



HIPAA Tool Kit

2017

Contents

Introduction	1
About This Manual.....	1
A Word About “Covered Entities”	1
A Brief Refresher Course on HIPAA.....	2
A Brief Update on HIPAA	2
Progress Report	4
Ongoing Compliance with HIPAA.....	6
Enforcement Rule Changes as Required by the HITECH Act	7
HIPAA Privacy in Emergency Situations	8
Modifications to HIPAA Privacy Rules for Genetic Information	8
Notice of Privacy Practices	8
HIPAA Privacy Standards	15
Overview of HIPAA Privacy Requirements.....	15
Scope of the HIPAA Privacy Standards	15
Notice, Authorization, Accounting, and Amendment	15
Notice and Authorization	16
Patient Requests to Restrict Uses and Disclosures of Protected Health Information	16
Using and Disclosing Protected Health Information	16
The Minimum Necessary Standard	17
Privacy Violations	19
Office for Civil Rights Audits	22
Special Situations	36
Ensuring that Business Associates Comply with the Privacy Rules	37
What the BA Agreement Must Contain	38
Documentation Requirements	40
Rules for Accessing and Amending Information	42
Status of the Privacy Rules	44
Monitoring the Impact of the Privacy Rules.....	45
Understanding Protected Health Information	45
Reviewing HIPAA Privacy Requirements and Model Policies	47
Comparing HIPAA and State Privacy Requirements	47
Examining Users, Uses, and Disclosures of Information	47
Examining Current Privacy Practices	48
Examining How Business Associates Use Information	49
Developing a Strategy for Complying with HIPAA’s Privacy Rules.....	50
Strategic Considerations	50
HIPAA Privacy Milestones	55
Key Compliance Decisions	55
HIPAA Compliance Work Plan.....	56
Privacy Policy and Procedure Manual	56
Notice and Authorization Forms	56
Review Minimum Necessary Policies	56
Amend Contracts with Business Associates	56
Procedures to Provide for Access to and Amendment of Protected Health Information	57
Complaint Process	57
Documentation Procedures and Systems	57
Conduct Privacy Training Sessions	57
Privacy Audit Program	58
Resources on the Web	58

Privacy Model Policies and Procedures59

Creating a HIPAA Privacy Compliance Plan..... 59

Model Policies and Procedures60

 P-1000 General Administrative Policies and Procedures62

 P-1100 Staff Responsibilities63

 P-1200 Staff Training66

 P-1300 Staff Compliance and Sanctions68

 P-1400 Business Associates and Protected Information72

 NIST Resource Guide74

 PF-1400 Sample Business Associate Agreement Language76

 P-1500 Development and Maintenance of Privacy Policies and Procedures81

 P-1600 Documentation and Record Keeping83

 P-2000 Use and Disclosure of Protected Health Information85

 P-2100 Use and Disclosure of Information for Treatment Purposes86

 P-2200 Use of Patient Information for Payment Purposes88

 P-2300 Use and Disclosure of Information for Health Care Operations90

 P-2400 Law Enforcement and Public Health91

 P-2500 Marketing and Fundraising97

 P-2600 Other Disclosure Situations99

 P-2700 Disclosure of Protected Health Information After Death102

 P-2800 Communications and Media Relations103

 P-3000 Notice and Authorization105

 P-3100 Notice of Privacy Practices106

 PF-3100 Notice of Privacy Practices110

 P-3300 Authorization of Use or Disclosure114

 PF-3300 Standard Authorization of Use and Disclosure of Protected Health Information118

 P-3400 Patient Requests for Restrictions on Uses and Disclosures of Confidential Communications122

 PF-3400 Request for Confidential Communication of Protected Health Information125

 P-4000 Personal Representatives, Parents, Spouses, and Others126

 P-4100 Personal Representatives127

 P-4200 Parental Access to Protected Health Information Concerning Children129

 P-4300 Disclosure of Information to Family Members130

 P-4400 Disclosure of Information to Close Personal Friends131

 P-4500 Disclosure of Information in an Emergency Situation132

 P-5000 Patient Access to Health Information134

 PF-5000 Request to Inspect or Copy Protected Health Information140

 PF-5030 Approval of Request to Inspect or Copy Protected Health Information141

 PF-5040 Denial of Request to Inspect or Copy Protected Health Information142

 PF-5042 Review of Denial to Permit Inspection or Copying of Protected Health Information143

 P-5200 Amendment of Health Information144

 PF-5210 Request to Amend Protected Health Information145

 P-7000 Accounting for Disclosures151

 P-7200 Accounting to Patients for Disclosures of Information152

 PF-7200 Request for Accounting of Protected Health Information Disclosures154

 P-7300 Information to Be Provided in an Accounting of Disclosures155

 P-7400 Documentation of Accountings Provided to Patients156

 P-7500 Documentation of Disclosures Requiring an Accounting157

 P-8000 Resolution of Complaints and Breaches158

 P-8100 Submission of Complaints159

 P-8200 Complaint Resolution Procedures160

 P-8300 Documentation of Complaints162

 P-8400 Mitigation163

Security Regulations In-Depth165

Overview165

 Administrative Safeguards165

 Physical Safeguards166

 Technical Safeguards166

General Obligation to Ensure Security..... 167

Flexibility..... 168

Administrative Safeguards 182

 Administrative Safeguard Standard 1: Security Management Process 183

 Administrative Safeguard Standard 2: Assigned Security Responsibility 194

 Administrative Safeguard Standard 3: Workforce Security 194

 Administrative Safeguard Standard 4: Information Access Management 195

 Administrative Safeguard Standard 5: Security Awareness and Training 197

 Administrative Safeguard Standard 6: Security Incident Procedures 199

 Administrative Safeguard Standard 7: Contingency Plan 199

 Administrative Safeguard Standard 8: Evaluation of Compliance 203

 Administrative Safeguard Standard 9: Business Associate Contracts 204

Physical Safeguards..... 204

 Physical Safeguard Standard 1: Facility Access Controls 205

 Physical Safeguard Standard 2: Workstation Use 206

 Physical Safeguard Standard 3: Workstation Security 207

 Physical Safeguard Standard 4: Device and Media Controls 207

Technical Safeguards 209

 Technical Safeguard Standard 1: Access Control 209

 Technical Safeguard Standard 2: Audit Controls 212

 Technical Safeguard Standard 3: Integrity Controls 213

 Technical Safeguard Standard 4: Person or Entity Authentication 213

 Technical Safeguard Standard 5: Transmission Security 214

Business Associate Contracts/Agreements Standard 215

Policies and Procedures Standards..... 217

 Documentation Requirements 217

Breach Notification Interim Final Rule/Final Rule..... 218

 Breach Notification Rule Requirements 218

 Definitions 218

 Risk Assessment 220

 Techniques for Protecting PHI 220

 Limited Data Sets 221

 Exceptions to Breach 222

 Timing of Breach 223

 Notification to Individuals—Timeliness, Content, and Methods 223

 Notification by a Business Associate 227

 Law Enforcement Delay 228

 Administrative Requirements 228

 Preemption Over or by State Laws 228

 HHS Guidance on Securing PHI 229

How to Respond to a Data Breach—Case Study 229

Red Flags Rule..... 232

 Questions and Answers About the Red Flags Rule 233

Security Model Policies and Procedures 235

 Creating a HIPAA Security Compliance Plan 235

 Instructions for Using the Model Policies and Procedures 235

 Introduction to the Security Policy and Procedure Manual 236

 Compliance Checklist..... 236

 Instructions 236

 Administrative Safeguards 238

 SP-1 Assigned Security Responsibility 238

 Sample Job Description 238

 NIST Resource Guide 240

 SP-2 Security Management Process 240

 SP-2.1 Risk Analysis 240

 SP-2.2 Risk Management 241

 SP-2.3 Sanction Policy 242

 SP-2.4 Information System Activity Review 243

 SP-3 Workforce Security 244

 NIST Resource Guide 244

SP-3.1	Authorization/Supervision	245
SP-3.2	Workforce Clearance	247
SP-3.3	Termination Procedures	247
SP-4	Information Access Management	249
	NIST Resource Guide	249
SP-4.1	Isolating Health Care Clearinghouse Functions	250
SP-4.2	Access Authorization	251
SP-4.3	Access Establishment and Modification	252
SP-5	Security Awareness and Training	252
SP-5.1	Security Reminders	254
SP-5.2	Protection from Malicious Software	255
SP-5.3	Log-in Monitoring	256
SP-5.4	Password Management	256
SP-6	Security Incident Procedures	258
	NIST Resource Guide	258
SP-7	Contingency Plan	260
	NIST Resource Guide	260
SP-7.1	Data Backup Plan	262
SP-7.2	Disaster Recovery Plan	263
SP-7.3	Emergency-mode Operation Plan	264
SP-7.4	Testing and Revision Procedures	265
SP-7.5	Applications and Data Criticality Analysis	266
SP-8	Evaluation	267
	NIST Resource Guide	268
SP-9	Business Associate Contracts	269
Physical Safeguards.....		270
SP-10	Facility Access Controls	270
	NIST Resource Guide	270
SP-10.1	Contingency Operations	272
SP-10.2	Facility Security Plan	273
SP-10.3	Access Control and Validation Procedures	274
SP-10.4	Maintenance Records	275
SP-11	Workstation Use	275
	NIST Resource Guide	276
SP-12	Workstation Security	277
SP-13	Device and Media Controls	278
	NIST Resource Guide	278
SP-13.1	Disposal	279
SP-13.2	Media Re-use	280
SP-13.3	Accountability	280
SP-13.4	Data Backup and Storage	281
Technical Safeguards		282
SP-14	Access Control	282
SP-14.1	Unique User Identification	282
SP-14.2	Emergency Access Procedures	282
SP-14.3	Automatic Logoff	282
SP-14.4	Encryption and Decryption	283
	NIST Resource Guide	283
SP-15	Audit Controls	284
	NIST Resource Guide	284
SP-16	Integrity	285
SP-17	Person or Entity Authentication	286
	NIST Resource Guide	287
SP-18	Transmission Security	288
	NIST Resource Guide	288
SP-18.1	Integrity Controls	289
	NIST Resource Guide	289
SP-18.2	Encryption	290
SP-19	Business Associate Contracts/Agreements	290
Breach Notification Sample Policies.....		293
SP-20	Discovery of a Breach	293

SP-21 Breach Investigation 294

SP-22 Risk Assessment 294

SP-23 Notification 294

SP-24 Breach Information Log 296

Red Flag Rules Sample Policies..... 297

SP-25 Creation of Medical Identity Theft Prevention Program 297

SP-26 Identify the Red Flags That Signal Possible Medical Identity Theft 297

SP-27 Detect Medical Identity Theft As It Occurs 298

SP-28 Prevent and Mitigate Identity Theft 298

SP-29 Update the Medical Identity Theft Prevention Program 299

Identifiers301

HIPAA Uniform Identifier Requirements 301

 Uses of Identifiers 301

 Provider Identifiers 301

 Employer Identifiers 306

 Health Plan Identifiers 306

 Continued Compliance with Identifiers 308

Identifiers Model Policies and Procedures309

Compliance Checklist..... 309

Model Policies and Procedures 310

 IP-1 Patient Identifiers 310

 IP-2 Provider Identifiers 310

Transaction Standards311

The Purpose of This Chapter 311

A Reminder About ‘Covered Entities’ 311

HIPAA Highlights/Review 311

Health Plan Requirements 312

Mandatory Submission of Claims Electronically to Medicare 312

 Contingency Plan 312

 Initial Claims 313

 Small Employers 314

 Types of Claims Exempt from Electronic Submission 314

 Waivers to the Electronic Submission Requirement 314

 Contractor Approval for Waivers 315

 Unusual Circumstances 315

Claims Attachments 316

Use of Health Care Clearinghouses 317

Content of HIPAA Transaction Standards 317

Transaction Standards Approved So Far..... 319

Terms Used in the Transaction Standards 321

Electronic Funds Transfer..... 323

Claim Edits and Rejections..... 323

 Interchange Control or ISA Edits 323

 GS Edits 324

 IG Edits 324

 Provider Authorization Edits 324

 Payer-Specific Edits 324

 Trading Partner EDI Specifications 324

Top Errors Found in Medicare Test Submissions..... 325

 Top Errors Found in 5010 Testing 325

HIPAA Code Sets..... 326

 The Meaning of ‘Code Sets’ 326

 Revisions to the Code Set Regulations 327

ICD-10 Code Set..... 329

 Establishing Better Clinical Outcomes and Treatment Protocols 331

Trading Partner Agreements..... 332

 Responsibilities of Trading Partners 332

 Effective Date for Transaction Standards 332

 How to Assess HIPAA’s Impact 332

Survey of Coding Practices333

Survey of Trading Partners334

Transaction Standards Model Policies and Procedures337

Compliance Checklists.....337

 Survey of Information Systems337

 Survey of Trading Partners338

 Survey of Coding Practices340

 T-1000 Use of Standard Transactions341

 T-1200 Testing and Certification of Compliance with Federal Transaction Standards344

 T-2000 Trading Partner Agreements344

 T-3000 Updating Code Sets and Practices344

Employee Training and Education347

Privacy Training347

 Developing and Implementing Training Programs347

 Instructor’s Guide.....348

 Section 1: A Hypothetical Case History348

 Section 2: Using and Sharing Information352

 Section 3: Notice of Privacy Practices358

 Section 4: Authorization365

 Section 5: Accountings369

 Section 6: Patient Access to Information371

 Privacy Training Presentation373

 Privacy Refresher Training413

 HIPAA Skills Test—Privacy Regulations414

Security Training426

 Developing and Implementing Training Programs426

 Instructor’s Guide.....426

 Information Security426

 Administrative Safeguards427

 Physical Safeguards430

 Technical Safeguards431

 Privacy and Security Training433

 Security Training Presentation434

HIPAA Skills Test—Security Regulations446

 HIPAA Skills Test—Security455

What Would You Do?458

Conducting Internal HIPAA Audits461

Making the Case for HIPAA Auditing461

 Deciding What Information to Audit462

 Creating an Audit Plan464

 Conducting the Audit465

 Evaluating and Reporting Audit Findings465

 Privacy and Security Auditing466

HIPAA Topics477

Accredited Standards Committee477

 Transaction Standards and Code Sets477

 What Is the ASC?477

 What Is the ASC’s Role Under HIPAA?477

 Mission of the ASC477

 Principles of the ASC478

Administrative Simplification478

 General: HIPAA478

 Privacy Standards479

 Requirements479

 Transaction Standards and Code Sets480

 Security Standards482

 Identifiers484

Administrative Simplification Compliance Act..... 485

- Transaction Standards and Code Sets 485
- What Is the Administrative Simplification Compliance Act (ASCA)? 485
- Model Compliance Plan 485
- Electronic Claims 485

American Recovery and Reinvestment Act of 2009 486

- What is the ARRA? 486
- Business Associates 487
- Privacy-Related Provisions 488
- What can we expect? 490

ANSI 490

- General 490
- What Is ANSI? 491
- Standards-Setting Organizations 491
- The Mission of ANSI 491

ASC X12N 491

- Transaction Standards and Code Sets—45 CFR §162.920 491
- The Final Approved ASC X12N Standards 491
- Approved Versions 492
- Future ASC X12N Standards 492

CMS 493

- General 493
- What Is CMS? 493
- CMS’s Role Under HIPAA 493
- CMS Assistance to the Provider Community 493
- CMS As a Covered Entity 494

Code-Set Maintaining Organization..... 494

- Transaction Standards and Code Sets—45 CFR §162.1002 494
- Definition of Code-Set Maintaining Organizations 494
- Approved Code-Set Maintaining Organizations 494

Code Sets..... 495

- Transactions and Code Sets—45 CFR Part 162 Subpart J..... 495
- Definition of Code Sets 495
- Approved Medical Code Sets 495
- International Classification of Diseases, Ninth Edition, Clinical Modification 495
- ICD-10-CM 496
- ICD-10-PCS 497
- Current Procedural Terminology (CPT) 497
- Healthcare Common Procedure Coding System (HCPCS) 498
- National Drug Codes 500
- Code on Dental Procedures and Nomenclature (CDT-4) 501
- Nonmedical Code Sets 501
- Modifications to Approved Code Sets 502
- Table of Medical and Nonmedical Code Sets 503

Communications Under HIPAA 509

- Privacy 509
- Communication by Telephone 509
- Communication by Fax 509
- Communication by Email 509
- Frequently Asked Questions 510
- Tips for Office Communication 512

Companion Guides..... 515

- Transaction Standards and Code Sets 515
- Definition of Companion Guides 515
- Trading Partners 515
- Sample Companion Guide 515

Compliance Dates 517

- General 517
- Compliance Dates for Transactions and Code Sets 517
- Compliance Dates for Privacy 517
- Compliance Dates for Security 517

- Compliance Dates for Identifiers517
- Covered Entity519
 - General—45 CFR §160.102519
 - Definition of a Covered Entity519
 - Subdivisions of Covered Entities519
 - Am I a Covered Entity?519
 - How to Use These Charts519
- Credentials/Certifications521
 - General521
 - AHIMA-Sponsored Credentials522
 - ISC2-Sponsored Credentials522
- Data Element523
 - Transactions and Code Sets—45 CFR §162.103523
 - Definition of a Data Element523
 - Data Element Summary523
- Data Segment524
 - Transactions and Code Sets—45 CFR §162/103524
 - Definition of a Data Segment524
 - Example of a Data Segment524
 - Segment Delimiters525
 - Segment Terminator525
 - Implementation Guides525
- Decedents526
 - Privacy—45 CFR §164.512(g)526
 - The General Rule Regarding PHI of Decedents526
 - Special Disclosures of PHI Regarding Decedents526
 - Research and the PHI of Decedents526
- De-identified Information.....527
 - Privacy—45 CFR §164.514527
 - Definition of De-identified Information527
 - Reasons for Data De-identification527
 - How to De-identify Protected Health Information527
- Designated Record Set530
 - Privacy—45 CFR §164.501530
 - The Definition of Designated Record Set530
 - The Definition of a Record530
 - Examples of Inclusions in the Designated Record Set530
 - Examples of Exclusions from the Designated Record Set531
 - State Law531
- Direct Data Entry532
 - Transactions and Code Sets—45 CFR §162.923(b)532
 - Definition of Direct Data Entry532
 - Rules Surrounding Direct Data Entry Systems532
 - Data Entry Through an Intermediary532
- Direct Versus Indirect Treatment Relationship533
 - Privacy—45 CFR §164.520533
 - Definition of an Indirect Treatment Relationship533
 - Definition of a Direct Treatment Relationship533
 - Privacy Requirements Based on Treatment Relationship533
- Disclosure.....534
 - Privacy—45 CFR §164.501534
 - Definition of Disclosure534
 - Verification Requirements534
 - Examples of Verification Procedures534
 - Disclosures to the Patient535
 - Example Situations and Suggested Protocols535
 - Disclosures to Family, Friends, or Others Involved in the Patient’s Care535
 - Disclosures to Clergy535
 - Facility/Hospital Directories536
 - Disclosures to Other Providers537
 - Disclosures to Third Parties Involved in Payment537

DSMO 538

- Transactions and Code Sets—45 CFR §162.910 538
- What Are the DSMOs? 538
- The Review/Modification Process 538
- Currently Designated DSMOs 538

Electronic Data Interchange (EDI) 539

- Transactions and Code Sets 539
- Definition of EDI 539
- Benefits of EDI 539
- The Administrative Simplification Compliance Act and EDI Requirements for Small Providers 539

Electronic Media 540

- General—45 CFR §160.103 540
- Definitions of Electronic Media 540
- What Is Not Electronic Media 540

Electronic Signatures 541

- Security 541
- Electronic Signatures and the Security Rule 541
- State Law on Electronic Signatures 541
- AHIMA Best Practice Standards 541
- SAFE Project 542

Electronic Transactions 542

- Transactions and Code Sets—45 CFR §160.103 542
- Definition of an Electronic Transaction 542
- Types of Electronic Transactions 542
- Electronic Transactions and HIPAA Standards 543

Emergency Situations 543

- Release of Information During Emergency Situations 543

Employer Identifiers 544

- Unique Identifiers—45 CFR §162.610 544
- Rule for Employer Identifiers 544
- Adopted Standards 544
- Transactions Affected 545

Enforcement 545

- General 545
- OCR Enforcement of the Privacy and Security Rule 545
- Office for Civil Rights Organizational Chart 547
- Privacy Complaint Process 547
- Compliance and Enforcement Rule 549
- Transactions and Code Sets Complaint Process 554
- Electronic Data Interchange (EDI) 556

Fundraising Under HIPAA 561

- Privacy—45 CFR §164.514 (f) 561
- Requirements Under the Regulations 561
- Issues with Current Typical Fundraising Practices 561

Genetic Non-Discrimination Act (GINA) of 2008 564

- Privacy—45 CFR §164.520 564
- GINA’s Requirements 564
- HIPAA Omnibus and GINA 564

Government Access to Information 565

- Privacy—45 CFR §164.512(f) 565
- The Privacy Rule and Government Access to Information 565
- Guidance from the Office for Civil Rights on Government Access to PHI 565

Health Care 568

- General—45 CFR §160.103 568
- Health Care Defined 568
- Other Government Definitions 568
- Other Services 572
- Helpful Questions and Answers 573

Health Care Clearinghouse 574

- General—45 CFR §160.103 574

- Clearinghouse Defined574
- Frequently Asked Questions574
- Health Care Operations577
 - Privacy—45 CFR §164.501577
 - Health Care Operations Defined577
 - Operations Versus Research578
 - American Recovery and Reinvestment Act of 2009578
- Health Care Provider579
 - General—45 CFR §160.103579
 - Health Care Provider Defined579
 - Other Government Definitions579
 - Are You a Health Care Provider?580
- Health Information583
 - General—45 CFR §160.103583
 - Health Information Defined583
 - Individually Identifiable Health Information583
 - Protected Health Information583
- Health Information Technology for Economic Health (HITECH) Act.....583
- Health Plan584
 - General—45 CFR §160.103584
 - Health Plan Defined584
 - Health Plan Comparisons584
- Health Plan Identifiers588
 - Unique Identifiers588
 - Unique Identifiers Defined588
 - HPID and OEID588
- HHS.....589
 - General589
 - HHS: What It Does589
 - HHS Operating Divisions590
 - Other HHS Agencies591
 - Organization of HHS592
- Implementation Guides594
 - Transactions and Code Sets—45 CFR §162.920594
 - Implementation Guides594
 - Details on the Specifications594
 - Retail Pharmacy Specifications594
 - Companion Guides595
- Incidental Disclosures.....595
 - Privacy—45 CFR §164.502(a)(1)595
 - Incidental Disclosures Defined and Regulatory Context596
 - Tips for Monitoring596
- Individual Identifiers597
 - Unique Identifiers597
 - Purpose of Individual Identifiers598
 - Issues with Individual Identifiers598
 - Frequently Asked Questions on Individual Identifiers598
- Limited Data Set.....599
 - Privacy—45 CFR §164.514(e)599
 - Requirements of a Limited Data Set599
 - Data-Use Agreements600
 - American Recovery and Reinvestment Act of 2009600
 - HIPAA Compliance Tool600
 - Data Use Agreement for Limited Data Set601
- Loop602
 - Transaction Standards and Code Sets602
 - Loop Defined602
 - Required and Situational Loops602
 - Examples603
- Marketing Under HIPAA.....603
 - Privacy—45 CFR §164.508(a)(3)603
 - Definition of Marketing604

Exceptions to the Definition 604

American Recovery and Reinvestment Act of 2009 604

OCR Frequently Asked Questions 605

NCPDP Format 607

 Transactions and Code Sets—45 CFR §162.1102 607

 Details on the Standards 607

NDC..... 611

 Transactions and Code Sets—45 CFR §162.1002 611

 Requirements 611

 The Code Set 611

Notice of Privacy Practices 612

 Privacy—45 CFR §164.520 612

 Who Must Receive the Notice 612

 Good-Faith Effort to Obtain Written Acknowledgment of Receipt 613

 Content Requirements 613

 Request for Restrictions on Use or Disclosure and Confidential Communication 615

 Documentation of Compliance 615

 Emergency Treatment 615

Paper Transactions 616

 Transactions and Code Sets 616

Payment 617

 Privacy—45 CFR §164.500 617

 Definition of Payment 617

 Payment and the Standard Transactions 617

 Required, Situational, and Optional Data Elements Compared 618

Personal Representatives..... 619

 Privacy—45 CFR 164.502(g) 619

 Who Must Be Recognized As a Personal Representative 619

 Parents and Unemancipated Minors 619

 Abuse, Neglect, and Endangerment Situations 620

Pre-emption 621

 Privacy—45 CFR §160 Subpart B 621

 Exceptions to the Pre-emption Standards 621

 Sample Analysis 621

New York State Office of Mental Health HIPAA Pre-emption Analysis 622

Privacy and Litigation 625

 Subpoena of Records in Qui Tam and Class Action 625

Privacy Rule 625

 Privacy—45 CFR Parts 160 & 164 625

 Purpose of Privacy Regulations 625

 Fundamental Concepts 626

Protected Health Information 629

 Privacy—45 CFR §164.501 629

Provider Identifiers 629

 Unique Identifiers—45 CFR §162.402-414 629

 Final Rule 629

 Other Provisions of the Final Rule 630

Psychotherapy Notes 631

 Privacy—45 CFR 164.508(a)(2) 631

 Definition of Psychotherapy Notes 631

 Maintaining Psychotherapy Notes 631

 Use and Disclosure Requirements 631

 Authorization Exceptions 632

 Patient Right to Access 632

Red Flags Rule 632

 General 632

 Questions and Answers About the Red Flags Rule 633

Required Safeguards 635

 Privacy—45 CFR 164.530(c) 635

 Where Privacy and Security Overlap 635

 Administrative Safeguards 635

- Physical Safeguards636
- Technical Safeguards636
- Retail Pharmacy.....636
 - Transactions and Code Sets636
 - Frequently Asked Questions636
- Reviews of Compliance by the Office of Inspector General637
- Security Rule638
 - Security—45 CFR Parts 160, 162 and 164638
 - Security Safeguard Groupings638
 - Overlap Between Safeguards639
 - The Five General Organizational Obligations Established by the Security Rule639
 - Covered Entity Legal Obligations Under Federal Law640
 - American Recovery and Reinvestment Act of 2009640
- Security Standards Matrix.....640
- Small Provider Exemption642
 - Transactions and Code Sets642
- Standard Setting Organization.....642
 - Transactions and Code Sets—45 CFR §160.102642
 - Details on SSOs642
 - DSMOs642
- Standards.....643
 - General643
- Trading Partner.....643
 - Transactions and Code Sets—45 CFR §162.915643
 - Definition of a Trading Partner643
 - Examples of Trading Partner Relationships644
 - Trading Partner Agreements644
- Training Requirements644
 - General—45 CFR §164.530(b), 164.308(a)(5)644
 - Privacy Training645
 - Security Training645
 - NIST Resource Guide646
 - Other Educational Options647
- Transaction Standards649
 - Transactions and Code Sets649
 - Health Plan Requirements649
 - Mandatory Submission of Claims Electronically to Medicare650
 - Use of Health Care Clearinghouses in the Transaction Process651
 - Content of HIPAA Transaction Standards651
 - Approved Transactions652
 - 270/271655
 - 275/277655
 - 276/277656
 - 278656
 - 820656
 - 834657
 - 835657
 - 837657
 - Claims Attachment658
 - Claims Testing Issues658
 - Top Errors Found in 5010 Testing660
- Treatment662
 - Privacy—45 CFR §164.501662
 - Definition of Treatment662
- Verification Requirements662
 - Privacy—45 CFR §164.504662
 - Verification Scenarios663
 - Example Situations and Suggested Protocols664
- Index665**

P-1200 Staff Training

This section establishes the responsibility for development and updating of staff training programs and materials on privacy policies and procedures. It also establishes the responsibility of all staff members to complete privacy training.

P-1210 Content of Privacy Training Program for Staff

The **[title of privacy official]** or a staff member designated by the **[title of privacy official]** will develop a privacy policy orientation and training program.

The purpose of this program is to make sure that all staff members are familiar with the privacy policies and procedures adopted by **[name of organization]**.

The training and orientation program will cover:

- ◆ The definition and identification of protected health information
- ◆ Providing the “Notice of Privacy Practices” to all patients and obtaining a written acknowledgment of receipt
- ◆ Using and disclosing protected health information for treatment, payment, and health care operations
- ◆ Obtaining authorization, when required, for use and disclosure of protected information
- ◆ Procedures for handling suspected violations of privacy policies and procedures
- ◆ Penalties for violations of privacy policies and procedures
- ◆ Documentation required by the policies and procedures manual

Staff members will:

- ◆ Receive a summary of the medical practice’s privacy policies and procedures
- ◆ Have an opportunity to review the policies and procedures manual
- ◆ Have an opportunity to ask questions about the privacy policies and procedures of **[name of organization]**

Regulation

45 CFR 164.530(b)(1)

Requires training of all staff members on privacy policies and procedures.

P-1220 Initial Privacy Orientation and Training

All staff members must complete the privacy policy orientation and training program during their probationary period.

1. Completion of the privacy policy orientation and training program will be documented in the employee’s personnel file by the **[title of privacy official]** or the staff member who conducts the training.
2. Until staff members complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
3. Prior to the end of a staff member’s probationary period, his or her supervisor should confirm that he or she has completed privacy training.

- The probationary period of any new employee who has not completed the privacy policy orientation and training program will be extended, and the employee will be ineligible for benefits that would have become available upon completion of the probationary period. In some cases, an employee who does not complete the privacy orientation and training program prior to the end of his or her probationary period will be required to complete the program before resuming normal job duties.

Regulation

45 CFR 164.530(b)

Establishes HIPAA requirements for staff training.

P-1230 Revised Policies and Procedures Training

The **[title of privacy official]** or a staff member designated by the **[title of privacy official]** will develop training materials on new or revised privacy policies and procedures.

Procedures

- Staff whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within one month of their effective date.
- Completion of training on revised policies and procedures will be documented in the employee's personnel file.

Regulation

45 CFR 164.530(b)(2)(ii)

Requires documentation of training.

IMPORTANT

Note: The medical practice's legal counsel should review and approve any penalty that is proposed to be assessed for non-compliance with privacy policies and procedures.

P-2300 Use and Disclosure of Information for Health Care Operations

This section addresses the uses and disclosures of information in the course of day-to-day operations that do not require specific authorization (see policy P-3300).

Regulation

45 CFR 164.506

Establishes requirements for the use and disclosure of protected health information for the purposes of treatment, payment, and health care operations.

P-2310 Definition of Health Care Operations

Use and disclosure of protected health information is permitted under this policy to conduct the following activities:

- ◆ Quality assessment and improvement
- ◆ Professional credentialing
- ◆ Medical and utilization review
- ◆ Legal services
- ◆ Auditing
- ◆ Business planning and market research
- ◆ Grievance procedures
- ◆ Due diligence analysis related to sales and acquisitions
- ◆ Creation of de-identified information and limited data sets
- ◆ Customer service
- ◆ Patient directories
- ◆ Compliance monitoring

Before using or disclosing protected health information for any of the functions included in health care operations, a good-faith effort must be made to obtain the patient's written acknowledgment of having received the "Notice of Privacy Practices." Obtaining the written acknowledgment is the responsibility of the **[title of receptionist]**. If the patient's acknowledgment cannot be obtained, the reason the attempt to obtain an acknowledgment was unsuccessful must be documented in writing.

Procedures for obtaining an acknowledgment are established by policy P-3190.

IMPORTANT

Review by legal counsel is advised.

Conducting Internal HIPAA Audits

Making the Case for HIPAA Auditing

The foundation of all good compliance programs—whether they address compliance with the government’s rules on coding and billing or health information privacy and security—is auditing and monitoring. Any good audit program helps an entity maintain compliance with whatever area the auditor is examining.

Although there are no set guidelines for auditing an existing Health Insurance Portability and Accountability Act program, two standards within the security rule require some form of auditing. If an organization has a HIPAA program in place, these areas should already be an active part of their HIPAA processes.

- ◆ Section 164.308(a)(1)(ii)(d), *Information system activity review (Required): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
- ◆ Section 164.312(1)(b), *Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

Beginning in 2011 the Office for Civil Rights (OCR) established a pilot audit program to determine if covered entities (CE) and business associates (BA) had implemented HIPAA privacy, security, and breach notification programs as required by HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act and to assess if the guidelines and processes that were established by the CE comply with the rules. If the Department of Health and Human Services (HHS) and the OCR feel it is necessary to audit these programs, then so should covered entities.

Proof of the need for ongoing auditing and monitoring is evident in OCR’s finding from the initial pilot audits conducted in 2012. At the joint OCR and National Institute of Standards in Technology (NIST) conference, “Safeguarding Health Information: Building Assurance Through HIPAA Security,” held in September 2014, the OCR reported that “58 out of the 59 health care providers audited had at least one negative finding regarding security rule compliance, 56 percent became aware of additional HIPAA regulations that apply to their organizations, and two-thirds of all entities had no complete or accurate risk assessment program.” Based on the less-than-flattering findings from these phase one audits, the OCR is likely to step up HIPAA enforcement.

According to the numbers posted on the HHS website, the number of complaints received in 2012 was 10,454, rising to 12,915 in 2013. Independent research conducted by the Ponemon Institute on the cost of a data breach over several industry sectors, including health care, “found the average cost of a data breach to be \$5.5 million with average cost per compromised record around \$200” after a loss or theft of protected personal information.

IMPORTANT

An entity relying on its own complaint/grievance process to catch instances of noncompliance could be missing processes that violate HIPAA rules.

IMPORTANT

Two-thirds of CEs audited did not perform a complete or accurate risk assessment. Remember, some standards are required and some are addressable. “Required” means the policies and/or procedures must be implemented. “Addressable” means the CE must assess if the standard is “reasonable and appropriate” for the environment. A risk assessment is a required element of the security rule and includes a risk analysis [164.308(a)(1)(ii)(A)] and risk management [64.308(a)(1)(ii)(B)].