



HIPAA Manual for Healthcare Providers

Including Doctors, Clinics, Psychologists, Dentists,
Chiropractors, Nursing homes, Pharmacies, and more

Prepared in consultation with HIPAA experts and healthcare professionals

Note: This manual provides extensive coverage of various HIPAA regulations for healthcare providers such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, etc. provided they transmit any information in an electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted a standard. This information has mainly been collected from HHS regulatory texts. Additional information has been collected from materials published by the Office of the National Coordinator for Health Information Technology, the Office for Civil Rights (OCR) and various other locations. It is our intention to make HIPAA compliance easy for your facility. The manual has comprehensive information for training purposes only. If you need documentation or all the various plans mandated by the Office for Civil Rights, you must purchase our Documentation Kit, which is sold separately. Please refer to the training outline that has been provided to assist you in navigating through this manual.

© Copyright 2020 Gamma Compliance Solutions LLC. All rights reserved.

Table of Contents

1	What is HIPAA?	1
1.1	Importance of Privacy and Security	1
1.1.1	Impact public perception of privacy and security can have on support for EHRs and HIEs	1
1.1.1.1	Individuals are less likely to support the use of Electronic Health Records when they do not believe their information is protected	2
1.1.1.2	Individuals are less likely to support Health Information Exchange when they do not believe their information is protected	3
1.1.1.3	Individuals are more likely to withhold information if they have privacy or security concerns	4
1.1.2	Protected health information privacy and security are important... now what?	5
1.2	Background and History of HIPAA Regulations	6
1.2.1	The Health Insurance Portability and Accountability Act of 1996	6
1.2.2	The Privacy Rule	6
1.2.3	The Security Rule	7
1.2.4	The Enforcement Rule	7
1.2.5	The Omnibus Rule	8
1.2.6	The Breach Notification Rule	8
1.2.7	The HITECH Act	8
1.3	Governing Bodies	9
1.3.1	Department of Health and Human Services	9
1.3.2	Office for Civil Rights	9
2	Who must comply with HIPAA?	11
2.1	Covered Entities	11
2.1.1	Providers	12
2.1.2	Health Plans	13
2.1.3	Clearinghouses	14
2.2	Business Associates	15
2.2.1	Business Associate Contracts	16

2.2.2	Business Associate Listing	19
2.3	Special Cases	20
2.3.1	Hybrid Entity	20
2.3.2	Affiliated Covered Entity (ACE)	21
2.3.3	Organized Health Care Arrangement (OHCA)	21
2.3.4	Covered Entities with Multiple Covered Functions	22
2.3.5	Group Health Plan Disclosure to Plan Sponsors	23
3	What information is protected by HIPAA?	25
3.1	Exclusions to information covered by HIPAA	26
3.1.1	Where FERPA and HIPAA Intersect	27
3.1.2	De-identified health information	27
3.1.2.1	Expert Determination	28
3.1.2.2	Safe Harbor	29
3.1.2.3	Re-identification	31
3.1.2.4	Limited Data Set	31
4	What is the Privacy Rule?	33
4.1	Use and disclosure of PHI	33
4.1.1	Permitted Uses and Disclosures	34
4.1.1.1	Treatment, Payment, Operations	34
4.1.1.2	Uses and Disclosures with Opportunity to Agree or Object	35
4.1.1.3	Incidental Use and Disclosure	35
4.1.1.4	Public Interest and Benefit Activities	36
4.1.1.5	Psychotherapy Notes	38
4.1.1.6	Marketing	38
4.2	Minimum Necessary Principle of Uses and Disclosures	41
4.2.1	Requirements of the Minimum Necessary Principle	41
4.2.2	Exceptions of the Minimum Necessary Principle	42
4.3	Administrative Requirements	42
4.3.1	Privacy Personnel [45 CFR 164.530(a)]	43
4.3.2	Workforce Training and Management [45 CFR 164.530(b)]	43

4.3.3	Safeguards [45 CFR 160.530(c)]	43
4.3.4	Complaints [45 CFR 164.530(d)]	44
4.3.5	Sanctions [45 CFR 164.530(e)]	44
4.3.6	Mitigation [45 CFR 164.530(f)]	44
4.3.7	Refraining from Retaliation [45 CFR 164.530(g)]	44
4.3.8	Waiver of Rights [45 CFR 164.530(h)]	45
4.3.9	Privacy Policies and Procedures [45 CFR 164.530(i)]	45
4.3.10	Documentation and Record Retention [45 CFR 164.530(j)]	45
4.4	How State and Federal law intersect with regards to HIPAA	45
4.4.1	Preemption of Federal Law	45
4.4.2	Contrary State Laws	46
4.4.3	Exceptions to Federal Preemption	46
4.4.4	More Stringent State Laws	47
5	What are a patient's rights to their health information?	49
5.1	Right to authorize use and disclosure of PHI	49
5.2	Right to Access of PHI	50
5.2.1	Designated Record Set	51
5.2.2	Providing Access to PHI	52
5.2.2.1	Form and Format Access	52
5.2.2.2	Manner of Access	53
5.2.2.3	Timeliness in Providing Access	54
5.2.2.4	Duration of Right to Access	55
5.2.2.5	Fees for Providing Access to PHI	55
5.2.2.6	Confidential Communications Requirements.	56
5.2.3	Making a Request for Access to PHI	57
5.2.3.1	Requiring a Written Request	57
5.2.3.2	Unreasonable Measures	57
5.2.3.3	Verification	57
5.2.3.4	Exclusions from the Right of Access	58
5.2.3.5	Redirecting a Request for Access	59

5.2.4	Authority for Denial of Access	59
5.2.4.1	Grounds for Denial	59
5.2.4.2	Executing the Denial	61
5.2.4.3	Review of Denial	62
5.3	Right to Designate a Personal Representative	62
5.3.1	Designating a Personal Representative	62
5.3.2	Rights of a Personal Representative	63
5.3.3	Exception to a Personal Representative Designation	63
5.3.4	Who may be recognized as a Personal Representative	64
5.3.5	How unemancipated minors may designate a Personal Representative	65
5.4	Individual's right for Privacy Practice Notice	67
5.4.1	Content of the Notice of Privacy Practices	67
5.4.2	Notice of Privacy Practices Distribution	67
5.4.3	Acknowledgement of Notice Receipt	68
5.5	Right to make Amendments	69
5.5.1	Accepting an Amendment Request	69
5.5.2	Denying an Amendment Request	69
5.6	Right to Accounting of Disclosures	69
5.6.1	Duration to Maintain Disclosure Accounting	70
5.6.2	Exceptions	70
5.6.2.1	Oral Communications	71
5.7	Right to Restrictions	71
5.7.1	Making a Restriction Request	72
5.7.2	Accepting or Denying a Restriction Request	72
5.8	Right to Confidential Communications	72
5.9	Right to Make Complaints	73
5.9.1	Communicating the Right to Complain	73
5.9.2	Complaint Protections	73
5.9.3	Complaint Record Retention	73
5.9.4	Making a Complaint	74

6	What is the Security Rule?	75
6.1	Differences between the Privacy Rule and Security Rule	76
6.2	Security Rule Flexibility	77
6.3	General Rules	78
6.3.1	Security Rule Definitions of Integrity, Availability and Confidentiality	79
6.3.2	Risk Assessment and Management	79
6.3.2.1	Risk Assessment Activities	80
6.3.2.2	When is a Risk Assessment Required?	80
6.3.3	Explanation of Safeguards	81
6.3.3.1	Types of Safeguards	81
6.3.3.2	Definition of Standards and Implementation Specifications	81
6.3.3.3	Required vs. Addressable Specifications	83
6.3.4	Training	84
6.4	Preemption of Federal Law over State Law	84
6.5	Compliance	84
7	What are the Security Rule Safeguards?	85
7.1	Administrative Safeguards	85
7.1.1	Security Management Process	86
7.1.1.1	Risk Analysis - R	86
7.1.1.2	Risk Management - R	87
7.1.1.3	Sanction Policy - R	87
7.1.1.4	Information System Activity Review - R	87
7.1.2	Assigned Security Responsibility	88
7.1.3	Workforce Security	89
7.1.3.1	Authorization and/or Supervision - A	89
7.1.3.2	Workforce Clearance Procedure - A	90
7.1.3.3	Termination Procedures - A	90
7.1.4	Information Access Management	90
7.1.4.1	Isolating Health Care Clearinghouse Functions - R	91
7.1.4.2	Access Authorization - A	91

7.1.4.3	Access Establishment and Modification - A	92
7.1.5	Security Awareness and Training.....	92
7.1.5.1	Security Reminders - A	93
7.1.5.2	Protection from Malicious Software - A	93
7.1.5.3	Log-In Monitoring - A.....	93
7.1.5.4	Password Management - A.....	93
7.1.6	Security Incident Procedures.....	94
7.1.6.1	Response and Reporting - R	95
7.1.7	Contingency Plan	95
7.1.7.1	Data Backup Plan - R.....	96
7.1.7.2	Disaster Recovery Plan - R.....	96
7.1.7.3	Emergency Mode Operation Plan - R.....	96
7.1.7.4	Testing and Revision Procedures - A	96
7.1.7.5	Applications and Data Criticality Analysis	96
7.1.8	Evaluation	97
7.1.9	Business Associate Contracts and Other Arrangements.....	98
7.1.9.1	Written Contract or Other Arrangement.....	98
7.1.9.2	When BA contracts are not needed	99
7.2	Physical Safeguards	99
7.2.1	Facility Access Control	100
7.2.1.1	Contingency Operations - A	100
7.2.1.2	Facility Security Plan - A.....	101
7.2.1.3	Access Control and Validation Procedures - A.....	101
7.2.1.4	Maintenance Records - A	102
7.2.2	Workstation Use.....	102
7.2.3	Workstation Security.....	103
7.2.4	Device and Media Controls.....	104
7.2.4.1	Disposal - R.....	104
7.2.4.2	Media Re-use - R.....	105
7.2.4.3	Accountability - A.....	105

7.2.4.4	Data Backup and Storage - A.....	105
7.3	Technical Safeguards	106
7.3.1	Access Control	106
7.3.1.1	Unique User Identification - R	107
7.3.1.2	Emergency Access Procedures - R.....	107
7.3.1.3	Automatic Logoff - A	107
7.3.1.4	Encryption and Decryption - A.....	108
7.3.2	Audit Controls	108
7.3.3	Integrity	109
7.3.3.1	Mechanism to Authenticate Electronic Protected Health Information - A	109
7.3.4	Person or Entity Authentication.....	110
7.3.5	Transmission Security.....	110
7.3.5.1	Integrity Controls - A.....	111
7.3.5.2	Encryption - A	111
7.4	Organization, Policies and Procedures and Documentation Requirements	112
7.4.1	Business Associate Contracts or Other Arrangements	112
7.4.1.1	Business Associate Contracts - R	113
7.4.1.2	Other Arrangements - R.....	113
7.4.2	Requirements for Group Health Plans	114
7.4.2.1	Implementation Specifications - R.....	114
7.4.3	Policies and Procedures.....	115
7.4.4	Documentation.....	116
7.4.4.1	Time Limit - R.....	116
7.4.4.2	Availability - R.....	117
7.4.4.3	Updates - R.....	117
8	What is the Breach Notification Rule?.....	119
8.1	What is a Breach?	119
8.1.1	Disqualification of a breach.....	119
8.1.2	Exceptions to the definition of a breach	120
8.1.3	Unsecured PHI and Guidance	121

8.2	Breach Notification Requirements	122
8.2.1	Notice to the Individual	122
8.2.1.1	Responsible parties	122
8.2.1.2	Manner of providing notice	123
8.2.1.3	Timeframe to provide notice	123
8.2.2	Notice to the HHS Secretary.....	124
8.2.2.1	When to notify the HHS Secretary	124
8.2.2.2	How to notify the HHS Secretary	124
8.2.2.3	HHS responsibility to post breaches	125
8.2.3	Notice to the Media	125
8.2.3.1	When to notify the media.....	125
8.2.3.2	How to notify the media.....	125
8.2.3.3	Timeframe to notify the media.....	125
8.2.4	Notification by a BA.....	125
8.2.4.1	Timeframe to notify the CE.....	125
8.2.4.2	How to notify the CE	126
8.2.4.3	Additional notification responsibilities.....	126
8.2.5	Burden of Proof	126
8.2.6	Administrative Requirements	126
9	How is HIPAA compliance enforced?.....	129
9.1	HIPAA Enforcement Process.....	129
9.1.1	Complaints.....	130
9.1.1.1	Complaint Intake and Review.....	131
9.1.1.2	Complaint Investigation	133
9.1.1.3	Complaint Closure.....	133
9.1.2	Compliance Audits.....	133
9.1.2.1	Eligibility for Audit.....	134
9.1.2.2	Basis for Audit Selection.....	134
9.1.2.3	Selection Process.....	135
9.1.2.4	Audit Process	135

9.1.2.5	Audit Timeline	136
9.1.2.6	Post-Audit.....	136
9.1.3	Compliance Reviews.....	136
9.2	OCR Closure of Cases.....	137
9.2.1	Complaint resolved after intake & review	137
9.2.2	Complaint technical assistance provided.....	137
9.2.3	No Violation.....	137
9.2.4	Corrective Action Obtained	138
9.2.4.1	Resolution Agreements.....	138
9.2.5	Other closures of cases	139
9.3	Penalties.....	139
9.3.1	Civil Money Penalties	139
9.3.2	Criminal Penalties.....	142
9.4	Enforcement Statistics.....	142
10	What is the Administrative Simplification Rule?.....	143
10.1	Transactions Standard	143
10.1.1	What is a transaction?.....	143
10.1.2	Standard Transaction.....	143
10.1.2.1	ASC x12N.....	144
10.1.2.2	NCPDP.....	144
10.2	Codes Set Standard.....	145
10.2.1	About Code Sets	145
10.2.2	HIPAA Code Sets.....	145
10.2.2.1	International Classification of Diseases, 10th edition (ICD-10).....	145
10.2.2.2	Health Care Common Procedure Coding System (HCPCS)	145
10.2.2.3	Current Procedure Terminology (CPT)	146
10.2.2.4	Code on Dental Procedures and Nomenclature (CDT).....	146
10.2.2.5	National Drug Codes (NDC)	147
10.3	Employer Identifier Standard.....	147
11	Conclusion.....	149

12	Our Five Stage Process for HIPAA Compliance	151
12.1	Stage 1: Identify your team and set your objectives & scope	151
12.1.1	Action 1A: Appoint a HIPAA Compliance Officer and their team.....	152
12.1.2	Action 1B: Define the roles and responsibilities of each member in the HIPAA compliance team.....	152
12.1.3	Action 1C: Create a HIPAA documentation repository	153
12.1.4	Action 1D: Promote a culture of protecting patient privacy and securing health Information	153
12.2	Stage 2: Assess your current system & policies and identify gaps & risks	154
12.2.1	Action 2A: Document your current process and archive your records.....	154
12.2.2	Action 2B: Perform and document an Initial Risk Analysis.....	154
12.3	Stage 3: Determine corrective and preventative actions.....	155
12.3.1	Action 3A: Develop an Action Plan	156
12.3.2	Action 3B: Develop a Risk Management Plan	156
12.3.3	Tips for CAPAs.....	157
12.3.4	Action 3C: Evaluate Residual Risk Level	157
12.4	Stage 4: Implement new processes, policies and systems.....	160
12.4.1	Action 4A: Implement Written Policies and Procedures.....	160
12.4.2	Action 4B: Implement your Corrective and Preventative Actions.....	161
12.4.3	Action 4C: Educate and train your workforce	161
12.4.3.1	Frequency of Workforce Training	162
12.4.3.2	Updating Workforce Training	162
12.4.4	Action 4D: Communicate your Privacy and Security Practices	163
12.4.4.1	Tips when communicating with patients	163
12.4.5	Action 4E: Update your Business Associate Contracts and Listing.....	164
12.5	Stage 5: Evaluate, monitor and update as needed	164
12.5.1	Action 5A: Evaluate the effectiveness of your Privacy and Security infrastructure... 165	
12.5.1.1	Considerations for an internal assessment.....	165
12.5.2	Action 5B: Monitor how your PHI and ePHI are used	165
12.5.2.1	Considerations for monitoring capabilities:.....	166
12.5.3	Action 5C: Update Privacy and Security practices as necessary.....	167

12.6	Conclusion.....	167
13	Basics of Risk Analysis and Management.....	169
13.1	Important Definitions to Understand.....	169
13.2	Risk Analysis Process.....	170
13.2.1	Identify the scope of the analysis	171
13.2.2	Gather data	171
13.2.3	Identify and document potential risks	171
13.2.4	Assess current security measures.....	172
13.2.5	Determine the probability and severity of risk occurrence.....	172
13.2.5.1	Qualitative Rating	173
13.2.5.2	Quantitative Rating.....	173
13.2.6	Determine the Level of Risk	173
13.3	Risk Management Process	174
13.3.1	Develop and Implement a Risk Management Plan	175
13.3.2	Implement Security Measures.....	176
13.3.3	Evaluate and Maintain Security Measures.....	177
13.4	In Summary.....	178
14	Acronyms and Abbreviations.....	179
15	Security Safeguards Matrix.....	181
15.1	Administrative Safeguards.....	181
15.2	Physical Safeguards.....	182
15.3	Technical Safeguards	183
15.4	Organizational, Policies, Procedures and Documentation Requirements	184
16	Enforcement Statistics.....	185
16.1	Enforcement Highlights.....	185
16.2	Referrals to DOJ	187
16.3	Complaints Received by Calendar Year.....	187
16.4	Status of All Complaints	188
16.5	Total Investigated Resolutions.....	189
16.6	Investigated Resolutions by Year.....	190

16.7	Audit Results by Year	190
16.7.1	Non-Breach Audit Results.....	191
16.7.2	Breach Audit Results	191
16.8	Enforcement Results by State	192
16.9	Top 5 Issues in Investigated Cases Closed with Corrective Action by Year	195

Listing of Figures

Figure 1: Percentage of individuals who support electronic health records by whether they agree that health care providers are providing reasonable protections for EHRs.....	2
Figure 2: Percentage of individuals who support electronic health information exchange by whether they agree that health care providers are providing reasonable protections for EHRs.....	3
Figure 3: Percentage of individuals who have withheld information from their provider due to privacy or security concerns.....	5
Figure 4: Relationship between ACE and OHCA	22
Figure 5: Two methods to achieve de-identification in accordance with HIPAA Privacy Rule	28
Figure 6: Relationship between safeguards, standards, and implementation specifications	82
Figure 7: HIPAA OCR Complaint Handling Process.....	131
Figure 8: Total Complaints by Year	187
Figure 9: Status of All Complaints	188
Figure 10: Total Investigated Resolutions	189
Figure 11: Investigated Resolutions by Year.....	190

Listing of Tables

Table 1: Covered Entities	12
Table 2: 18 Identifiers of PHI [45 CFR 164.514].....	31
Table 3: Public interest and benefit activities in which PHI use and disclosure is permitted	38
Table 4: Forms and Formats of PHI conveyed to an individual.....	53
Table 5: Manners in which an individual may request their PHI	54
Table 6: Calculating fees to fulfill PHI access requests.....	56
Table 7: Examples of Personal Representatives.....	65
Table 8: Examples of exceptions to Parent Personal Representation.....	66
Table 9: Privacy Rule and Security Rule Key Differences	77
Table 10: Security Rule Definitions of Integrity, Availability, and Confidentiality	79
Table 11: Explanation of Policy and Procedure.....	116
Table 12: Civil Money Penalties Structure	141
Table 13: Risk Analysis and Management Important Terms and Definitions.....	170
Table 14: Risk Level Matrix.....	174
Table 15: Acronyms and Abbreviations	180
Table 16: Enforcement Results by State.....	194
Table 17: Top 5 Issues in Investigated Cases Closed with Corrective Action by Year.....	196

Sample for illustrative purposes
Actual product will be latest available version