrawal Requirements .....	700
2. Market Exit Requirements .....	701
<i>C. Guaranteed-Availability Rules Applicable to Small Group Market (and to Large Group Market in 2014)</i> .....	701
1. Issuers Must Accept Every Small Employer and Make All Actively Marketed Products Available.....	702
2. Issuers Must Accept Every Eligible Individual When First Eligible .....	703
3. Effect of HIPAA’s Small Group Requirements on State-Law Group Participation Rules .....	704
<i>D. Special Rules Applicable to “Bona Fide Association” Plans</i> .....	705
1. Associations and “Bona Fide Associations” .....	705
2. Restrictions on Membership Not Permitted .....	706
3. Is Coverage That Is Offered Through an Association Group or Individual Coverage? .....	706
4. Guaranteed Availability and Coverage Offered to Members of a Bona Fide Association .....	707
5. Guaranteed Renewability and Coverage Offered to Members of a Bona Fide Association .....	707
<i>E. Renewability Rules Apply to Multiemployer Plans That Are Group Health Plans</i> .....	708
<i>F. Fair Health Insurance Premium Requirement</i> .....	708
1. Application of Premium Requirement .....	708
2. Special Rule for Grandfathered Health Coverage .....	708
<i>G. Comprehensive Health Coverage Requirement</i> .....	708
1. Insurers in the Small Group Market Must Offer Essential Health Benefits .....	709
2. Insurers in the Small and Large Group Markets and Group Health Plans (Including Self-Insured Plans) Must Comply With Cost-Sharing Limits .....	709
3. Insurers in the Small Group Market Must Meet Coverage-Level Requirements.....	710
4. Special Rule for Grandfathered Health Plans .....	711

H. Accounting for Costs and Rebate Requirement.....	711
1. Requirement to Prepare Report and Provide Rebates .....	711
2. Coverage That Is Grandfathered Must Comply.....	712
I. Preemption Issues .....	712
<b>XIX. HIPAA’s Individual Insurance Market Rules.....</b>	<b>731</b>
A. Overview .....	731
B. What Is a Health Insurance Issuer Offering Coverage in the Individual Market? .....	732
1. Individual Market Defined .....	732
2. Conversion Coverage.....	732
3. Coverage Offered Through Associations.....	732
4. Individual Policies Offered Through the Employer’s Workplace.....	733
C. Excepted Benefits .....	733
1. Blanket Exception for Certain Benefit Types .....	733
2. Limited-Scope Benefits (Including Dental and Vision) .....	733
3. Certain Independent, Noncoordinated Benefits .....	734
4. Medicare and CHAMPUS Supplemental Insurance.....	734
5. Other Similar Supplemental Insurance Coverage .....	734
D. Guaranteed Availability .....	734
1. Definition of an Eligible Individual.....	735
2. Insurer Must Use Reasonable Diligence to Determine Whether Applicant Is an Eligible Individual .....	739
3. Insurer Must Not Prevent Seamless Coverage .....	740
4. Medical Questionnaires May Be Used for Limited Purposes .....	740
5. Issuer May Limit Coverage to Two Policies .....	741
E. Federal Requirements Do Not Apply in a State That Has Implemented an Alternative Mechanism .....	742
F. Guaranteed Renewability.....	743
1. All Individuals Purchasing Coverage in the Individual Market Are Entitled to Renew .....	743
2. Coverage Provided Through Association Plans .....	743
3. Nonrenewal of Coverage Permitted in Limited Circumstances .....	743
G. Certificate of Creditable Coverage.....	745
H. No Discrimination on the Basis of Genetic Information .....	745
1. What Is “Genetic Information”?.....	746
2. Limitations on Eligibility, Premiums, and PCEs .....	746
3. Limitation on Requesting or Requiring Genetic Testing .....	746
4. Prohibition on Collection of Genetic Information .....	747
I. No Discrimination on the Basis of a Health Status-Related Factor.....	748
1. What Are Health Status-Related Factors?.....	748
2. Special Rule for Grandfathered Health Coverage.....	748
J. Fair Health Insurance Premium Requirement.....	748
1. Application of Premium Requirement .....	749
2. Special Rule for Grandfathered Health Coverage.....	749
K. Comprehensive Health Coverage Requirement .....	749
1. Insurers in the Individual Market Must Offer Essential Health Benefits .....	749
2. Insurers in the Individual Market Must Comply With Cost-Sharing Limits .....	750

3. Insurers in the Individual Market Must Meet Coverage Level Requirements .....	750
4. Special Rule for Grandfathered Health Plans .....	750A
<i>L. Accounting for Costs and Rebate Requirement.....</i>	<i>750A</i>
1. Requirement to Prepare Report and Provide Rebates .....	750A
2. Coverage That Is Grandfathered Must Comply.....	750A
<b>XX. [Reserved].....</b>	<b>751</b>

<b>PART 4 OF 5</b> <b>ADMINISTRATIVE SIMPLIFICATION</b>
--

<b>XXI. Privacy, Security, and EDI: Sources of Law and Enforcement.....</b>	<b>751</b>
<i>A. Introduction .....</i>	<i>751</i>
<i>B. Statutes .....</i>	<i>752</i>
1. HIPAA Statute .....	752
2. The Health Information Technology for Economic and Clinical Health Act .....	753
3. The Patient Protection and Affordable Care Act .....	753
<i>C. Regulations and Compliance Dates.....</i>	<i>753</i>
1. Chart: Regulations and Compliance Dates.....	753
2. Privacy Regulations.....	755
3. Security Regulations.....	755
4. Transactions and Code Sets Regulations .....	756
5. Other Regulations .....	757
6. Other Guidance .....	758
<i>D. Enforcement .....</i>	<i>758</i>
1. Complaints and Compliance Reviews .....	758
2. Civil Money Penalties.....	767
3. Recordkeeping for CMS HIPAA Investigations .....	776
4. HIPAA Compliance Audits by HHS .....	776
5. Criminal Penalties.....	778
6. No Specific Private Cause of Action in the Statute or Regulations.....	779
7. Cause of Action for State Attorneys General Under the HITECH Act .....	781
8. Plan Document May Result in ERISA Fiduciary Liability for Noncompliance With Administrative Simplification Provisions.....	782
9. HIPAA Insurance.....	782A
<i>E. State Laws Affecting Administrative Simplification.....</i>	<i>782A</i>
1. Subject to Several Significant Exceptions, HIPAA Preempts Contrary State Laws .....	782A
2. Impact of ERISA Preemption for Health Plans Subject to ERISA .....	790
3. Gramm-Leach-Bliley Privacy Laws Are Subject to HIPAA Preemption Analysis .....	792
4. Other Federal Privacy Laws Generally Are Not Affected by HIPAA .....	792
<b>XXII. Privacy, Security, and EDI: What Information Is Protected and Which Entities Must Comply?.....</b>	<b>801</b>
<i>A. What Information Is Protected?.....</i>	<i>801</i>
1. Health Information .....	802
2. Individually Identifiable Health Information.....	803
3. Protected Health Information (PHI) .....	803
4. De-Identified Information Is Not PHI.....	807

5. PHI Created Before the Effective Date of the HIPAA Regulations .....	807
6. Electronic PHI Is Subject to HIPAA’s Security Standards .....	808
7. Special Disclosure Rules for Certain Types of PHI .....	810
8. PHI in Designated Record Set Is Subject to Access and Amendment .....	810
9. FERPA Education Records and Treatment Records Are Not PHI.....	811
<b>B. Which Entities Must Comply?.....</b>	<b>814</b>
1. Covered Entities .....	814
2. Business Associates.....	819
3. Vendors of Personal Health Records and Other Non-HIPAA Covered Entities .....	820
<b>C. What Is a “Health Plan”?.....</b>	<b>821</b>
1. Health Plan Defined .....	821
2. “Group Health Plan” Defined .....	822
3. What Is Medical Care?.....	822
4. Types of Plans and Whether They Must Comply .....	822
<b>D. Special Rules for Certain Types of Covered Entities.....</b>	<b>837</b>
1. The Hybrid Entity .....	837
2. Affiliated Covered Entities.....	838
3. Covered Entity That Performs Multiple Covered Functions .....	839
4. Organized Health Care Arrangement.....	839
5. Processing Payment Transactions by Financial Institutions Excluded .....	841
6. Covered Entities That Participate in Health Information Sharing Arrangements .....	842
<b>E. Notification Requirements In the Case of a Breach of Unsecured PHI.....</b>	<b>844</b>
1. What Constitutes a Breach?.....	844
2. Notification by Covered Entities .....	849
3. Notification by Business Associates.....	852
4. Application to Vendors of Personal Health Records and Related Entities.....	853
5. Administrative Requirements and Burden of Proof .....	855
6. Impact of HITECH Breach Requirements on State Law .....	855
7. Action Steps for Compliance .....	855
<b>XXIII. How the Privacy and Security Rules Affect Group Health Plans and Plan Sponsors .....</b>	<b>871</b>
<b>A. Introduction to HIPAA’s Privacy and Security Requirements.....</b>	<b>871</b>
1. Overview: Privacy and PHI; Security and Electronic PHI.....	872
2. Overview: Who Must Comply With HIPAA’s Privacy and Security Requirements? .....	872
3. Overview: What Does the Privacy Rule Require? .....	873
4. Overview: What Does the Security Rule Require? .....	874
<b>B. Quick Reference of Common Employer Issues That May Be Affected by the HIPAA Privacy Rule .....</b>	<b>874</b>
<b>C. Sharing PHI and Electronic PHI With Plan Sponsors.....</b>	<b>887</b>
1. Employer Information or Plan Information? .....	887
2. Disclosure of Information From Group Health Plan to Sponsor .....	888
3. Disclosure of De-Identified Information .....	889
4. Disclosure of Group Health Plan Enrollment Information.....	889
5. Disclosure of Summary Health Information for Limited Purposes.....	892
6. Disclosure of PHI Pursuant to an Authorization.....	893

7. Disclosure of PHI and Electronic PHI for Plan Administration Functions: Plan Document, Certification, and Firewall Requirements .....	893
8. Can An Employer Take Employment Action Against an Employee Who Commits Fraud Against the Health Plan? .....	898
<i>D. Many Common Employer Functions Require Authorization .....</i>	<i>903</i>
1. Plan Generally May Not Condition Treatment, Payment, Enrollment, or Eligibility on Receipt of an Authorization.....	903
2. In Some Circumstances, an Employer May Condition Employment on Receipt of an Authorization .....	903
3. Is Drug and Alcohol Testing Information Health Information? May It Be Disclosed to an Employer Without an Authorization? .....	904
4. Authorization Might Be Required to Obtain PHI for Purposes of FMLA or ADA.....	904
5. An Authorization May Be Required for an Employer to Help Its Employee With a Claim.....	907
6. Authorization Required for Employers to Receive Confirmation From an EAP That Employees Have Received Employer-Mandated Counseling .....	907
<i>E. HIPAA Exceptions Permit Some Common Employer Practices.....</i>	<i>908</i>
1. State/Federal Law Disclosure Requirements .....	908
2. Workers' Compensation .....	908
3. Health information Contained in Employment Records.....	909
<i>F. Applying the HIPAA Privacy and Security Rules to Group Health Plans and Their Sponsors.....</i>	<i>909</i>
1. Chart Summarizing Plan Sponsor Responsibilities in Various Scenarios.....	910
2. Fully Insured Group Health Plans .....	911
3. Self-Funded Group Health Plans .....	916
<i>G. Contracting With Business Associates.....</i>	<i>923</i>
<i>H. HIPAA and ERISA Claims Procedures.....</i>	<i>923</i>
1. Who Is Responsible for ERISA Claims Procedures? .....	924
2. Administrative Safeguards to Ensure Consistency in Benefit Determinations .....	925
3. Benefit Claim Notices: Providing PHI of Spouse or Child to Plan Participant .....	925
4. PHI Disclosures to Claimant's Authorized Representative.....	927
5. Business Associate Contracts for Medical Experts Consulted on Benefit Claims .....	928
6. Consultation With Medical Professionals .....	928
<i>I. Sharing PHI With Other Benefit Plans of the Same Employer .....</i>	<i>929</i>
1. May a Group Health Plan Share PHI With Other Plans of the Same Employer? .....	929
2. Locating Missing 401(k) Plan Participants .....	930
<i>J. HIPAA Privacy and Security and the Summary Plan Description.....</i>	<i>930</i>
1. Should the SPD Include a Description of HIPAA Privacy or Security Rights? .....	931
2. May a Plan Satisfy Its Obligation to Provide the Notice of Privacy Practices by Including the Notice in the SPD? .....	931
<i>K. HIPAA Privacy and Security and the Medicare Part D Retiree Drug Subsidy .....</i>	<i>932</i>
<i>L. HIPAA Privacy and Collective Bargaining.....</i>	<i>933</i>
1. Does the HIPAA Privacy Rule Apply to the Information? .....	933
2. Is an Accommodation Available That Would Permit the Employer to Disclose the Information? .....	934
<i>M. HIPAA Privacy and Security Issues for Debit Card Programs Under Health FSAs and HRAs.....</i>	<i>934</i>
1. What Types of Debit Card Transactions Are Allowed by the IRS? .....	935
2. Looking Behind the Plastic: The Parties in a Debit Card Transaction .....	938

3.	Recordkeeping Requirements for Health FSA and HRA Debit Card Programs.....	938A
4.	HIPAA Privacy and Security Implications for Debit Card Transactions.....	938B
N.	<i>HIPAA Privacy and Security Issues for Employers Whose Employees “Telework”</i> .....	940A
1.	Teleworkers Raise Special Issues .....	940A
2.	Teleworking Action Plan for Employers .....	940B
<b>XXIV.</b>	<b>Business Associate Contracts .....</b>	<b>941</b>
A.	<i>What Is a Business Associate?</i> .....	943
1.	HIPAA’s Definition of Business Associate.....	944
2.	Certain Service Providers Are Business Associates .....	946
3.	Service Providers That Might Be Business Associates .....	946B
4.	Relationships That Generally Are Not Business Associate Arrangements .....	951
5.	Health Insurer or HMO Generally Is Not a Business Associate of Plan.....	953
6.	Stop-Loss Insurer Is Not a Business Associate of Plan .....	954
7.	Exceptions to Business Associate Contract Requirement.....	954
B.	<i>Contract Must Include Specific Privacy and Security Provisions</i> .....	955
1.	Required Terms of a Business Associate Contract.....	956
2.	Fewer Requirements for Business Associates Than for Covered Entities (but HITECH Act Changed Much of That).....	960
3.	Violations of Privacy and Security Provisions by Business Associate .....	961
4.	Business Associates Must Comply With EDI Standards .....	963
5.	Additional Items Included by HHS in Sample Business Associate Contract Provisions.....	963
6.	Business Associate Contract Compliance Dates .....	964
7.	Changes to Business Associate Contracts Due to HITECH Act Changes .....	965
C.	<i>Agents and Subcontractors of a Business Associate</i> .....	969
1.	Must a Business Associate Monitor Its Agents or Subcontractors? .....	970
2.	Must a Business Associate Obtain the Return of PHI From Its Agents or Subcontractors?.....	971
3.	What Should Be In a Business Associate Subcontract? .....	971
D.	<i>The Business Associate Contract: Beyond HIPAA’s Requirements</i> .....	975
1.	Drafting Contracts From the Plan Sponsor/Covered Entity’s Perspective.....	975
2.	Drafting Contracts From the Business Associate’s Perspective .....	978
E.	<i>HIPAA Audits</i> .....	980
F.	<i>Contracting With Business Associates: An Overview of ERISA Issues</i> .....	982
1.	Prudent Selection of Business Associates.....	982
2.	Form and Content of the Contract.....	982
3.	Remedies, Right to Terminate, and Indemnification .....	983
4.	Monitoring Business Associates.....	983
G.	<i>Attorneys as Business Associates</i> .....	983
1.	When Are Attorneys Business Associates?.....	983
2.	Special Business Associate Contract Issues for Attorneys.....	984
H.	<i>Transferring PHI Outside the United States</i> .....	990
I.	<i>Roadmap for Compliance</i> .....	990
<b>XXV.</b>	<b>[Reserved] .....</b>	<b>999</b>

<b>XXVI. Core Privacy Requirement #1: Use and Disclosure Rules</b> .....	<b>999</b>
A. <i>Introduction to Use and Disclosure Rules</i> .....	999
B. <i>Uses and Disclosures for Treatment, Payment, and Health Care Operations</i> .....	1000
1. Covered Entities Generally May Use and Disclose PHI for Treatment, Payment, and Health Care Operations.....	1000
2. What Are Treatment, Payment, and Health Care Operations?.....	1002
3. Sharing PHI for Coordination of Benefits Purposes.....	1005
4. Sharing PHI With Stop-Loss Insurer .....	1005
5. Exchanging PHI in Mergers and Acquisitions .....	1006
6. Sharing PHI With Interpreters, Translators, and Telecommunications Relay Services .....	1006
7. Electronic Health Records and Storage of PHI in a Health Data Warehouse .....	1008
8. Disclosures of PHI by Whistleblowers and Workforce Crime Victims .....	1011
C. <i>Disclosures to Family Members, Close Personal Friends, and Other Persons Identified by the     Individual</i> .....	1012
1. Covered Entity Must Provide Opportunity to Agree or Object .....	1012
2. Who Is a “Family Member, Close Personal Friend, or Other Person Identified by the Individual”?.....	1014
3. Uses and Disclosures for Notification or for Disaster Relief Efforts.....	1015
D. <i>Disclosures for Specific Public Policy-Related Purposes</i> .....	1015
1. Uses and Disclosures Required by Law .....	1016
2. Uses and Disclosures for Public Health Activities.....	1018
3. Disclosures About Victims of Abuse, Neglect, or Domestic Violence .....	1019
4. Uses and Disclosures for Health Care Oversight Activities .....	1019
5. Disclosures for Judicial and Administrative Proceedings.....	1020
6. Disclosures for Law-Enforcement Purposes .....	1022A
7. Uses and Disclosures About Decedents .....	1023
8. Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation Purposes .....	1023
9. Uses and Disclosures for Certain Limited Research Activities .....	1024
10. Uses and Disclosures to Avert a Serious Threat to Health or Safety .....	1024
11. Uses and Disclosures for Specialized Government Functions .....	1025
12. Disclosures Relating to Work-Related Injuries or Illness .....	1025
13. Rule Does Not Expand Government or Law-Enforcement Access to PHI .....	1025
E. <i>Uses and Disclosures Requiring Individual Authorization</i> .....	1026
1. When Is an Authorization Required?.....	1026
2. General Authorization Requirements .....	1029
3. The “Core Elements” for an Authorization .....	1030A
4. Additional Required Statements.....	1033
5. Plain Language Requirement.....	1035
6. Copy to Individual .....	1035
F. <i>Uses and Disclosures for Health Plan Underwriting Purposes</i> .....	1035
1. Authorization Required for a Provider to Disclose PHI for Underwriting Purposes .....	1035
2. Plan May Use PHI for Its Own Underwriting Purposes .....	1036
3. Plan or Issuer May Provide Summary Health Information (but Not Other PHI) to Plan Sponsor for Underwriting Purposes .....	1036
4. Entities That Are Part of an OHCA May Share PHI for Underwriting Purposes .....	1037

5.	No Minimum-Necessary Requirement for Disclosures Authorized by Individual .....	1037
G.	<i>Personal Representatives, Minors, and Spouses</i> .....	1039
1.	Individual’s Personal Representatives Must Be Treated as the Individual .....	1039
2.	Minor Dependents .....	1039
3.	Spouses, Family Members, and Close Personal Friends .....	1041
H.	<i>“Minimum-Necessary” Standard</i> .....	1042
1.	Uses of PHI .....	1042
2.	Disclosures of PHI .....	1042
3.	Requests for PHI .....	1043
4.	Special Justification Needed for “Entire Medical Record” .....	1043
5.	Flexible Standard Applies .....	1043
6.	Incidental Disclosures Permitted .....	1043
7.	Exceptions to the Minimum-Necessary Standard .....	1044
I.	<i>De-Identified Information May Be Used and Disclosed</i> .....	1044
1.	Professional Statistical Analysis .....	1044
2.	Removal of 18 Specific Identifiers .....	1044
3.	Re-Identification .....	1045
J.	<i>Limited Data Set May Be Disclosed When Data Use Agreement Is in Place</i> .....	1045
1.	What Is a “Limited Data Set”? .....	1045
2.	Agreement Must Limit Recipient’s Uses and Disclosures .....	1046
3.	Consequences If Recipient Violates Agreement .....	1046
4.	Other Privacy Requirements Apply .....	1047
5.	Use of Limited Data Sets by Health Plans and Sponsors .....	1047
K.	<i>Verification Requirement</i> .....	1047
L.	<i>Disaster Relief Efforts</i> .....	1047
1.	Permissible Disclosures .....	1047
2.	Planning for Emergencies .....	1050
<b>XXVII.</b>	<b>Core Privacy Requirement #2: Individual Rights &amp; Privacy Notice</b> .....	<b>1051</b>
A.	<i>“Designated Record Set” Is Subject to Individual Rights of Access and Amendment</i> .....	1052
B.	<i>Right to Access Own PHI</i> .....	1053
1.	Access Rights of Employees of Covered Entities or Employees Who Perform Plan Administration Functions .....	1054
2.	Timeframes for Responding to a Request for Access .....	1054
3.	Granting a Request for Access .....	1054
4.	Denying a Request for Access .....	1055
5.	Recordkeeping Requirements .....	1055
C.	<i>Right to Amend or Correct PHI That Is Inaccurate or Incomplete</i> .....	1056
1.	Amendment of PHI of Employees of Covered Entities or Employees Who Perform Plan Administration Functions .....	1056
2.	Timeframes for Responding to a Request for Amendment .....	1057
3.	Granting a Request for Amendment .....	1057
4.	Denying a Request for Amendment .....	1057
5.	Recordkeeping Requirements .....	1058

<i>D. Right to Obtain an Accounting of Disclosures</i> .....	1058
1. Timeframes for Responding to a Request for Accounting .....	1058
2. Providing the Accounting .....	1059
3. What Disclosures Must Be Included in an Accounting? .....	1060
4. Suspending the Right to Receive an Accounting Upon Request of Law Enforcement .....	1063
5. Recordkeeping Requirements .....	1063
<i>E. Right to Request Restrictions on Uses and Disclosures</i> .....	1063
1. Privacy Rule Provisions .....	1063
2. Requests to Restrict Uses and Disclosures of Social Security Numbers .....	1064
3. Right to Restrict Uses and Disclosures in Case of Self-Payment .....	1064
<i>F. Right to Request Alternate Communications</i> .....	1065
<i>G. Right to Receive Privacy Notice</i> .....	1065
1. Covered Entities Generally Must Provide Notice .....	1065
2. Special Rules for Fully Insured Group Health Plans .....	1066
3. To Whom Must the Notice Be Provided? .....	1066
4. When Must the Notice Be Provided? .....	1066
5. Method of Delivery .....	1067
6. Privacy Notice Must Meet Specific Content Requirements .....	1069
7. Drafting a Plain Language Privacy Notice .....	1072
8. Alternative Means of Communicating a Privacy Notice .....	1073
<b>XXVIII. Core Privacy Requirement #3: Administrative Requirements</b> .....	<b>1091</b>
<i>A. Privacy Official and Contact Person or Office</i> .....	1091
1. Privacy Official .....	1091
2. Contact Person or Office .....	1093
<i>B. Training</i> .....	1094
1. What Does the Term “Workforce” Mean? .....	1094
2. Training and Business Associates .....	1095
3. Designing a Training Program .....	1095
4. Types of Training Methods .....	1096
5. The Training Process .....	1096
<i>C. Safeguards (the “Mini-Security Rule”)</i> .....	1097
1. Administrative Safeguards .....	1098
2. Technical Safeguards .....	1098
3. Physical Safeguards .....	1099
<i>D. Complaint Procedure</i> .....	1100
<i>E. Sanctions</i> .....	1100A
1. The General Rule .....	1100A
2. Exception for Whistleblowers .....	1101
3. Exception for Workforce Crime Victims .....	1101
4. Exception for Individuals Who Take Certain Actions .....	1101
<i>F. Duty to Mitigate Harmful Effects of Improper Uses or Disclosures</i> .....	1102
<i>G. Prohibitions on Retaliation and Waiver of Rights</i> .....	1102
1. Refraining From Intimidating or Retaliatory Acts .....	1102
2. Prohibition on Requiring a Waiver of Rights .....	1103

H. Policies and Procedures.....	1103
1. The General Rule.....	1103
2. Changes in Law.....	1104
3. Changes to Practices Stated in Notice of Privacy Practices.....	1104
4. Other Changes.....	1104
I. Documentation.....	1105
1. Documentation Requirements.....	1105
2. Documenting PHI in a Designated Record Set.....	1106
3. ERISA’s Recordkeeping Requirements: Interaction With HIPAA’s Requirements.....	1106
4. Business Associate Contracts Should Address Recordkeeping Requirements.....	1107
5. Storage and Destruction of Records.....	1108
J. Limited Exception for Certain Fully Insured Group Health Plans.....	1108
K. Impact on Business Associates and Plan Sponsors.....	1110
1. Business Associates.....	1110
2. Plan Sponsors.....	1110
<b>XXIX. Security Requirements: General Concepts.....</b>	<b>1121</b>
A. Introduction to HIPAA’s Security Requirements.....	1121
1. Structure of the HIPAA Security Rule.....	1122
2. Basic Concept: Entities Must Implement Safeguards to Protect Electronic PHI.....	1122
3. Overview of the HIPAA Security Rule.....	1123
B. What Information Is Protected and What Entities Must Comply?.....	1124
1. The Security Rule Applies to Electronic PHI.....	1124
2. What Entities Must Comply With the HIPAA Security Rule?.....	1125
C. General Obligations Under the HIPAA Security Rule.....	1127
D. Flexibility of Approach: Written Risk Analysis Required.....	1128
1. Standards.....	1129
2. Implementation Specifications.....	1129
3. Maintenance of Security Measures.....	1131
<b>XXX. Core Security Requirements.....</b>	<b>1181</b>
A. Introduction.....	1181
B. Administrative Safeguards.....	1182
1. Standard: Security Management Process.....	1182
2. Standard: Assigned Security Responsibility.....	1186
3. Standard: Workforce Security.....	1186
4. Standard: Information Access Management.....	1188
5. Standard: Security Awareness and Training.....	1189
6. Standard: Security Incident Procedures.....	1191
7. Standard: Contingency Plan.....	1193
8. Standard: Evaluation.....	1195
9. Standard: Business Associate Contracts and Other Arrangements.....	1195
C. Physical Safeguards.....	1196
1. Standard: Facility Access Controls.....	1197
2. Standard: Workstation Use.....	1199
3. Standard: Workstation Security.....	1199

4. Standard: Device and Media Controls .....	1199
<i>D. Technical Safeguards</i> .....	1202
1. Standard: Access Control .....	1202
2. Standard: Audit Controls .....	1203
3. Standard: Integrity .....	1204
4. Standard: Person or Entity Authentication .....	1205
5. Standard: Transmission Security .....	1205
<i>E. Organizational Requirements</i> .....	1206
1. Standard: Business Associate Contracts or Other Arrangements .....	1207
2. Standard: Requirements for Group Health Plans .....	1207
<i>F. Policies, Procedures and Documentation Requirements</i> .....	1208
1. Standard: Policies and Procedures .....	1208
2. Standard: Documentation .....	1209
<b>XXXI. Mistakes Happen: Correcting HIPAA Privacy and Security Compliance Problems</b> .....	<b>1211</b>
<i>A. Overview</i> .....	1211
1. Consequences of Failing to Satisfy HIPAA’s Privacy and Security Requirements .....	1211
2. Self-Correction May Help to Minimize Consequences of Noncompliance .....	1211
3. Response Plans .....	1212
<i>B. Chart Summarizing Possible Remedial Action for HIPAA Privacy and Security Violations</i> .....	1212
<i>C. Problems Relating to Authorizations</i> .....	1215
1. The Failure to Obtain an Authorization .....	1215
2. The Authorization Is Not Written or the Authorization Form Does Meet HIPAA Requirements .....	1216
3. The Authorization Is Not Signed or Is Signed By the Wrong Person .....	1216
<i>D. Problems Relating to Notices of Privacy Practices</i> .....	1216
1. Failure to Distribute Notice of Privacy Practices to Employees .....	1216
2. Failure to Distribute Reminder of Notice of Privacy Practices Availability Every Three Years .....	1217
3. Failure by Health Insurance Company to Provide Notice of Privacy Practices .....	1217
4. Failure by TPA to Provide Notice of Privacy Practices as Promised .....	1217
5. Use or Disclosure of PHI in a Manner Not Consistent With Plan’s Notice of Privacy Practices That Otherwise Is Consistent With HIPAA Requirements .....	1217
6. Changes to Privacy Practices That Are Not Reflected in the Notice of Privacy Practices .....	1218
<i>E. Failure to Undertake Required HIPAA Privacy Measures</i> .....	1218
1. Failure to Appoint a Privacy Official or Contact Person (or Appointed Individual Has Left Employment or Changed Positions) .....	1218
2. Failure to Train Workforce .....	1219
3. Failure to Discipline Workforce Who Fail to Comply With HIPAA Privacy Rules and/or Policies and Procedures .....	1219
4. Retaliation Against Plan Participant for Exercising HIPAA Privacy Rights .....	1219
5. Failure to Adopt or Document Policies and Procedures .....	1220
6. Requiring Plan Participants to Waive HIPAA Privacy Rights as a Precondition to Participation in the Plan .....	1220
7. PHI Sent in Error by Fax, E-mail, or Regular Mail .....	1220
8. Improper Access of PHI by Workforce .....	1221
<i>F. Failure to Undertake Required HIPAA Security Measures</i> .....	1221
1. Failure to Perform Risk Assessment .....	1221

2.	Failure to Update the Risk Assessment (or the Risk Management Analysis) .....	1221
3.	Failure to Appoint or Reappoint a Security Official .....	1222
4.	Failure to Train Workforce.....	1222
G.	<i>Failure to Properly Safeguard PHI</i> .....	1223
1.	Discovery of Unauthorized Access to Secured Area .....	1223
2.	Lost or Stolen Laptop (or Other Electronic Portable Device or Media) with PHI .....	1223
3.	Shared Passwords or User IDs .....	1224
4.	Discovery That Passwords or User IDs Have Been Stolen .....	1224
H.	<i>Problems Relating to Business Associates</i> .....	1224
1.	Failure to Have a Business Associate Contract in Place.....	1224
2.	The Business Associate Contract Contains the Privacy Rule Requirements But Not the Security Rule Requirements .....	1225
<b>XXXII.</b>	<b>Electronic Transactions and Code Sets .....</b>	<b>1231</b>
A.	<i>Introduction to HIPAA’s Electronic Transaction Requirements</i> .....	1231
B.	<i>Implementation Date and Enforcement Policy</i> .....	1234
1.	Implementation Date and Extension.....	1234
2.	CMS Enforcement .....	1235
C.	<i>What Do the EDI Standards Require?</i> .....	1236
1.	General Requirements.....	1236
2.	Application of EDI Standards to Health Care Providers .....	1237
3.	Application of EDI Standards to Health Plans .....	1237
4.	Application of EDI Requirements to Health Care Clearinghouses .....	1239
D.	<i>What Transactions and Transmissions Are Covered?</i> .....	1240
1.	Flowchart: Is This Transaction Subject to the EDI Standards? .....	1241
2.	Covered Transactions Defined.....	1241
3.	Do We Have the Correct Type of Sender and Recipient for the Transaction Involved? .....	1244
4.	Internal Transactions .....	1245
5.	Transactions Conducted by a Business Associate.....	1246
6.	What Electronic Transmissions Trigger HIPAA’s Requirements? .....	1246
E.	<i>Standards Applicable to Covered Transactions</i> .....	1247
F.	<i>What Exceptions Apply to HIPAA’s EDI Requirements?</i> .....	1251
1.	Direct Data Entry .....	1251
2.	Paper Transactions .....	1251
3.	Transactions by Noncovered Entities .....	1251
4.	Group Health Plan Exclusion for Self-Administered Plans With Fewer Than 50 Participants.....	1252
5.	Certain Excepted Benefits.....	1252
6.	Workers’ Compensation.....	1253
7.	Health Plan Sponsors .....	1253
8.	Other Exceptions .....	1253
G.	<i>Modifications</i> .....	1253
H.	<i>Code Sets</i> .....	1253
I.	<i>Operating Rules</i> .....	1255
1.	What Are Operating Rules?.....	1255
2.	Who Creates Operating Rules? .....	1255

3. Implementation Timeline for Operating Rules .....	1256
4. Operating Rules Adopted.....	1256
5. How Do the Operating Rules Affect Employer-Sponsored Health Plans and Their Business Associates?.....	1257
<i>J. Unique Health Identifiers.....</i>	<i>1258</i>
1. Individual Identifiers .....	1258
2. Health Plan Identifier.....	1258
3. Employer Identifiers .....	1259
4. National Provider Identifier.....	1259
<i>K. Action Items for Health Plan Sponsors .....</i>	<i>1262</i>
<b>XXXIII. [Reserved] .....</b>	<b>1311</b>
<b>XXXIV. Other Privacy Laws .....</b>	<b>1311</b>
<i>A. Overview .....</i>	<i>1311</i>
<i>B. Gramm-Leach-Bliley Act .....</i>	<i>1311</i>
1. State Implementation .....	1311
2. Application of GLB to Insurers and TPAs .....	1312
3. Interaction of GLB With the HIPAA Privacy Requirements.....	1312
4. TPA Notice Requirements .....	1312
<i>C. Americans with Disabilities Act (ADA).....</i>	<i>1313</i>
<i>D. Federal Trade Commission Act.....</i>	<i>1314</i>
<i>E. Federal Substance Abuse Rules.....</i>	<i>1314</i>
<i>F. Federal Computer Fraud and Abuse Act .....</i>	<i>1317</i>
1. The CFAA.....	1317
2. The CFAA and HIPAA .....	1317
<i>G. Federal Constitutional Rights of Privacy for Medical Records.....</i>	<i>1319</i>
<i>H. Federal Identity Theft Prevention Program (Red Flags Rule).....</i>	<i>1320</i>
1. Overview of the Red Flags Rule.....	1320
2. What Entities Must Comply With the Red Flags Rule? .....	1321

**PART 5 OF 5**

**ADDITIONAL HIPAA RULES AFFECTING GROUP HEALTH PLANS**

<b>XXXV. Fraud and Abuse Rules Apply to Health Plans, Providers, and Individuals.....</b>	<b>1341</b>
<i>A. Prohibitions Against Inducements for Referrals (Anti-Kickback Laws).....</i>	<i>1341</i>
1. General Prohibitions .....	1341
2. Exceptions and Safe Harbors in General .....	1342
3. The Safe Harbors for Electronic Health Records and Electronic Prescribing.....	1342
<i>B. Prohibition Against Inducements to Beneficiaries.....</i>	<i>1343</i>
<i>C. Federal Health Care Offenses .....</i>	<i>1344</i>
<i>D. Fraud &amp; Abuse Data Collection Program .....</i>	<i>1346</i>
1. Adverse Actions Will Be Compiled .....	1346
2. Health Plans Must Report to Data Bank.....	1347
3. Reporting Deadlines .....	1348
4. Only Eligible Entities May Access Information.....	1348
5. Confidentiality of HIPDB Information .....	1348

6. Fees for Queries.....	1348
7. Penalty for Failure to Report .....	1348
<b>XXXVI. Multiple Employer Welfare Arrangements (MEWAs) .....</b>	<b>1381</b>
A. Overview .....	1381
1. MEWAs Provide Welfare Benefits to Employees of Two or More Employers .....	1382
2. Does HIPAA Apply at the MEWA Level, the Health Plan/Employer Level, or Both? .....	1382
B. When Is a MEWA a Group Health Plan and Why Does it Matter?.....	1383
1. Three Different Definitions of “Group Health Plan” Are Used Under HIPAA .....	1383
2. Most MEWAs Are Group Health Plans Under the Code’s Definition.....	1383
3. Some MEWAs Are Group Health Plans Under the ERISA and PHSA Definitions.....	1384
4. HIPAA’s Administrative Simplification Provisions Apply to Health Plans and ERISA Group Health Plans.....	1385
C. Portability, Special Enrollment, and Nondiscrimination Rules Apply to MEWAs That Are Group Health Plans.....	1386
D. Special Renewability Rules Apply to MEWAs That Are Group Health Plans .....	1386
E. HIPAA’s Administrative Simplification Provisions Apply to All MEWAs .....	1387
1. Health Plans Must Comply with HIPAA’s Administrative Simplification Provisions .....	1387
2. What’s the Effect on Privacy, Security, and EDI Compliance if a MEWA Is Not a Group Health Plan? .....	1387
3. What’s the Effect on Privacy, Security, and EDI Compliance If a MEWA Is a Group Health Plan? .....	1387
F. MEWAs Raise Issues Under ERISA .....	1388
1. Special ERISA Preemption Rules Subject All MEWAs to State Insurance Laws .....	1388
2. Form M-1: Annual Report for MEWAs Providing Health Benefits.....	1389
3. Other ERISA Compliance Issues.....	1389
<b>Index .....</b>	<b>behind the Index and Glossary Tab</b>
<b>Glossary of Terms .....</b>	<b>behind the Index and Glossary Tab</b>

## Appendix Tabs

<b>Tab 1: Portability: Federal Statutes</b>	<b>Tab 7: Privacy &amp; Security: Gov’t Forms</b>
<b>Tab 2: Portability: Federal Regulations</b>	<b>Tab 8: Privacy &amp; Security: Other Guidance</b>
<b>Tab 3: Portability: Government Forms</b>	<b>Tab 9: Legislative History</b>
<b>Tab 4: Portability: Other Federal Guidance</b>	<b>Tab 10: Sample Documents</b>
<b>Tab 5: Privacy &amp; Security: Statutes</b>	<b>Tab 11: Miscellaneous</b>
<b>Tab 6: Privacy &amp; Security: Regulations</b>	