

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>PART 1 OF 5 INTRODUCTION</p>

I. Overview of This Manual	1
A. <i>What This Manual Covers</i>	1
1. Part 1—Introduction	1
2. Part 2—HIPAA’s Portability, Special Enrollment, and Nondiscrimination Rules	1
3. Part 3—Insurance Market Rules	1
4. Part 4—Administrative Simplification	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
II. HIPAA Portability, Privacy & Security: A Short Course	31
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	35
5. Plan or Issuer Must Issue Certificate of Creditable Coverage	35
6. New Plan Must Review Information and Issue PCE Determination Notice	36
F. <i>Special Enrollment Rights</i>	36
1. Loss of Other Coverage	37
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	40
5.	Discrimination in Favor of Individuals With Adverse Health Conditions	40
6.	The Genetic Information Nondiscrimination Act (GINA).....	40
H.	<i>HIPAA’s Portability Rules in Practice—Amy’s & Bob’s Stories</i>	40
1.	Amy and Bob Start Work.....	40
2.	Amy and Bob Get Married (But Not to Each Other)	41
3.	Amy’s Husband Loses Health Coverage	41
4.	Bob Has a Child.....	42
5.	Amy and Bob Are Laid Off.....	42
I.	<i>Compliance Checklist for HIPAA’s Portability Requirements</i>	42
1.	Plan Design/Administrative Issues.....	42
2.	Plan Document	42
3.	Summary Plan Descriptions (SPDs) and Other Participant Communications	43
4.	Procedures.....	43
5.	Participant Planning Considerations.....	44
J.	<i>HIPAA’s Insurance Market Rules</i>	44
K.	<i>Overview of HIPAA’s Administrative Simplification Requirements</i>	44
1.	What Entities Must Comply?.....	45
2.	What Information Is Covered?.....	45
L.	<i>How the Privacy & Security Rules Affect Group Health Plans and Plan Sponsors</i>	46
1.	How Do the Privacy & Security Rules Apply to Group Health Plan Sponsors?	46
2.	Sharing Group Health Plan PHI With the Plan Sponsor.....	47
3.	Special Requirements for Business Associates	48
M.	<i>Core Privacy Requirements</i>	48
1.	Core Requirement #1: Use and Disclosure Rules	48
2.	Core Requirement #2: Individual Rights & Privacy Notice	49
3.	Core Requirement #3: Administrative Requirements	50
N.	<i>HIPAA Privacy Rule in Practice: Three Plan Sponsors</i>	51
1.	Fully Insured Group Health Plan: Plan and Employer Are “Hands-Off” PHI	51
2.	Fully Insured Group Health Plan: Plan and Sponsor Are “Hands-On” PHI.....	51
3.	Self-Funded Group Health Plans and Their Sponsors.....	52
O.	<i>Core Security Requirements</i>	52
P.	<i>EDI Standards</i>	53
Q.	<i>Privacy and Security Compliance Checklist</i>	54
1.	General Health Plan Activities	54
2.	Determine Privacy Requirements for Each Health Plan.....	54
3.	Determine Security Requirements for Each Health Plan	54
4.	Other HIPAA Compliance Concerns.....	55

R. Conclusion	55
III. [Reserved].....	111

PART 2 OF 5

HIPAA'S PORTABILITY, SPECIAL ENROLLMENT AND NONDISCRIMINATION RULES

IV. Portability: Sources of Governing Law	111
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
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	112
4. Jointly Issued Final Regulations	113
5. Jointly Issued Final Regulations on Nondiscrimination and Wellness Programs	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	113
1. The General Rule With Regard to Laws Affecting HIPAA's PCE and Special Enrollment Provisions	113
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?	114
3. Scope of HIPAA Preemption With Regard to Nondiscrimination Requirements	116
4. Which State's Laws Apply?	116
V. How Are HIPAA's Portability Requirements Enforced?	151
A. Both Employers and Issuers Are Responsible for HIPAA Portability Compliance	151
1. What Is a HIPAA Group Health Plan?	151
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 Penalties for HIPAA Violations	153
D. HIPAA Enforcement by the DOL	153
1. Overview of the DOL's Enforcement Authority	153
2. DOL Audits of Health Plans	154
E. HIPAA Enforcement by the HHS	154
1. Overview of CMS Enforcement Authority	154
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	156
1. DOL, HHS, and IRS May Impose Penalties	156
2. Amount of Penalty	157
3. Exceptions and Limitations	157

G. Private Lawsuits	157
VI. What Plans Are Subject to HIPAA’s Portability Requirements?	191
A. Overview	191
B. Table Summarizing Whether Particular Plans and Benefits Are Subject to HIPAA Portability	192
C. What Is a HIPAA Group Health Plan for Portability Purposes?.....	193
1. Group Health Plan Definitions Applicable Under HIPAA Portability.....	194
2. Under ERISA and PHSA Definitions, a Group Health Plan Must Be an ERISA Employee Welfare Benefit Plan	194
D. Individual Health Insurance Policies Can Be Subject to HIPAA’s Group Rules	195
1. Common Individual Policy Arrangements.....	196
2. When Are Individual Policy Arrangements Subject to HIPAA Portability?.....	196
3. Consequences If Individual Policies Are Subject to HIPAA Portability	198
E. Stop-Loss Coverage Probably Is Not Subject to HIPAA’s Portability Rules	198A
F. Exception for Plans Covering Fewer Than Two Current Employees	198A
G. Plans Covering Partners, Sole Proprietors, and Independent Contractors Must Comply	199
H. Medicare, Certain Other Governmental Programs, and Tribal Plans Must Comply With Certification Requirements Only	199
I. Self-Funded Non-Federal Governmental Plans May Opt Out	199
J. Church Plans Must Comply Subject to Limited Exception.....	201
K. Retiree Medical Plans May Be Exempt From HIPAA Portability	201
L. Certain Health Flexible Spending Accounts Are Excepted Benefits.....	202
1. Two Conditions Must Be Met for a Health FSA to Be an Excepted Benefit.....	203
2. When Is the HIPAA Maximum Benefit Condition Met?.....	204
3. When Is the HIPAA Availability Condition Met?	205
4. Becoming a HIPAA Excepted Benefit by Plan Design	206
M. Health Savings Accounts (HSAs) and Archer Medical Savings Accounts (MSAs).....	207
1. HSAs and Archer MSAs as Group Health Plans	207
2. HSAs and Archer MSAs as Exempt Plans	208
N. Health Reimbursement Arrangements (HRAs).....	208
O. Blanket Exception for Certain Benefit Types	208
P. Exception for Limited-Scope Benefits (Including Dental and Vision)	209
1. Dental/Vision Benefits Must First Be Limited in Scope for Exception to Apply	209
2. Limited Benefits Offered Under a Separate Policy	209
3. Limited Benefits That Are Not Integral to a Plan	210
Q. Exception for Certain Independent, Noncoordinated Benefits.....	211
R. Exception for Certain Supplemental Benefits.....	212
1. Medicare and TRICARE Supplemental Insurance Are Clearly Excluded.....	212
2. The Exception for Other Similar Supplemental Insurance Coverage: Safe Harbor Rules	212
3. Employee Assistance Programs	214
4. Retiree Medical Programs.....	214
S. Wellness Programs.....	215
1. Stand-Alone Wellness Programs	215
2. Wellness Programs That Relate to Group Health Plans	215
T. Employee Discount Programs.....	215

VII. HIPAA’s Restrictions on Preexisting Condition Exclusions	241
A. <i>Overview—Preexisting Condition Exclusions, Creditable Coverage, and Other Limitations</i>	241
B. <i>Flowchart: Operation of HIPAA’s PCE Provisions</i>	243
C. <i>HIPAA’s Limitations on Preexisting Condition Exclusions</i>	244
1. <i>What Is a Preexisting Condition?.....</i>	244
2. <i>What Preexisting Conditions May Be Excluded From Group Health Plan Coverage?.....</i>	244
3. <i>Maximum Duration: The 12-Month Look-Forward Rule (18 Months for Late Enrollees).....</i>	247
4. <i>Enrollment Date Triggers the 6-Month Look-Back and 12-Month Look-Forward Periods— Important to Take into Account the “Waiting Period”.....</i>	248
5. <i>Using Creditable Coverage to Offset the Maximum Duration.....</i>	250
6. <i>Affiliation Periods.....</i>	250
D. <i>Applying the PCE</i>	251
1. <i>Medical Advice, Diagnosis, Care, or Treatment Must Have Been Recommended or Received During the 6-Month Look-Back Period.....</i>	251
2. <i>Subsequent Sickness or Injury Must Be Directly Attributable to the Preexisting Condition.....</i>	255
3. <i>Provider of Care Must Be Licensed.....</i>	255
4. <i>Conditions First Discovered During a Waiting Period Are Not Preexisting Conditions</i>	256
5. <i>Does a Benefit-Specific Waiting Period Operate as a PCE?</i>	256
E. <i>Illustrations of the 6-Month Look-Back and 12-Month Look-Forward Rules.....</i>	257
F. <i>The Creditable Coverage Rules.....</i>	257
1. <i>Group Health Plan Coverage</i>	258
2. <i>Health Insurance Coverage</i>	259
3. <i>Medicaid and Other Coverage</i>	259
4. <i>Excepted Benefits Do Not Count as Creditable Coverage</i>	260
G. <i>Specifics of the PCE 12-Month Look-Forward Rule With Offsets for Creditable Coverage</i>	261
1. <i>Overview</i>	261
2. <i>Coverage Before a 63-Day Break Generally Is Not Counted as Creditable Coverage.....</i>	261
3. <i>Creditable Coverage Before a 63-Day Break Is Counted for Certain Individuals Under the Trade Act of 2002</i>	263
4. <i>Waiting Periods Generally Do Not Count as a Break in Coverage</i>	265
5. <i>Impact of Overlap Between Waiting Period and Creditable Coverage</i>	266
6. <i>Illustrations of How the Creditable Coverage Rules Work</i>	267
7. <i>Options for Determining Creditable Coverage</i>	267
8. <i>HMO Affiliation Period as Alternative</i>	269
H. <i>Notice Requirements to Impose a PCE</i>	270
1. <i>The Initial (General) PCE Notice Requirement.....</i>	270
2. <i>Individual PCE Determination Notice</i>	273
I. <i>Application of PCEs to Alternate Recipients Under QMCSOs.....</i>	275
1. <i>May a PCE Be Applied to an Alternate Recipient?.....</i>	275
2. <i>If the Plan Applies a PCE, What is the Length of the Exclusionary Period?.....</i>	276
J. <i>Current Plan Designs and Strategies.....</i>	276
VIII. HIPAA Certificate of Creditable Coverage: Obligation to Furnish	291
A. <i>Overview</i>	291
B. <i>Who Must Furnish the HIPAA Certificate?</i>	291
1. <i>Self-Funded Plans</i>	292

2.	Insured Plans.....	292
3.	Employee Changing Coverage Options Under a Single Plan	293
4.	Employer Changes Insurance Carriers	294
C.	<i>To Whom Must a HIPAA Certificate Be Issued?</i>	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.	<i>What Triggers the Requirement to Issue a HIPAA Certificate?</i>	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?.....	297
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?.....	298
8.	HIPAA Certificates and FMLA Leave.....	298
9.	Caution for Employers With Multiple Plans	299
E.	<i>Content of the HIPAA Certificate</i>	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.	<i>Method of Delivery of HIPAA Certificate</i>	302
1.	First-Class Mail to Last-Known Address.....	302
2.	Electronic Disclosure of HIPAA Certificate	302
G.	<i>Procedures for Requesting Certificates</i>	303
H.	<i>HIPAA Certificate Obligation: Mergers & Acquisitions</i>	304
1.	Stock Acquisition.....	304
2.	Asset Acquisition	304
3.	“COBRA Plus” Rules of Thumb for Merger & Acquisition Certifications	304
IX.	HIPAA Certificate of Creditable Coverage: Obligations Upon Receipt	331
A.	<i>Overview</i>	331
B.	<i>Individual Notice of Determination of Creditable Coverage and Remaining PCE Period</i>	331
1.	General Requirements.....	331
2.	Electronic Delivery of Notice	332
C.	<i>When Should a HIPAA Certificate Be Processed?</i>	333
D.	<i>How to Handle Claims or Inquiries Received Before a Determination Is Made</i>	334
E.	<i>Modifying an Individual Notice</i>	334
F.	<i>Consequences of Relying Upon an Erroneous or Fraudulent Certificate</i>	335
G.	<i>Limiting Exposure Relating to the Receipt of a HIPAA Certificate</i>	335
H.	<i>Demonstrating Creditable Coverage Without a HIPAA Certificate</i>	336

X. Special Enrollment Rights	371
A. <i>Overview</i>	371
B. <i>Individuals Who Lose Coverage</i>	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. <i>Individuals Who Become Eligible for State Premium Assistance Subsidy</i>	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. <i>Acquisition of a New Dependent</i>	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. <i>Who Qualifies as a Dependent for Special Enrollment?</i>	391
F. <i>Disclosure Requirements for Special Enrollment Rights</i>	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. <i>COBRA Qualified Beneficiaries Have Special Enrollment Rights</i>	397
1. Qualified Beneficiaries on COBRA May Add Family Members Under the Special Enrollment Rules	397
2. But Qualified Beneficiaries Must Be Receiving COBRA Coverage to Have Special Enrollment Rights	398
H. <i>Cafeteria Plan Issues</i>	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	400
5. Prospective Election Changes Outside of HIPAA's Minimum Special Enrollment Window	401
6. Loss of Medicare, Medicaid or SCHIP Entitlement; Eligibility for Medicaid or SCHIP	401
I. <i>Retirees and Special Enrollment</i>	402
1. Retiree Medical Plans, Long-Term Disability Continuees, and Survivors	402
J. <i>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
XI.	Nondiscrimination Rules for Group Health Plans.....	421
A.	<i>Overview and Sources of Nondiscrimination Rules.....</i>	<i>421</i>
B.	<i>What Is a Health Status-Related Factor?.....</i>	<i>421</i>
C.	<i>Nondiscrimination Rules for Eligibility and Benefits.....</i>	<i>422</i>
1.	Nondiscrimination Rules for Eligibility—In General.....	423
2.	Some PCE Limitations and Exclusions Are Permissible.....	424
3.	Eligibility Rules and Benefit Restrictions That Apply to All Similarly Situated Individuals Are Permissible.....	425
4.	HRAs and HIPAA Nondiscrimination Rules.....	427
5.	Benefit-Specific Waiting Periods Raise Additional Issues.....	428
6.	Special Rules Apply to Source-of-Injury Exclusions or Limitations.....	429
D.	<i>No Discrimination in Individual Premiums or Contributions.....</i>	<i>430</i>
E.	<i>Defining Groups of “Similarly Situated Individuals”.....</i>	<i>431</i>
1.	Groups of Participants Based on Bona Fide Employment Classifications.....	432
2.	Differences Permitted Between Participants and Beneficiaries.....	432
3.	Differences Permitted Among Beneficiaries.....	432
4.	Differences Directed at Specific Individuals Not Allowed.....	433
F.	<i>Nonconfinement and Normal Life Activity Provisions Not Allowed.....</i>	<i>433</i>
G.	<i>Traditional Actively-at-Work and Continuous-Service Clauses Not Allowed.....</i>	<i>434</i>
1.	Traditional Actively-at-Work or Continuous-Service Requirements Violate HIPAA.....	435
2.	Limited Actively-at-Work or Continuous-Service Provision Permissible.....	435
3.	First-Day-of-Work Rule Permissible.....	436
4.	Plan May Terminate Coverage When Eligibility Criteria Are No Longer Satisfied.....	436
5.	Making Sense of the Actively-at-Work Prohibition.....	437
H.	<i>Plans May Discriminate in Favor of Individuals Who Have Adverse Health Conditions.....</i>	<i>438</i>
I.	<i>No Discrimination on the Basis of Genetic Information.....</i>	<i>439</i>
1.	What Is “Genetic Information”?.....	439
2.	What Is a “Genetic Test”?.....	439
3.	Who Is a “Family Member”?.....	439
4.	Group Health Premiums or Contributions.....	440
5.	Plans and Issuers May Not Request or Require Genetic Testing.....	440
6.	Employers Also May Not Request or Require Genetic Information.....	441
7.	Genetic Information May Not Be Used for Underwriting.....	442
J.	<i>Wellness Programs Must Meet Specific Requirements.....</i>	<i>443</i>
1.	What Is a Wellness Program?.....	443
2.	Health Risk Assessments.....	444
3.	Participation-Only Programs: Wellness Programs That Do Not Reward Participants Based on a Health Factor.....	444
4.	Standard-Based Programs: Requirements for Wellness Programs That Provide Rewards Based on a Health Factor.....	444
5.	Examples of Standard-Based Wellness Programs That Meet HIPAA’s Requirements.....	448
6.	Examples of Standard-Based Wellness Programs That Do Not Meet HIPAA’s Requirements.....	449

7. Wellness Program Checklist.....	450
8. ADA Considerations.....	451
9. Cafeteria Plan Issues.....	452
K. <i>Steps to Reduce Adverse Selection</i>	452
L. <i>Transition Rule for Governmental Plans Opting Into HIPAA Coverage</i>	453
M. <i>Limited Exception for Certain Grandfathered Church Plans</i>	453
XII. [Reserved].....	501
XIII. HIPAA in the SPD.....	501
A. <i>ERISA Requires Group Health Plans to Furnish SPD</i>	501
B. <i>ERISA Requires Disclosures About Benefits and Loss of Benefits</i>	501
C. <i>Disclosures About HIPAA Portability Requirements</i>	502
1. Preexisting Condition Exclusions (PCEs).....	502
2. Special Enrollment Periods.....	503
3. Nondiscrimination Rules.....	504
4. Claims Procedures.....	504
5. Disclosure of Interaction Between HIPAA and COBRA.....	504
D. <i>Disclosures About HIPAA Privacy</i>	505
E. <i>Disclosures About Other Federal Mandates</i>	505
XIV. HIPAA Portability Checklists.....	541
A. <i>Overview</i>	541
B. <i>Plan Design/Administrative Issues</i>	541
C. <i>Plan Document</i>	542
1. Preexisting Condition Exclusions (PCEs).....	542
2. Special Enrollment Periods.....	542
3. Nondiscrimination Rules.....	542
4. Claims Procedures.....	543
D. <i>Summary Plan Descriptions (SPDs)</i>	543
E. <i>Paperwork That Goes to Participants</i>	543
F. <i>Participant Planning Considerations</i>	544
XV. Mistakes Happen: Correcting HIPAA Portability and Nondiscrimination Compliance Problems.....	581
A. <i>Overview</i>	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. <i>Chart Summarizing Possible Remedial Action for HIPAA Portability and Nondiscrimination Violations</i>	582
C. <i>Correcting PCE Limitation and Notice Violations</i>	583
1. Failure to Provide Initial Notice of PCE Limitation.....	583
2. Incorrect Determination That Specific Individual or Condition Was Subject to PCE Limitation.....	583
3. Incorrect Determination of Duration of PCE Limitation Period.....	584
D. <i>Correcting HIPAA Certificate Violations</i>	584
1. The Requirement.....	584
2. The Correction.....	585

<i>E. Correcting HIPAA Special Enrollment Violations</i>	585
1. The Requirement	585
2. Failure to Provide Notice: The Correction	585
3. Failure to Allow Required Special Enrollment: The Correction	585
<i>F. Correcting HIPAA Nondiscrimination Violations</i>	585
1. The Requirement	585
2. Eligibility Denied: The Correction	585
3. Impermissible Contribution Rate or Benefits Exclusion: The Correction	586

PART 3 OF 5
INSURANCE MARKET RULES

XVI.-XVII. [Reserved]	691
XVIII. Group Insurance Market Requirements	693
<i>A. Overview—Group Insurance Market Rules</i>	693
1. What Is a Health Insurance Issuer That Is Subject to the Group Insurance Rules?	693
2. When Is An Issuer Offering Insurance in the Small Group Market?	694
3. Potential Applicability of Group Market Rules to Individual Coverage	697
<i>B. Guaranteed-Renewability Rules Applicable to All Group Insurance</i>	698
1. Product Withdrawal Requirements	698
2. Market Exit Requirements	699
<i>C. Guaranteed-Availability Rules Applicable to Small Group Market</i>	699
1. Issuers Must Accept Every Small Employer and Make All Actively Marketed Products Available	700
2. Issuers Must Accept Every Eligible Individual When First Eligible	701
3. Effect of HIPAA’s Small Group Requirements on State-Law Group Participation Rules	702
<i>D. Special Rules Applicable to “Bona Fide Association” Plans</i>	707
1. Associations and “Bona Fide Associations”	707
2. Restrictions on Membership Not Permitted	707
3. Is Coverage That Is Offered Through an Association Group or Individual Coverage?	708
4. Guaranteed Availability and Coverage Offered to Members of a Bona Fide Association	708
5. Guaranteed Renewability and Coverage Offered to Members of a Bona Fide Association	708
<i>E. Renewability Rules Apply to Multiemployer Plans That Are Group Health Plans</i>	709
<i>F. Preemption Issues</i>	710
XIX. HIPAA’s Individual Insurance Market Rules	731
<i>A. Overview</i>	731
<i>B. What Is a Health Insurance Issuer Offering Coverage in the Individual Market?</i>	731
1. Individual Market Defined	732
2. Conversion Coverage	732
3. Coverage Offered Through Associations	732
4. Individual Policies Offered Through the Employer’s Workplace	732
<i>C. Excepted Benefits</i>	732
1. Blanket Exception for Certain Benefit Types	733
2. Limited-Scope Benefits (Including Dental and Vision)	733
3. Certain Independent, Noncoordinated Benefits	733

4. Medicare and CHAMPUS Supplemental Insurance.....	733
5. Other Similar Supplemental Insurance Coverage.....	733
<i>D. Guaranteed Availability Under Federal Fallback Provisions</i>	734
1. Definition of an Eligible Individual.....	734
2. Insurer Must Use Reasonable Diligence to Determine Whether Applicant Is an Eligible Individual.....	738
3. Insurer Must Not Prevent Seamless Coverage.....	739
4. Medical Questionnaires May Be Used for Limited Purposes	739
5. Issuer May Limit Coverage to Two Policies	740
<i>E. Federal Requirements Do Not Apply in a State That Has Implemented an Alternative Mechanism</i>	741
<i>F. Guaranteed Renewability</i>	742
1. All Individuals Purchasing Coverage in the Individual Market Are Entitled to Renew	742
2. Coverage Provided Through Association Plans	742
3. Nonrenewal of Coverage Permitted in Limited Circumstances	742
<i>G. Certificate of Creditable Coverage</i>	744
<i>H. No Discrimination on the Basis of Genetic Information</i>	744
1. Eligibility, Premiums, and PCEs	744
2. Genetic Testing	745
3. Underwriting.....	745
4. What Is “Genetic Information”?.....	745
XX. [Reserved]	751

PART 4 OF 5 ADMINISTRATIVE SIMPLIFICATION
--

XXI. Privacy, Security, and EDI: Sources of Law and Enforcement	751
<i>A. Introduction</i>	751
<i>B. Statutes</i>	752
1. Privacy	752
2. Security	753
3. Standard Transactions, Code Sets, and Unique Health Identifiers.....	754
<i>C. Regulations and Compliance Dates</i>	754
1. Chart: Regulations and Compliance Dates.....	755
2. Compliance Dates One Year Later for “Small Health Plans”	756
3. Privacy Regulations.....	756
4. Security Regulations.....	756
5. Transactions and Code Sets Regulations	757
6. Other Regulations	758
7. Other Guidance	759
<i>D. Enforcement</i>	759
1. Complaints and Compliance Reviews	759
2. Civil Money Penalties.....	766
3. CMS Recordkeeping for HIPAA Investigations	773
4. HIPAA Compliance Audits by HHS	773
5. Criminal Penalties.....	775

6.	No Specific Private Cause of Action in the Statute or Regulations	777
7.	Plan Document May Result in ERISA Fiduciary Liability for Noncompliance With Administrative Simplification Provisions	778
8.	HIPAA Insurance.....	779
<i>E.</i>	<i>Preemption of State Laws Affecting Administrative Simplification</i>	780
1.	Subject to Several Significant Exceptions, HIPAA Preempts Contrary State Laws	780
2.	Impact of ERISA Preemption for Health Plans Subject to ERISA	787
3.	Gramm-Leach-Bliley Privacy Laws Are Subject to HIPAA Preemption Analysis	788
4.	Other Federal Privacy Laws Generally Are Not Affected by HIPAA	789
XXII.	Privacy, Security, and EDI: What Information Is Protected and What Entities Must Comply?	801
<i>A.</i>	<i>What Information Is Protected?</i>	801
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
<i>B.</i>	<i>Covered Entities Must Comply</i>	814
1.	Health Plan	814
2.	Health Care Clearinghouse.....	814
3.	Health Care Provider That Conducts Certain Transactions Electronically	815
4.	Endorsed Sponsors of the Medicare Prescription Drug Discount Card.....	816
5.	Are Indian Tribal Governments and Entities That Are Covered by Tribal Law Subject to the HIPAA Administrative Simplification Requirements?	817
6.	Who Is Responsible for the Privacy of Medical Records When a Group Health Plan Ceases to Exist?	818
<i>C.</i>	<i>What Is a “Health Plan”?</i>	821
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
<i>D.</i>	<i>Special Rules for Certain Types of Covered Entities</i>	837
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
XXIII.	How the Privacy and Security Rules Affect Group Health Plans and Plan Sponsors	871
<i>A.</i>	<i>Introduction to HIPAA’s Privacy and Security Requirements</i>	871
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
<i>B. Quick Reference of Common Employer Issues That May Be Affected by the HIPAA Privacy Rule</i>	<i>874</i>
<i>C. Sharing PHI and Electronic PHI With Plan Sponsors</i>	<i>887</i>
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
<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
K.	<i>HIPAA Privacy and Security and the Medicare Part D Retiree Drug Subsidy</i>	932
L.	<i>HIPAA Privacy and Collective Bargaining.....</i>	933
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
M.	<i>HIPAA Privacy and Security Issues for Electronic Payment Card Programs Under Health FSAs and HRAs.....</i>	934
1.	What Types of Electronic Payment Card Transactions Are Allowed by the IRS?	935
2.	Looking Behind the Plastic: The Parties in Card Transaction	936
3.	Application of HIPAA Privacy and Security Requirements to an IIAS	938
4.	Application of HIPAA Privacy and Security Requirements to Electronic Payment Card Transactions at Merchants and Service Providers With Health Care-Related MCCs.....	940
N.	<i>HIPAA Privacy and Security Issues for Employees Working From Home and Gaining Remote Access to PHI.....</i>	940
1.	Step One: Employers Must Document Clear Business Need for Remote Access	940A
2.	Step Two: Perform Risk Analysis and Risk Management	940A
3.	Step Three: Remote Access Should be Added to Existing HIPAA Policies and Procedures	940D
4.	Step Four: Training	940E
5.	Step 5: Addressing Security Incidents and Noncompliance	940E
6.	Step 6: Monitoring	940E
XXIV.	Business Associate Contracts	941
A.	<i>What Is a Business Associate?.....</i>	943
1.	HIPAA’s Definition of Business Associate.....	943
2.	Certain Service Providers Are Business Associates	944
3.	Service Providers That Might Be Business Associates	946
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>	957
1.	Required Terms of a Business Associate Contract.....	957
2.	Fewer Requirements for Business Associates Than for Covered Entities	961
3.	Violations of Privacy and Security Provisions by Business Associate	962
4.	Business Associates Must Comply With EDI Standards.....	963
5.	Additional Items Included by HHS in Sample Business Associate Contract Provisions.....	964
6.	Business Associate Contract Compliance Dates	965
C.	<i>Agents and Subcontractors of a Business Associate.....</i>	967
1.	Must a Business Associate Monitor Its Agents or Subcontractors?	968
2.	Must a Business Associate Obtain the Return of PHI From Its Agents or Subcontractors?.....	968
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. HIPAA Audits.....	980
F. Contracting With Business Associates: An Overview of ERISA Issues	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. Attorneys as Business Associates	983
1. When Are Attorneys Business Associates?.....	983
2. Special Business Associate Contract Issues for Attorneys.....	984
H. Transferring PHI Outside the United States	990
I. Roadmap for Business Associates	990
XXV. [Reserved]	999
XXVI. Core Privacy Requirement #1: Use and Disclosure Rules.....	999
A. Introduction to Use and Disclosure Rules.....	999
B. Uses and Disclosures for Treatment, Payment, and Health Care Operations	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. Disclosures to Family Members, Close Personal Friends, and Other Persons Identified by the Individual.....	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. Disclosures for Specific Public Policy-Related Purposes	1015
1. Uses and Disclosures Required by Law	1016
2. Uses and Disclosures for Public Health Activities.....	1017
3. Disclosures About Victims of Abuse, Neglect, or Domestic Violence	1018
4. Uses and Disclosures for Health Care Oversight Activities	1019
5. Disclosures for Judicial and Administrative Proceedings.....	1019
6. Disclosures for Law-Enforcement Purposes	1022
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

<i>E. 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	1030
4. Additional Required Statements	1033
5. Plain Language Requirement.....	1035
6. Copy to Individual	1035
<i>F. 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
<i>G. 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
<i>H. “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
<i>J. 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
<i>K. Verification Requirement</i>	1047
<i>L. Disaster Relief Efforts</i>	1047
1. Permissible Disclosures.....	1047
2. Planning for Emergencies	1050

XXVII. Core Privacy Requirement #2: Individual Rights & Privacy Notice	1051
A. <i>“Designated Record Set” Is Subject to Individual Rights of Access and Amendment</i>	<i>1051</i>
B. <i>Right to Access Own PHI</i>	<i>1053</i>
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>	<i>1056</i>
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
D. <i>Right to Obtain an Accounting of Disclosures.....</i>	<i>1058</i>
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
E. <i>Right to Request Restrictions on Uses and Disclosures</i>	<i>1063</i>
1. Privacy Rule Provisions	1063
2. Requests to Restrict Uses and Disclosures of Social Security Numbers	1064
F. <i>Right to Request Alternate Communications.....</i>	<i>1064</i>
G. <i>Right to Receive Privacy Notice.....</i>	<i>1065</i>
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 Notices.....	1072
8. Alternative Means Of Communicating a Privacy Notice	1072
XXVIII. Core Privacy Requirement #3: Administrative Requirements	1091
A. <i>Privacy Official and Contact Person or Office.....</i>	<i>1091</i>
1. Privacy Official	1091
2. Contact Person or Office	1093
B. <i>Training</i>	<i>1094</i>
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
C. Safeguards (the “Mini-Security Rule”)	1097
1. Administrative Safeguards	1097
2. Technical Safeguards	1098
3. Physical Safeguards	1098
D. Complaint Procedure	1099
E. Sanctions	1100
1. The General Rule	1100
2. Exception for Whistleblowers	1101
3. Exception for Workforce Crime Victims	1101
4. Exception for Individuals Who Take Certain Actions	1101
F. Duty to Mitigate Harmful Effects of Improper Uses or Disclosures	1102
G. Prohibitions on Retaliation and Waiver of Rights	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	1107
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
XXIX. Core Security Requirements	1121
A. Introduction to HIPAA’s Security Requirements	1121
1. Structure of the HIPAA Security Rule	1122
2. HIPAA’s Security Requirements	1122
3. Overview of the HIPAA Security Rule	1123
B. What Information Is Protected and What Entities Must Comply?	1124
1. What Information Is Protected by the HIPAA Security Rule?	1124
2. What Entities Must Comply With the HIPAA Security Rule?	1126
C. General Obligations Under the HIPAA Security Rule	1127
1. Security: General Requirements	1127
2. Policies and Procedures	1128
3. Documentation	1129
D. Flexibility of Approach: Written Risk Analysis Required	1130
1. Standards	1130

2. Implementation Specifications	1130
3. Maintenance of Security Measures	1132
E. <i>What Must a Covered Entity Do to Comply With the HIPAA Security Rule?</i>	1132
1. Administrative Safeguards	1132
2. Physical Safeguards.....	1149
3. Technical Safeguards.....	1153
XXX. Security & Privacy Compliance Roadmaps	1181
A. <i>Security Compliance Action Plan for Group Health Plans and Their Sponsors</i>	1181
1. Steps Toward Security Compliance	1181
2. Security Standards and Implementation Specifications	1183
B. <i>Privacy Compliance Action Plan for Group Health Plans and Their Sponsors</i>	1191
XXXI. Mistakes Happen: Correcting HIPAA Privacy and Security Compliance Problems	1211
A. <i>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
B. <i>Chart Summarizing Possible Remedial Action for HIPAA Privacy and Security Violations</i>	1212
C. <i>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 Not Meet HIPAA Requirements	1216
3. The Authorization Is Not Signed or Is Signed By the Wrong Person	1216
D. <i>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
E. <i>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
F. <i>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
<i>G. Failure to Properly Safeguard PHI.....</i>	<i>1223</i>
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
<i>H. Problems Relating to Business Associates.....</i>	<i>1224</i>
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
XXXII. Electronic Transactions and Code Sets.....	1231
<i>A. Introduction to HIPAA’s Electronic Transaction Requirements.....</i>	<i>1232</i>
<i>B. Implementation Date and Enforcement Policy.....</i>	<i>1234</i>
1. Implementation Date and Extension.....	1234
2. CMS Enforcement Policy.....	1235
<i>C. What Do the EDI Standards Require?.....</i>	<i>1237</i>
1. General Requirements.....	1237
2. Application of EDI Requirements to Health Care Providers.....	1237
3. Application of EDI Standards to Health Plans.....	1238
4. Application of EDI Requirements to Health Care Clearinghouses.....	1239
<i>D. What Transactions and Transmissions Are Covered?.....</i>	<i>1240</i>
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
<i>E. Standards Applicable to Covered Transactions.....</i>	<i>1247</i>
<i>F. What Exceptions Apply to HIPAA’s EDI Requirements?.....</i>	<i>1249</i>
1. Direct Data Entry.....	1249
2. Paper Transactions.....	1249
3. Transactions by Noncovered Entities.....	1250
4. Group Health Plan Exclusion for Self-Administered Plans With Fewer Than 50 Participants.....	1250
5. Certain Excepted Benefits.....	1250
6. Workers’ Compensation.....	1251
7. Health Plan Sponsors.....	1251
8. Other Exceptions.....	1251
<i>G. Modifications.....</i>	<i>1251</i>
<i>H. Code Sets.....</i>	<i>1251</i>
<i>I. Unique Health Identifiers.....</i>	<i>1253</i>
1. Individual Identifiers.....	1253
2. Health Plan Identifier.....	1253
3. Employer Identifiers.....	1253
4. National Provider Identifier.....	1253

<i>J. Action Items for Health Plan Sponsors</i>	1259
XXXIII. [Reserved]	1311
XXXIV. Other Privacy Laws	1311
<i>A. Gramm-Leach-Bliley Act</i>	1311
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>B. Americans with Disabilities Act (ADA)</i>	1313
<i>C. Federal Trade Commission Act</i>	1314
<i>D. Federal Substance Abuse Rules</i>	1314
<i>E. Federal Computer Fraud and Abuse Act</i>	1317
1. The CFAA	1317
2. The CFAA and HIPAA	1317
<i>F. Federal Constitutional Rights of Privacy for Medical Records</i>	1319

PART 5 OF 5

ADDITIONAL HIPAA RULES AFFECTING GROUP HEALTH PLANS

XXXV. Fraud and Abuse Rules Apply to Health Plans, Providers, and Individuals	1341
<i>A. Prohibitions Against Inducements for Referrals (Anti-Kickback Laws)</i>	1341
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>	1343
<i>C. Federal Health Care Offenses</i>	1344
<i>D. Fraud & Abuse Data Collection Program</i>	1346
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
XXXVI. Multiple Employer Welfare Arrangements (MEWAs)	1381
<i>A. Overview</i>	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
<i>B. When Is a MEWA a Group Health Plan and Why Does it Matter?</i>	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

Indexbehind the Index and Glossary Tab

Glossary of Termsbehind the Index and Glossary Tab

Flowcharts, Tables and Graphics

Summarizing HIPAA’s Application to Particular Plans and Benefits192

The Two Conditions for a Health FSA to Be Considered as Providing HIPAA Excepted Benefits204

Operation of HIPAA’s PCE Provisions243

Illustrations of How the Creditable Coverage Rules Work267

Chart Summarizing Possible Remedial Action for HIPAA Violations582

Selected HIPAA Rules That May Impact Insured Individual and Group Health Plans691

Administrative Simplification Regulations Implementation Dates755

HIPAA Privacy Rule Complaint Process760

Disclosures From Group Health Plan to Plan Sponsor.....889

Quick Reference of Common Employer Issues That May Be Affected by the HIPAA Privacy Rule874

Summarizing Plan Sponsor Responsibilities in Various Scenarios910

Figure 1—Insured Plan; Sponsor Is “Hands-Off” PHI912

Figure 2—Insured Plan; Sponsor Is “Hands-On” PHI.....916

Figure 3—Self-Funded Plan; Sponsor Is “Hands-On” PHI918

Figure 4—Self-Funded Plan With TPA; Sponsor Is “Hands-On” PHI920

Permissible Disclosures of PHI for Treatment, Payment, and Health Care Operations 1001

Security Rule Compliance Charts..... 1183-1191

Is This Transaction Subject to the EDI Standards? 1241

Standards Applicable to Covered Transactions 1247

Appendix Tabs

Tab 1:	Portability: Federal Statutes	Tab 7:	Privacy & Security: Gov't Forms
Tab 2:	Portability: Federal Regulations	Tab 8:	Privacy & Security: Other Guidance
Tab 3:	Portability: Government Forms	Tab 9:	Legislative History
Tab 4:	Portability: Other Federal Guidance	Tab 10:	Sample Documents
Tab 5:	Privacy & Security: Statutes	Tab 11:	Miscellaneous
Tab 6:	Privacy & Security: Regulations		