

# TABLE OF CONTENTS

## Table of Contents, Current Contents

### How to Use This Service

### Newsletters

### Tab 100: HIPAA Overview

<b>Executive Summary .....</b>	<b>¶100</b>
<b>Growing Need for Data Standardization,</b>	
<b>Privacy Protection and Security.....</b>	<b>¶110</b>
Data Uniformity Is Central Goal .....	¶111
Consumer Demand for Privacy .....	¶112
Increasing Security Hazards .....	¶113
Commercial Uses of Health Care Data.....	¶114
Impact of Evolving Technologies.....	¶115
<b>The Development of HIPAA .....</b>	<b>¶120</b>
Early Stages of HIPAA .....	¶121
Development of Regulations .....	¶122
2009 ARRA (HITECH Act) Amendments .....	¶123
<b>Federal Oversight of HIPAA .....</b>	<b>¶130</b>
Department of Health and Human Services.....	¶131
National Committee on Vital and Health	
Statistics.....	¶132
OCR and CMS.....	¶133
DHHS Data Council .....	¶134
Office of the National Coordinator for Health	
Information Technology .....	¶135

### Tab 200: HIPAA Basics

<b>Executive Summary .....</b>	<b>¶200</b>
<b>Summary of HIPAA Requirements.....</b>	<b>¶210</b>
Electronic Transaction and Code Sets	
Standard.....	¶211
Privacy.....	¶212
Security Standards .....	¶213
National Identifier Standards .....	¶214
Notification in Case of Breach.....	¶215
<b>HIPAA Compliance Essentials .....</b>	<b>¶220</b>
Defining a Covered Entity .....	¶221
Defining Electronic Transmissions,	
Transactions and Code Sets .....	¶222
Confidentiality, Privacy and Security .....	¶223
Organizational Changes Under HIPAA .....	¶224
Small Business Considerations.....	¶225

### Tab 300: Electronic Transactions and Code Sets

<b>Executive Summary .....</b>	<b>¶300</b>
How EDI Works .....	¶301

<b>Necessity for Transaction Standards .....</b>	<b>¶310</b>
Defining Transaction Standards.....	¶311
Defining Code Sets .....	¶312
Developing Standards.....	¶313
<b>HIPAA EDI Transactions Standard.....</b>	<b>¶320</b>
Compliance Deadlines .....	¶321
Scope and Coverage .....	¶322
Entities Exempt From Coverage.....	¶323
Direct Data Entry (DDE) Exception .....	¶324
Description of Standard Transactions .....	¶325
Transactions Not Covered .....	¶326
Code Sets.....	¶327
Operating Rules.....	¶328
<b>Achieving Compliance .....</b>	<b>¶330</b>
Guides for Standard Transactions .....	¶331
Implementing the Standards .....	¶332

### Tab 400: Medical Records Privacy Requirements

<b>Executive Summary .....</b>	<b>¶400</b>
Protected Health Information .....	¶401
Enforcement and Penalties .....	¶402
Other Applicable Federal Laws .....	¶403
State Privacy Laws .....	¶404
<b>HIPAA Privacy Rules: Coverage and Scope .....</b>	<b>¶410</b>
Individual Right to Privacy.....	¶411
Covered Entities .....	¶412
Health Information .....	¶413
Obtaining Authorization or Optional	
Consent .....	¶414
Security Requirements Under Privacy Rule ...	¶415
<b>Protected Information.....</b>	<b>¶420</b>
Permitted Uses of Protected Information.....	¶421
Establishing a Workable Balance in a	
Complex Environment.....	¶422
Permitted Uses and Disclosures For	
Authorizations .....	¶423
Psychotherapy Uses and Disclosures.....	¶424
Permitted Uses and Disclosures Requiring	
Individuals To Have Opportunity To	
Agree or Object .....	¶425
Permitted Uses and Disclosures That Do Not	
Require Authorization or Required	
Opportunity To Agree or Object .....	¶426
Other Third-party Requirements Relating to	
Uses and Disclosures .....	¶427
Whistle-blowers and Workforce Member	
Crime Victims .....	¶428
<b>Business Associates.....</b>	<b>¶430</b>
What Is a Business Associate?.....	¶431

Tab 400 (cont'd)

Contracts With Business Associates .....	¶432
Disclosures to Business Associates .....	¶433
Ensuring Compliance .....	¶434
Responsibilities of the Business Associate .....	¶435
Sample Business Associate Contract Provisions .....	¶436
<b>Patient's Right to Privacy .....</b>	<b>¶440</b>
Notice of Privacy Practices.....	¶441
Requests To Restrict Uses and Disclosures .....	¶442
Individual Access to Records .....	¶443
Denying Access to PHI.....	¶444
Amending and Correcting Records.....	¶445
Accounting for Disclosures .....	¶446
Revocable Authorization .....	¶447
Confidential Communications .....	¶448
Deceased Individuals.....	¶449

**Tab 500: Security and Electronic  
Signature Standard**

<b>Executive Summary .....</b>	<b>¶500</b>
Scope of Security.....	¶501
Security Threats.....	¶502
Overall Approach to Security Under HIPAA .....	¶503
<b>Administrative Safeguards .....</b>	<b>¶510</b>
Security Management Process.....	¶511
Assigned Security Responsibility .....	¶512
Workforce Security.....	¶513
Information Access Management .....	¶514
Security Awareness and Training.....	¶515
Security Incident Procedures .....	¶516
Contingency Plan.....	¶517
Evaluation.....	¶518
Business Associate Agreement .....	¶519
<b>Physical Safeguards.....</b>	<b>¶520</b>
Device and Media Controls .....	¶521
Facility Access Controls .....	¶522
Workstation Use .....	¶523
Workstation Security .....	¶524
<b>Technical Safeguards.....</b>	<b>¶530</b>
Access Control.....	¶531
Audit Controls .....	¶532
Transmission Security .....	¶533
Integrity .....	¶534
Person or Entity Authentication.....	¶535
Rendering PHI Unusable, Unreadable or Indecipherable .....	¶536
<b>Electronic Signatures [RESERVED] .....</b>	<b>¶540</b>

**Tab 600: National Identifiers**

<b>Executive Summary .....</b>	<b>¶600</b>
<b>Standards for Identifiers.....</b>	<b>¶610</b>
Standards-setting Process .....	¶611
Identifier Selection Process .....	¶612
Implementation Teams.....	¶613
Types of Identifiers .....	¶614
Revising Identifiers.....	¶615
<b>National Provider Identifier Standard.....</b>	<b>¶620</b>
Overview of the National Provider Identifier .....	¶621
Scope of NPI Coverage .....	¶622
Approved Uses of NPI.....	¶623
Implementation.....	¶624
Impact on Health Care Entities.....	¶625
National Provider File Data Elements .....	¶626
Data Dissemination .....	¶627
<b>National Employer Identifier Standard.....</b>	<b>¶630</b>
Overview of the National Employer Identifier .....	¶631
Scope of EIN Coverage .....	¶632
Implementation.....	¶633
Using EIN.....	¶634

**Tab 700: Strategies for HIPAA  
Implementation**

<b>Executive Summary .....</b>	<b>¶700</b>
Scalable Solutions .....	¶701
Basic vs. Strategic Compliance .....	¶702
Best Practices .....	¶703
<b>HIPAA — A Long-term Enterprisewide Priority .....</b>	<b>¶710</b>
Departments and Staff Affected by HIPAA .....	¶711
Determining if Your Organization Is a Covered Entity? .....	¶712
<b>Planning Your HIPAA Compliance Project.....</b>	<b>¶720</b>
The Privacy Official .....	¶721
The Security Officer .....	¶722
The HIPAA Project Manager .....	¶723
The HIPAA Project Team .....	¶724
Six Phases of HIPAA Implementation.....	¶725
Small Covered Entities: Implementation Considerations .....	¶726
<b>Foundations of Compliance: Enterprise Awareness.....</b>	<b>¶730</b>
HIPAA Awareness Training .....	¶731
Training .....	¶732
Sanctions .....	¶733
Audits .....	¶734
<b>Foundations of Compliance: Impact Analysis .....</b>	<b>¶740</b>
Impact Analysis Objectives .....	¶741
Impact Analysis Preparation and Planning .....	¶742
Enterprise Baseline Inventory .....	¶743

Tab 700 (cont'd)

Vendor Relationships.....	¶744
Gap Analysis/Impact Analysis.....	¶745
Impact Analysis: Transactions, Code Sets and Identifiers .....	¶746
Impact Analysis: Privacy .....	¶747
Risk Analysis: Administrative, Physical and Technical Safeguards .....	¶748
Ongoing Risk Management and Final Report .....	¶749
<b>Implementation Planning .....</b>	<b>¶750</b>
Planning Considerations .....	¶751
<b>Transactions and Code Sets.....</b>	<b>¶760</b>
Compliance Deadlines.....	¶761
First Steps in Implementation.....	¶762
Transaction Sequencing.....	¶763
Code Sets Implementation Issues .....	¶764
Testing and Certification.....	¶765
Auditing, Monitoring and Enforcing .....	¶766
<b>Security .....</b>	<b>¶770</b>
Vulnerability of Critical Information.....	¶771
Barriers to Better Health Care Security .....	¶772
Nondirected Security Threats .....	¶773
Risk of Directed Attacks.....	¶774
Getting Started on Security.....	¶775
Security Infrastructure.....	¶776
Implementation Execution.....	¶777
<b>Privacy.....</b>	<b>¶780</b>
Privacy Policies and Procedures.....	¶781
Informing Individuals of Privacy Information Practices.....	¶782
Business Associate Agreements.....	¶783
Privacy Forms.....	¶784
Following Through: Training and Reinforcement .....	¶785
<b>Privacy and Security in Health Information Technology .....</b>	<b>¶790</b>
Governing the Exchange .....	¶791
Access and Disclosure.....	¶792
Health IT Future .....	¶793

**Tab 800: Enforcement and Breach  
Notification**

<b>Executive Summary .....</b>	<b>¶800</b>
<b>Enforcement Overview .....</b>	<b>¶810</b>
<b>Complaint System .....</b>	<b>¶820</b>
<b>Enforcement Penalties .....</b>	<b>¶830</b>
Civil Monetary Penalties .....	¶831
Appeals to Administrative Law Judge .....	¶832
Criminal Sanctions .....	¶833

<b>Legal Concerns .....</b>	<b>¶840</b>
Covered Entity Liability .....	¶841
Evidentiary Privilege .....	¶842
Whistleblower Protections.....	¶843
Patients' Standing Right to Sue .....	¶844
State Civil Actions.....	¶845
State Licensure Issues.....	¶846
Electronic Discovery .....	¶847
Red Flags Rule .....	¶848
Social Media.....	¶849
<b>Enforcement Actions .....</b>	<b>¶850</b>
Civil Enforcement .....	¶851
Criminal Enforcement .....	¶852
<b>Breach Notification.....</b>	<b>¶860</b>
What Is a Breach?.....	¶861
Timing of Notification .....	¶862
Notifying Individuals, DHHS and the Media ..	¶863
Notification by Business Associates .....	¶864
Organizational Policies, Sanctions and Training.....	¶865
FTC Rule and State Laws.....	¶866

**Appendix I: Federal Laws**

<b>The Privacy Act of 1974 (5 U.S.C. §552a)</b>
<b>The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §1320d)</b>
<b>American Recovery and Reinvestment Act of 2009, Title XIII – Health Information Technology, Subtitle D – Privacy (Pub. L. No. 111-5)</b>

**Appendix II: Administrative Notices and  
Guidance**

<b>Privacy</b>
General Overview of Standards for Privacy of Individually Identifiable Health Information
Frequently Asked Questions About the HIPAA Privacy Rule
Plain Language Principles and Thesaurus for Making HIPAA Privacy Notices More Readable
Consumer Fact Sheets: Privacy and Your Health Information; Your Health Information Privacy Rights
<b>Security</b>
Frequently Asked Questions About the HIPAA Security Rule
<b>Transactions and Code Sets</b>
Frequently Asked Questions About the HIPAA Transactions and Code Sets Rule

## **Appendix III: Glossary**

General HIPAA Glossary  
Acronym Glossary

## **Appendix IV: Forms and Checklists**

HIPAA Impact Analysis Action Checklist  
Policy and Procedure Questionnaire (Sample)  
HIPAA Pre-Assessment Inventory Survey for Providers  
Electronic Health Care Transactions and Code Sets Standards Model Compliance Plan  
HIPAA EDI Transaction Risk Assessment Checklist  
Health Information Privacy Complaint Form and Related DHHS Notices  
Sample Breach Notification Letter to Patients  
Sample Breach Notification News Release  
Comparison of Privacy Rule and HHS and FDA Human Subjects Protection Regulation  
HIPAA Risk Assessment Audit Checklist  
Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information  
Implementing HIPAA Security Rule: Security Rule/NIST Publications Crosswalk  
NPI Application/Update Form  
Sample Employee Confidentiality Agreement

## **Appendix V: Regulations**

Department of Health and Human Services (Title 45, Subtitle A, Subchapter C: Administrative Data Standards and Related Requirements)

General Administrative Requirements  
(45 C.F.R. Part 160)

General Provisions (§§160.101-.104)  
Preemption of State Law (§§160.201-.205)  
Compliance and Investigations (§§160.300-.316)  
Imposition of Civil Money Penalties (§§160.400-.426)  
Procedures for Hearings (§§160.500-.552)

## **Administrative Requirements (45 C.F.R. Part 162)**

General Provisions (§§162.100-.103)  
Standard Unique Health Identifier for Providers (§§162.402-.414)  
Standard Unique Employer Identifier (§§162.600-.610)  
General Provisions for Transactions (§§162.900-.940)  
Code Sets (§§162.1000-.1011)  
Health Care Claims or Equivalent (§§162.1101-.1102)  
Eligibility for a Health Plan (§§162.1201-.1202)  
Referral Certification and Authorization (§§162.1301-.1302)  
Health Care Claim Status (§§162.1401-.1402)  
Enrollment and Disenrollment in a Health Plan (§§162.1501-.1502)  
Health Care Payment and Remittance Advice (§§162.1601-.1602)  
Health Plan Premium Payments (§§162.1701-.1702)  
Coordination of Benefits (§§162.1801-.1802)  
Medicaid Pharmacy Subrogation (§§162.1901-.1902)

## **Security and Privacy (45 C.F.R. Part 164)**

General Provisions (§§164.102-.106)  
Security Standards for the Protection of Electronic Protected Health Information (§§164.302-.318; Appendix A - Security Standards Matrix)  
Notification in the Case of Breach of Unsecured Protected Health Information  
Privacy of Individually Identifiable Health Information (§§164.500-.534)

**Federal Trade Commission (Title 16, Chapter I, Subchapter C: Regulations Under Specific Acts of Congress)**

**Health Breach Notification Rule (16 C.F.R Part 318)**

## **INDEX**