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 - A 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 Controls 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 Transactions 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
17 HIPAA and Reproductive Health 197
17.1 HIPAA Privacy Rule and Reproductive Health Care Provisions 197
17.2 Definitions 198
17.2.1 Reproductive Health Care 198
17.2.2 Reproductive Health Information 199
17.2.3 Lawful 199
17.2.4 Seeking, obtaining, providing, or facilitating 200
17.3 Does the Final Rule apply to all healthcare providers? 200
17.4 Guidelines for Permissible Use/Disclosure 201
17.5 Prohibited Uses and Disclosures 201
17.6 Responding to a Request for Reproductive Health Information 202
17.6.1 Determining Legal Basis of a Request 203
17.6.2 Obtaining a Valid Attestation 203
17.6.2.1 Circumstances where attestation is required 203
17.6.2.2 Attestation form requirements 203
17.6.2.3 Restrictions 204
17.6.3 Determining Lawfully Provided Care 204
17.6.3.1 Rule of Applicability i.e. who makes the determination 205
17.6.3.2 Reasonability Determination 205
17.6.3.3 Presumption 205
17.6.4 Fulfilling a Request 206
17.7 Disclosures to Law Enforcement 207
17.8 Clarification of Personal Representative Qualifications 207
17.9 Accounting of Disclosures 208
17.10 Breach Notification 208
17.11 Business Associates 208

18 HIPAA and Part 2 209
18.1 What is Part 2? 209
18.2 What entities must comply with Part 2 requirements? 209
18.3 Part 2 Requirements 210
18.3.1 Patient consent 210
18.3.2 Other uses and disclosures 210
18.3.3 Safe harbor for investigative agencies 211
18.3.4 Segregation of information 211
18.3.5 Specific changes to the NPP required for Part 2 programs 211
18.3.6 Penalties 212
18.3.7 Breach Notification 212

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 140
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

This page intentionally left blank

1 What is HIPAA?

Introduction to the Health Insurance Portability and Accountability Act of 1996

1.1 Importance of Privacy and Security

In a digital age where patient information is increasingly stored and shared by health care providers and associated companies, it is important to ensure that an individual's health information is private and secure.

A lack of a robust privacy and security plan for protected health information may lead to the following:

1. A negative perception by the public that their information is not confidential or accurate in your institution
2. A negative financial impact to your institution due to that negative perception
3. Individuals withholding their information leading to potentially life-threatening consequences
4. A risk of an information breach, for example, through a cyber-attack

If individuals do not trust that their Electronic Health Records (EHRs) or how Health Information Exchanges (HIEs) are conducted are safe, then their support and willingness to utilize such services are diminished which can impact your ability to utilize these tools.

1.1.1 Impact public perception of privacy and security can have on support for EHRs and HIEs

In 2012, the Office of the National Coordinator for Health Information Technology (ONC) conducted a national telephone survey focusing on the audience's attitudes towards the privacy and security of their health information when utilized electronically via EHRs and HIEs[1]. Some of the outcomes of the survey are listed below.

1 http://www.healthit.gov/sites/default/files/022414_hit_attitudesaboutprivacydatabrief.pdf.

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*

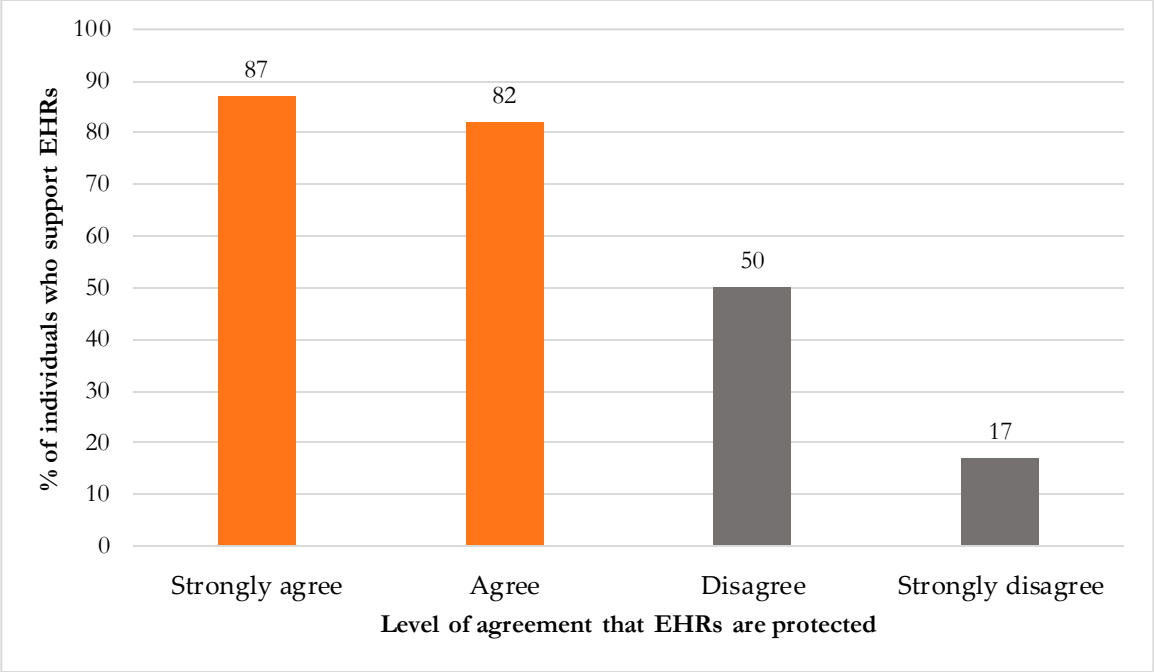

Figure 1: Percentage of individuals who support electronic health records by whether they agree that health care providers are providing reasonable protections for EHRs[2]

Explanation of Chart

In the survey, individuals were divided into 4 categories based on their level of agreement on whether electronic health records have reasonable protections put in place by their healthcare providers. In each category, the individuals were then asked if they supported the use of electronic health records. The percentage of individuals that were in support of the use of electronic health records is shown.

2 Source: 2012 Consumer Survey of Attitudes Toward the Privacy and Security Aspects of Electronic Health Records and Health Information Exchange

Key Takeaways

- The less an individual felt their electronic health records had reasonable protections put in place by their healthcare providers, the less they were in support of the use of electronic health records.
- 83% of individuals that strongly disagreed that their electronic health records were sufficiently protected were **not** in support of the use of electronic health record technology.

1.1.1.2 Individuals are less likely to support Health Information Exchange when they do not believe their information is protected

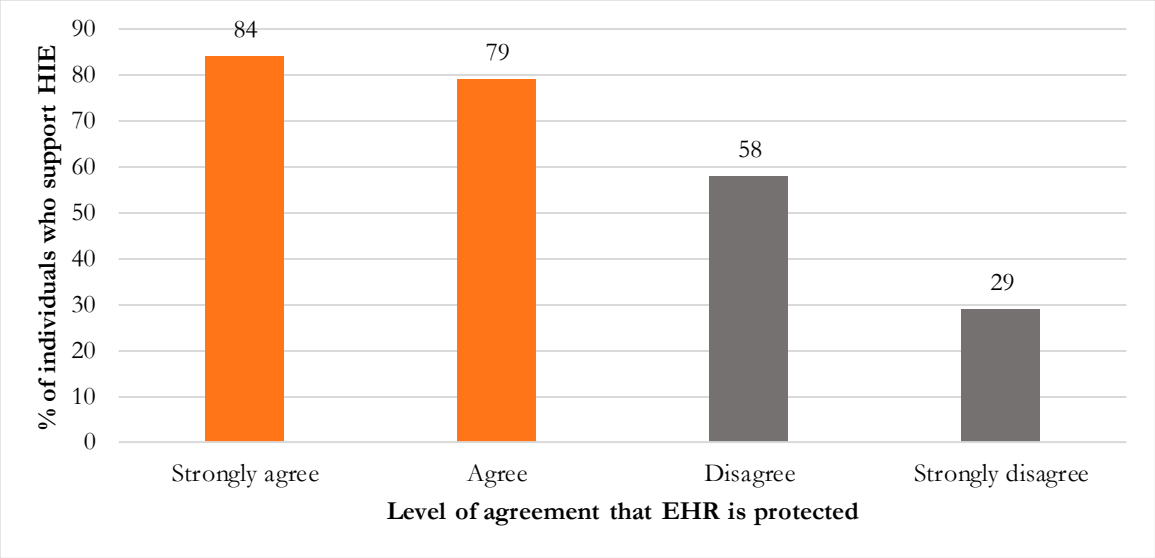

Figure 2: Percentage of individuals who support electronic health information exchange by whether they agree that health care providers are providing reasonable protections for EHRs[3]

Explanation of Chart

In the survey, individuals were divided into 4 categories based on their level of agreement on whether electronic health records have reasonable protections put in

3 Source: 2012 Consumer Survey of Attitudes Toward the Privacy and Security Aspects of Electronic Health Records and Health Information Exchange

place by their healthcare providers. In each category, the individuals were then asked if they supported the use of electronic exchange of their health information (HIE). The percentage of individuals that were in support of the use of electronic health information exchange is shown.

Key Takeaways

- The less an individual felt their electronic health records had reasonable protections put in place by their healthcare providers, the less they were in support of the use of electronic health information exchange.
- 71% of individuals that strongly disagreed that their electronic health records were sufficiently protected were **not** in support of the use of electronic health information exchange (HIE).

1.1.1.3 Individuals are more likely to withhold information if they have privacy or security concerns

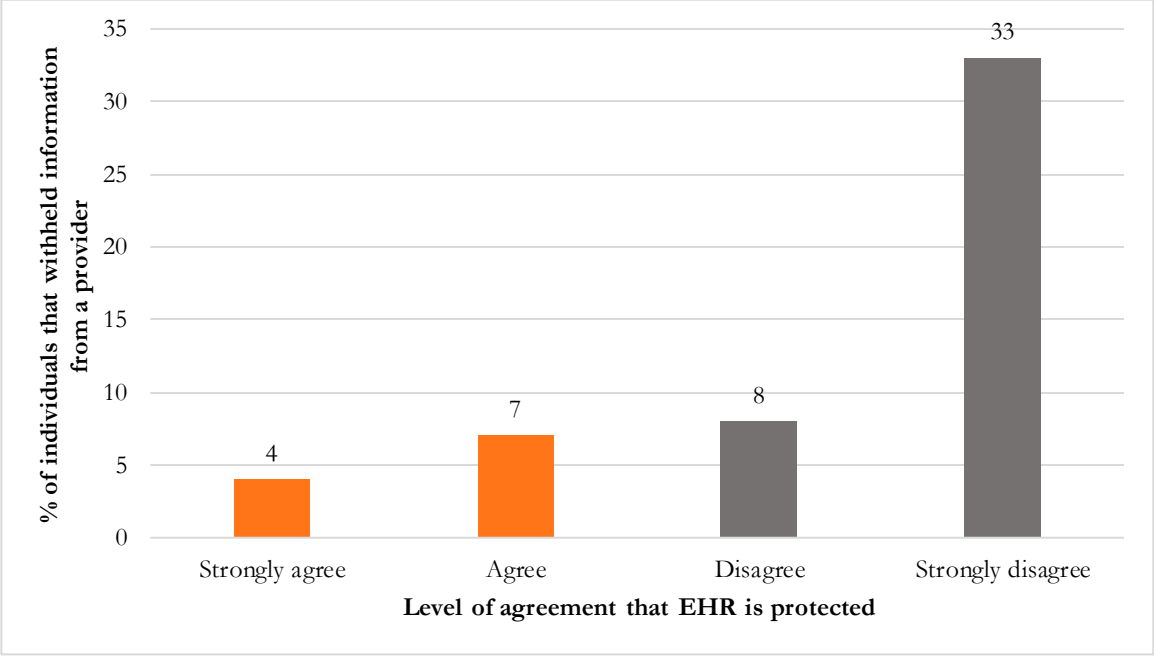

Figure 3: Percentage of individuals who have withheld information from their provider due to privacy or security concerns[4]

Explanation of Chart

In the survey, individuals were divided into 4 categories based on their level of agreement on whether electronic health records have reasonable protections put in place by their healthcare providers. In each category, the individuals were then asked if they withheld information from their healthcare provider. The percentage of individuals that have withheld information from their healthcare provider is shown.

Key Takeaways

- The less an individual felt their electronic health records had reasonable protections put in place by their healthcare providers, the more they withheld information from their healthcare provider.
- 33% of individuals that strongly disagreed that their electronic health records were sufficiently protected reported they had withheld information from their healthcare provider.

1.1.2 Protected health information privacy and security are important… now what?

In order to avoid the risks listed above and achieve more positive health outcomes, protected health information must be handled in such a way that it:

1. Ensures the privacy, security and integrity of the information
2. Gives the perception to the public that the information is private, secure and of good integrity
3. Is reasonably protected from the possibility of an information breach

4 Source: 2012 Consumer Survey of Attitudes Toward the Privacy and Security Aspects of Electronic Health Records and Health Information Exchange

4. Is accessible to the owner of the information i.e. the patient or their authorized representative

The Health Information Portability and Accountability Act of 1996 or HIPAA was put in place in order to achieve these goals.

1.2 Background and History of HIPAA Regulations

1.2.1 The Health Insurance Portability and Accountability Act of 1996

HIPAA or the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, was enacted on August 21, 1996 and originally established to require the Department Health and Human Services (see **1.3.1 Department of Health and Human Services**) to adopt national standards for electronic health care transactions per the Administrative Simplification Rule (see **10 What is the Administrative Simplification Rule?**).

However, over time and with the advancements in electronic technology in healthcare, Congress recognized the need to introduce protections for the privacy and security of health information and the rights for the individuals that are the subject of that information. In order to establish these protections and rights, certain rules were published over a period of years and are explained below.

1.2.2 The Privacy Rule

The *Standards for Privacy of Individually Identifiable Health Information* or Privacy Rule established a set of national standards for the protection of certain health information (see **3 What information is protected by HIPAA?**) as well as established an individual's rights with regards to their health information.

In 1999, the Department of Health and Human Services (HHS) developed the Privacy Rule and released it for public comment. After receiving over 52,000 public comments, it published the final regulation on December 28, 2000.

Following that in March 2002, HHS proposed modifications to the Privacy Rule and released the modifications for public comment. After receiving over 11,000 comments, these final modifications were published on August 14, 2002.

For more information on the Privacy Rule, see **4 What is the Privacy Rule?**.

1.2.3 The Security Rule

The *Security Standards for the Protection of Electronic Protected Health Information* or Security Rule established national standards for the security of **electronic** protected health information, distinguishing itself from the Privacy Rule which protects all types of protected health information (oral, written and electronic – see **3 What information is protected by HIPAA?**).

HIPAA tasked the Secretary with issuing security regulations for measures to protect the integrity, confidentiality, and availability of ePHI that is maintained or transmitted by Covered Entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The Department received over 2,000 public comments. On February 20, 2003, the final regulation known as the Security Rule was published.

The Security rule specifies a series of administrative, technical, and physical security safeguards (see **7 What are the Security Rule Safeguards?**) for Covered Entities and their Business Associates (see **2 Who must comply with HIPAA?**) to assure the integrity, availability, and confidentiality of electronic protected health information.

Compliance with the Security rule was required as of April 20, 2005, for most entities covered by HIPAA, and by September 23, 2013, for their business associates. The authority to administer and enforce the Security Rule was transferred to the Office for Civil Rights (see **1.3.2 Office for Civil Rights**) on July 27, 2009.

For more information on the Security Rule, see **6 What is the Security Rule?**.

1.2.4 The Enforcement Rule

The Enforcement Rule is what grants the Office for Civil Rights that authority to enforce HIPAA provisions and to impose financial penalties on entities violating HIPAA provisions.

For more information on the Enforcement Rule, see **9 How is HIPAA compliance enforced?**.

1.2.5 The Omnibus Rule

In January 2013, HIPAA was updated with the final Omnibus Rule. The Omnibus Rule included changes to the Security Rule (see **6 What is the Security Rule?**) and Breach Notification Rule (see **8 What is the Breach Notification Rule?**). The greatest changes were in regard to requiring Business Associates to comply with the Security Rule and Breach Notification Rule as well.

1.2.6 The Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities and their business associates to notify the Secretary, individuals, and in some cases, the media, regarding breaches of unsecured protected health information. Compliance with the standards was required as of September 23, 2009.

For more information on the Breach Notification Rule, see **8 What is the Breach Notification Rule?**.

1.2.7 The HITECH Act

The *Health Information Technology for Economic & Clinical Health Act* of 2009 or HITECH was signed into law on February 17, 2009. Its purpose was to promote the adoption and meaningful use of health information technology.

Subtitle D of the HITECH Act establishes several provisions that strengthen the civil and criminal enforcement of HIPAA among addressing other privacy and security concerns such as:

- Creating a tiered penalty system (see Table 12: Civil Money Penalties Structure)
- Establishing a maximum penalty amount of $1.5 million for all violations of an identical provision (see *Table 12: Civil Money Penalties Structure*)
- Permitting the imposition of penalties even if a CE was not aware and with the exercise of reasonable diligence would not have known about a violation

- Permitting a 30-day grace period in which a violation may be corrected without the imposition of a penalty so long as the violation was not due to willful neglect

1.3 Governing Bodies

1.3.1 Department of Health and Human Services

From the Department of Health and Human Services (HHS) website:

> *"It is the mission of the U.S. Department of Health & Human Services (HHS) to enhance and protect the health and well-being of all Americans. We fulfill that mission by providing for effective health and human services and fostering advances in medicine, public health, and social services."*

While HHS was responsible for the introduction of HIPAA legislation, it is enforced by its agency, the Office for Civil Rights.

1.3.2 Office for Civil Rights

The Office for Civil Rights enforces federal laws that prohibit discrimination and provides health information privacy rights. It does this by:

- Teaching health and social service workers about civil rights, health information privacy, and patient safety confidentiality laws
- Educating communities about civil rights and health information privacy rights
- Investigating civil rights, health information privacy, and patient safety confidentiality complaints to identify discrimination or violation of the law and acting to correct problems.[5]

5 https://www.hhs.gov/ocr/about-us/index.html

This page intentionally left blank

2 Who must comply with HIPAA?

Covered Entities and Business Associates

The HIPAA Rules apply to **Covered Entities** and **Business Associates**. In the context of HIPAA, Covered Entities and Business Associates can encompass a wide variety of different groups. Let's look into each.

> Note: If an organization does not meet the definition of a Covered Entity or business associate as explained below, they are not required to comply with HIPAA regulations.
>
> See 45 CFR 160.103 for more information on Business Associates and Covered Entities.

2.1 Covered Entities

A Covered Entity (CE) is an individual, business or agency that acts as a health care provider, health plan or health care clearinghouse. Examples of each of these CEs can be found in the below table.

Covered Entities		
Covered Health Care Providers	**Health Plans**	**Health Care Clearinghouses**
Providers who submit HIPAA transactions, like claims, electronically are covered. These providers include, but are not limited to:	• Health insurance companies • HMOs, or health maintenance organizations	Clearinghouses include organizations that process nonstandard health information to conform to standards for data content or format, or vice versa,

Covered Entities		
• **Doctors** • **Clinics** • **Psychologists** • **Dentists** • **Chiropractors** • **Nursing homes** • **Pharmacies**	• Employer-sponsored health plans • Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs	on behalf of other organizations.

Table 1: Covered Entities

Different types of CEs include:

- *Covered Health Care Providers* - Any provider of medical or other health care services or supplies who transmits any health information **in electronic form** about a transaction for which HHS has adopted a standard.
- *Health Plans* - Any individual or group plan that provides or pays the cost of health care (e.g. a health insurance issuer and the Medicare and Medicaid programs).
- *Health Care Clearinghouses* - A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa.

2.1.1 Providers

The first types of CEs are providers **who submit health information related transactions electronically**. These transactions include:

- Health claims and equivalent encounter information
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan

- Health care payment and remittance advice
- Health plan premium payments and remittance advice
- Health plan premium payments
- Health claim status
- Referral certification and authorization
- Coordination of benefits

Any health care provider that bills electronically is a CE

Simply using electronic technology like email does not make a health care provider a CE; in order for that to be the case, the transmission must be in connection with a standard transaction above. Providers covered under HIPAA can be either service providers or medical/health care providers, including, but are not limited to:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing homes
- Pharmacies

2.1.2 Health Plans

For HIPAA purposes, health plans include individual and group health plans that provide or pay for medical care, such as:

- Health insurance companies including health, dental, vision and prescription drug insurers
- HMOs, or health maintenance organizations
- Employer-sponsored health plans, government and church-sponsored health plans, and multi-employer health plans

- Government programs that pay for health care, like Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers and military and veterans' health programs
- Long-term care insurers (excluding nursing home fixed-indemnity policies)

There are exceptions:

- A group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a Covered Entity.
- Government-funded programs whose principal purpose is not providing or paying the cost of health care, such as the food stamps program.
- Government-funded programs whose principal activity is directly providing health care, such as a community health center or the making of grants to fund the direct provision of health care.
- Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. If an insurance entity has separable lines of business, one of which is a health plan, the HIPAA regulations apply to the entity with respect to the health plan line of business.

2.1.3 Clearinghouses

Clearinghouses include organizations that process nonstandard health information to conform to standards for data content or format, or vice versa, on behalf of other organizations. In most cases, health care clearinghouses will receive protected health information (PHI) only if they are providing processing services to a health plan or provider as a business associate (BA, which will be defined later in this chapter). In these instances, only specific provision of the HIPAA regulation will apply to the health care clearinghouse's uses and disclosures of PHI. Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

2.2 Business Associates

A CE may work with an external Business Associate (BA), which can be a person or entity outside of the CE's workforce (e.g. a member of the practice staff), to perform certain services that may involve access to, use of, or disclosure of PHI. These services may include:

- claims processing or administration
- data analysis
- utilization review
- quality assurance
- billing
- benefit management
- practice management
- repricing

If a Covered Entity works with a business associate to carry out its activities, there must be a **Business Associate Contract** that requires the BA to comply with HIPAA regulations.

Some other examples of business associate services are:

- legal
- actuarial
- accounting
- consulting
- data aggregation
- management
- administrative
- accreditation
- financial

The only time service providers are considered BAs is when their service involves the use or disclosure of PHI. Examples of BAs include:

- Health Information Organizations or Exchanges (HIOs/HIEs)
- Online prescription gateways
- Third-party administrator that assists a health plan with claims processing
- Consultant that performs utilization reviews for a hospital
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A pharmacy benefits manager that manages a health plan's pharmacist network.
- Independent medical transcriptionist that provides transcription services to a physician
- Any other person who has access to PHI (e.g. data transmission)
- Note: a CE can be a BA of another CE, for example in the case of covered health care providers, health care clearinghouses or health plans.

Who is or is not a BA?

Do they have access to PHI?

If yes, they are a BA.

If not, they are not a BA.

If a CE does engage a BA to help carry out its health care activities and functions, there must be a written contract between the two that establishes what specifically the BA has been engaged to do and requires the BA to comply with HIPAA regulation.

2.2.1 Business Associate Contracts

A CE's contract or other written arrangement with its BA must contain certain elements. For example, the contract must:

- Describe the permitted and required uses of PHI by the BA
- Provide that the BA will not use or further disclose the PHI other than as permitted or required by the contract or as required by law
- Require the BA to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.

Where a CE knows of a material breach or violation by the BA of the contract or agreement, the former is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a CE is required to report the problem to the Department of HHS Office for Civil Rights OCR (see **Chapter 8 What is the Breach Notification Rule?**).

There are exceptions, which allow the CE to not have a contract or other written agreement with a BA for the use and disclosure of PHI:

- Disclosures by a Covered Entity to a health care provider for treatment of the individual. For example:
    - A hospital is not required to have a BA contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
    - A physician is not required to have a BA contract with a laboratory as a condition of disclosing PHI for the treatment of an individual.
    - A hospital laboratory is not required to have a BA contract to disclose PHI to a reference laboratory for treatment of the individual.
- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures.
- The collection and sharing of PHI by a health plan that is a public benefits program, such as Medicare, and an agency other than the agency administering the health plan, such as the Social Security Administration, that collects PHI to determine eligibility or enrollment, or determines eligibility or enrollment, for the government program, where the joint activities are authorized by law.

- When a health care provider discloses PHI to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a CE, and not as the BA of the other.
- With persons or organizations (e.g. janitorial service or electrician) whose functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all.
- With a person or organization that acts merely as a conduit for PHI, for example, the US Postal Service, certain private couriers, and their electronic equivalents.
- Among CEs who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA (see **2.3.3 Organized Health Care Arrangement**).
- Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA with respect to the individuals they jointly serve or have served. Thus, these Covered Entities are permitted to share PHI that relates to the joint health care activities of the OHCA.
- Where one CE purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the CE purchases the insurance benefits, and when the CE submits a claim to the insurer and the insurer pays the claim.
- To disclose PHI to a researcher for research purposes, either with patient authorization, pursuant to a waiver, or as a limited data set. Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of BA (see **2.2 Business Associates**), the researcher is not a BA of the CE, and no BA agreement is required.
- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or

processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums, since it is only providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the CE.

2.2.2 Business Associate Listing

Covered entities are recommended to maintain a listing of their Business Associates with the following information:

- Business Associate Name
- Type of Service(s) provided
- First Point of Contact Title
- First Point of Contact First Name
- First Point of Contact Last Name
- First Point of Contact Address
- First Point of Contact Address Continued (if needed)
- First Point of Contact City
- First Point of Contact State
- First Point of Contact Zip
- First Point of Contact Phone
- First Point of Contact Phone Extension (if needed)
- First Point of Contact Fax
- First point of Contact Email
- Second Point of Contact Title
- Second Point of Contact First Name
- Second Point of Contact Last Name

- Second Point of Contact Address
- Second Point of Contact Address Continued (if needed)
- Second Point of Contact City
- Second Point of Contact State
- Second Point of Contact Zip
- Second Point of Contact Phone
- Second Point of Contact Phone Extension (if needed)
- Second Point of Contact Fax
- Second point of Contact Email
- Website URL

2.3 Special Cases

2.3.1 Hybrid Entity

A CE that is a single legal entity and that conducts both covered and non-covered functions (covered functions are activities that make an entity a CE) is permitted to be a "hybrid entity." In order to be a hybrid entity, the CE must designate in writing its operations that perform covered functions as one or more "health care components." **Once this designation is made, most of the requirements of the Privacy Rule will only apply to the health care components.** If a CE doesn't make this designation, the Privacy Rule will apply to all its functions.

For example, a university may choose to be a hybrid entity if it has a research laboratory that functions as a health care provider and utilizes electronic transactions that are covered by an HHS standard. In this case, the research laboratory specifically is subject to HIPAA regulations.

2.3.2 Affiliated Covered Entity (ACE)

By law, CEs that are affiliated by common control or ownership may classify themselves and their health care components in writing as a single CE for compliance with HIPAA regulations.

Under this affiliation, the organizations need only develop and disseminate one notice of privacy practices, comply with one set of policies and procedures, appoint one privacy official, administer common training programs, use one business associate contract, etc.

An affiliated CE that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.

For example, a dental practice with multiple locations or sites that are under common ownership or control would be considered an ACE and subject to HIPAA as a **single** CE.

2.3.3 Organized Health Care Arrangement (OHCA)

According to HIPAA regulations, relationships among CEs that share PHI to manage and benefit their common enterprise are identified as "organized health care arrangements." CEs in such an arrangement can share PHI with each other for the arrangement's joint health care functions.

For example, an academic medical center often includes university-affiliated physicians and a hospital or health system. Typically, the university is a separate legal entity, but the patients are treated by the faculty within the hospital or health system.

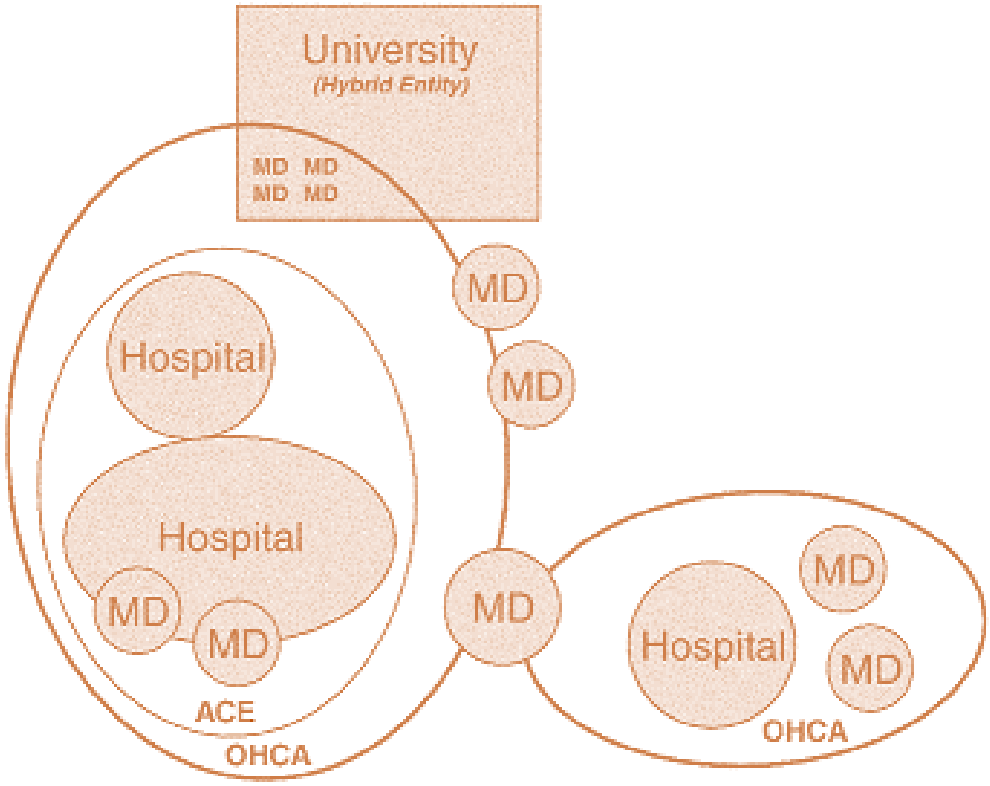

Figure 4: Relationship between ACE and OHCA[6]

2.3.4 Covered Entities with Multiple Covered Functions

When a CE performs multiple covered functions, it must make sure that each function is performed in compliance with HIPAA regulations according to the provisions applicable to each function. The CE cannot use or disclose PHI of a particular individual between functions if the individual is only involved with one of the functions.

For example, if a CE's health care provider functions have access to someone's PHI, the information cannot be shared with the CE's health plan functions unless the individual in question is directly involved with the latter function.

6 http://bok.ahima.org/doc?oid=60011#.WYNl74jys2w

2.3.5 Group Health Plan Disclosure to Plan Sponsors

The following information can be shared with the "plan sponsor" (the employer, union, or other employee organization that sponsors and maintains the groups health plan) by a group health plan and the insurer or HMO offered by the plan:

- Enrollment or disenrollment information regarding the group health plan or a health insurer or HMO offered by the plan
- Summary health information for the plan sponsor to use to obtain premium bids for providing health insurer coverage through the group health plan or to modify, amend or terminate the group health plans. Summary health information summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five-digit zip code (though it does not need to be qualify as de-identified protected health information).
- PHI of the health plan's enrollees for the plan sponsor to perform administrative functions related to the plan. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the PHI, including that the plan sponsor will not use or disclose the PHI for any employment-related action or decision or in connection with any other benefit plan.

This page intentionally left blank

3 What information is protected by HIPAA?

Definition of protected health information (PHI) and electronic protected health information (ePHI)

Oral protected health information

Health information that is communicated orally is covered under HIPAA.

For example:

Some small clinics within wholesale department stores may not have a separate waiting area and patient meeting room where protected health information can be discussed in private. In such clinics, HIPAA requires that patients waiting to be seen wait away from where active discussions are occurring (which in some cases may be outside the clinic itself).

Patient information that is protected by HIPAA is referred to as "protected health information" or PHI. This includes most information that can be used to identify an individual and can be in any form – including electronic (also known as "electronic protected health information or ePHI, paper or information that is communicated orally.

If you are a Covered Entity (CE) or business associate (BA), you are required to comply with HIPAA regulations regarding the protection of PHI or ePHI.

Some examples of this information include:

- Health history – an individual's past, present, or future physical health, mental health, other conditions
- Demographic information that directly identifies an individual or can reasonably be used to identify an individual

For example, an electronic hospital invoice is considered ePHI if the information contained includes a patient's name or any other identifying information.

- Treatment plans or health care provided to an individual in the past, currently being provided or will be provided
- Payment information regarding treatment done in the past, present or that will be done in the future

Unauthorized filming for television series "NY Med" results in settlement

In April 2016, the Department of Health and Human Services, Office for Civil Rights (OCR) announced that it reached a $2.2 million settlement with New York Presbyterian Hospital (NYP) for the unauthorized disclosure of two patients' PHI to film crews and staff during the filming of "NY Med", an ABC television series, without first obtaining authorization from the patients.

OCR found that NYP failed to safeguard protected health information and allowed ABC film crews free access to its health care facility, effectively creating an environment where PHI could not be protected.

In addition to a settlement, OCR will monitor NYP for two years as part of the settlement agreement, helping ensure that NYP will remain compliant with its HIPAA obligations while it continues to provide care for patients.

Takeaway: Unauthorized filming by members of the media of individuals receiving medical care violates HIPAA rules which prevent disclosure of PHI, ***including images****.*

3.1 Exclusions to information covered by HIPAA

There are exceptions to individually identifiable health information for which HIPAA rules do not apply. These exceptions include:

- Records covered by the Family Educational Rights and Privacy Act (FERPA)[7] (see 3.1.1 Where FERPA and HIPAA Intersect)
- Employment records that a CE maintains in the capacity of an employer
- De-identified health information

7 20 United States Code (USC) 1232g; 45 Code of Federal Regulations (CFR) 160.103; http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf

3.1.1 Where FERPA and HIPAA Intersect

FERPA is a Federal law that protects the privacy of students' educational records at educational institutions subject to FERPA. HIPAA excludes educational records that are subject to FERPA from its coverage.

An educational institution is not required to comply with HIPAA if:

1. The educational institution is not considered a CE i.e. does not execute a covered transaction. (See **2.1 Covered Entities** for more information on CEs and covered transactions).
2. The educational institution is a CE but does not have PHI. For example, a school may employ a health care provider that conducts covered transactions electronically, such as transmitting claims to a health plan for payment (this makes them a CE). However, if the health information is maintained only in education records, HIPAA does not consider that information PHI and therefore does not require the institution to comply with HIPAA law.

3.1.2 De-identified health information

De-identified information is one that neither identifies nor provides a reasonable basis to identify an individual. There are **no** restrictions on the use or disclosure of de-identified health information.[8]

There are two ways to de-identify information:

1. a formal determination by a qualified statistician, or
2. the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the remaining information could not be used by the CE to identify the individual.[9]

8 45 C.F.R. 164.502(d)(2), 164.514(a) and (b).

9 45 C.F.R. § 164.514(b).

A BA may be used to de-identify PHI.

Figure 5: Two methods to achieve de-identification in accordance with HIPAA Privacy Rule, elaborates on the two methods by which health information can be designated as de-identified.

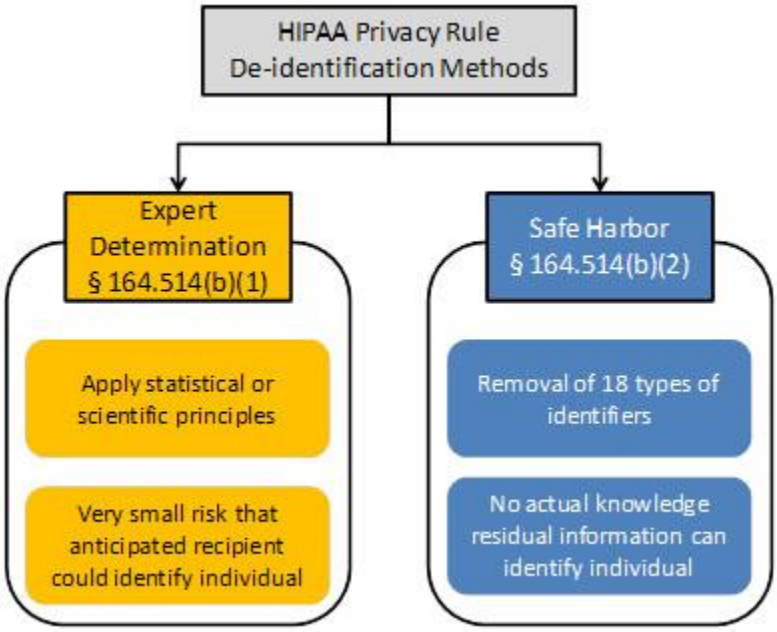

Figure 5: Two methods to achieve de-identification in accordance with HIPAA Privacy Rule[10]

3.1.2.1 Expert Determination

In this method, a person with appropriate knowledge and experience with accepted statistical and scientific principles and methods renders PHI and ePHI not individually identifiable. Using these principles and methods, this person is able to determine that the risk of identifying an individual with the residual information is very low and can document the justification of such a determination.

There are no specific credentials for designating who is an "expert" at rendering health information de-identified. Relevant expertise may be gained through various routes of

10 https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

education and experience. As long as a professional's experience and methodology are reasonably justifiable, their use is acceptable form an OCR perspective.

Methods that an expert may use to de-identify PHI include:

1. Suppressing patient values (e.g. removing specific identifiers such as age or ZIP code so as to make PHI non-unique to a patient)
2. Generalizing patient values (e.g. removing the last digit of a ZIP code to provide less granularity such as 1000* as opposed to 10001)
3. Perturbing the patient values (e.g. replacing the patient's actual age with another value +/- 5 years)

3.1.2.2 Safe Harbor

In this method, the CE must remove the following identifiers for the individual, as well as any relatives, employers, household members as applicable if their identifiers may be used to identify the individual.

#	Identifier
1	Names
2	All geographic subdivisions smaller than a state including street address, city, county, precinct, ZIP code, except if: • according to the Bureau of the Census, the geographic unit formed by combining all ZIP codes with the same initial three digits contains more than 20,000 people • the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3	All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age,

#	Identifier
	except that such ages and elements may be aggregated into a single category of age 90 or older
4	Telephone numbers
5	Fax numbers
6	Email addresses
7	Social Security Numbers
8	Health record numbers
9	Health plan beneficiary numbers
10	Account numbers
11	Certificate/license numbers
12	Vehicle identifiers and serial numbers, including license plate numbers
13	Device identifiers and serial numbers
14	Web Universal Resource Locators (URLs)
15	Internet Protocol (IP) addresses
16	Biometric identifiers, including finger prints and voice
17	Full-face photographs and any comparable images

#	Identifier
18	Any other unique identifying number, characteristic, or code, except as permitted as explained in **3.1.2.3 Re-identification**.

Table 2: 18 Identifiers of PHI [45 CFR 164.514]

3.1.2.3 Re-identification

The Privacy Rule permits the assignment of a unique code to the set of de-identified health information to permit re-identification by the CE.

If the CE or BA successfully undertook an effort to identify the subject of the de-identified information it maintained, the health information, since it is now related to a specific individual, would again be protected by the Privacy Rule (as it meets the definition of PHI). Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is also considered a disclosure of PHI.

A CE may assign a code or other means of record identification to allow information de-identified under this section to be re-identified provided:

1. **Derivation.** The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual
2. **Security.** The CE does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

3.1.2.4 Limited Data Set.

- A limited data set is PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed but may contain more identifiers than de-identified data (see *Table*

2: 18 Identifiers of PHI [45 CFR 164.514]). A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the PHI within the limited data set.

4 What is the Privacy Rule?

Details of the standards for privacy of individually identifiable health information

The Privacy Rule essentially comprises of two mandates:

1. one sets the limits on the uses and disclosures that can be made of PHI (see 4 What is the Privacy Rule?)
2. and the other establishes patients' rights over their health information including the rights to obtain a copy of their health records and request corrections (see **5 What are a patient's rights to their health information?**)

The **Privacy Rule** is located at 45 CFR Part 160 and Subparts A and E of Part 164.

4.1 Use and disclosure of PHI

A major purpose of the Privacy Rule is to balance the need for protection of a patient's health information with its utility in health care. It achieves this by defining and limiting the circumstances in which a CE may use or disclose an individual's PHI. The Privacy Rule is designed to be both flexible and comprehensive to cover the wide variety of situations that may arise during the course of a patient's healthcare.

Defining Use and Disclosure per HIPAA

Use: sharing, employment, application, utilization, examination or analysis of PHI within the Covered Entity (CE)

Disclosure: release, transfer, provision of access to, or divulging in any other manner of PHI outside of the CE

A CE may not use or disclose PHI, except:

1. as the Privacy Rule permits or requires (see 4.1.1 Permitted Uses and Disclosures)
2. to individuals or their personal representatives specifically when they make a request for access, an account of disclosures or corrections (**see 5 What are a patient's rights to their health information?**

3. to HHS when it is undertaking a compliance investigation or review or enforcement action (see 9 How is HIPAA compliance enforced?).

4.1.1 Permitted Uses and Disclosures

A CE is permitted, but not required, to use and disclose PHI for the following purposes or situations. CEs may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make:

4.1.1.1 Treatment, Payment, Operations.

A CE may use and disclose PHI for its own treatment, payment, and operations. A CE also may disclose PHI to another CE in regard to their treatment, payment and/or operations* if both CEs have or had a relationship with the individual and the PHI pertains to the relationship.

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization. Obtaining "consent" (written permission from individuals to use and disclose their PHI for treatment, payment, and health care operations) is optional under the Privacy Rule for all CEs. The content of a consent form, and the process for obtaining consent, are at the discretion of the CE electing to seek consent.

Health care operations* are any of the following activities:

- Quality assurance
- Performance evaluation
- Review, compliance and audit preparedness
- specified insurance functions, such as underwriting, risk rating, and reinsuring risk
- business planning, development, management, and administration
- general administrative activities of the entity, including but not limited to: de-identifying PHI, creating a limited data set, and certain fundraising for the benefit of the CE

.

4.1.1.2 Uses and Disclosures with Opportunity to Agree or Object.

PHI may be disclosed with informal permission by asking the individual outright in a manner in which the individual has the opportunity to agree or object.

A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, and location in the provider's facility. The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name.

A CE also may rely on an individual's informal permission to disclose PHI to the individual's family, relatives, or friends, or to other persons whom the individual identifies. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a CE may rely on an individual's informal permission to use or disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death.

If an individual is incapacitated, the CE has the ability to exercise their professional judgement in the use and disclosure of PHI provided it is in the best interests of the individual.

4.1.1.3 Incidental Use and Disclosure.

HHS understands that during the course of health care, the potential exists for an individual's health information to be disclosed incidentally due to the nature of health care practices, communication and environments. e.g. a hospital visitor may overhear a provider's confidential conversation with a patient.

The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated in order to satisfy its standards. Provided the appropriate safeguards are put in place (see **7 What are the Security Rule Safeguards?**) and use and disclosure of PHI is limited to those permitted by the Privacy Rule, any incidental use or disclosure of PHI does not violate HIPAA.

Consider the following practices to minimize incidental use and disclosure of PHI:

1. Speaking quietly when publicly discussing a patient's condition with family members
2. Avoiding using patients' names in public areas
3. Posting signs to remind employees to protect patient confidentiality
4. Locking file cabinets or otherwise instituting protections where patient records are kept

4.1.1.4 Public Interest and Benefit Activities.

The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, the following national priority purposes.

#	Use/Disclosure	Description
1	Required by law	As required by law, statute, regulation or court order
2	Public health activities	To health authorities for public health purposes such as surveillance, investigations and interventions
3	Victim of abuse, neglect or domestic violence	To report abuse, neglect, or domestic violence
4	Health oversight activities	To a health oversight agency for oversight activities authorized by law
5	Judicial and administrative proceedings	In the course of a judicial or administrative proceeding under specified circumstances

#	Use/Disclosure	Description
6	Law enforcement purposes	To law enforcement officials pursuant to a court order, subpoena, or other legal order in regard to an investigation
7	Decedents	To funeral directors as needed, and to coroners or medical examiners to identify a deceased person, and determine cause of death
8	Cadaveric organ, eye or tissue donation	Organ procurement agencies may use PHI for the purposes of facilitating transplants
9	Research	1. On receipt of a waiver from an institutional review board (IRB) or a privacy board 2. For activities preparatory to research 3. For research on a decedent's information
10	Serious threat to health or safety	If a CE believes it is necessary to prevent or lesson a serious and imminent threat to the person or public (may also disclose to law enforcement if necessary)
11	Essential government functions	Including but not limited to: 1. Assuring proper execution of a military mission 2. Conducting intelligence and national security activities 3. Providing protective services to the President 4. Making medical suitability determinations for U.S. State Department employees 5. Protecting the health and safety of inmates or employees in a correctional institution

#	Use/Disclosure	Description
12	Workers' compensation	(work related health information) as authorized by, and to the extent necessary to comply with workers' compensation programs

Table 3: Public interest and benefit activities in which PHI use and disclosure is permitted[11]

4.1.1.5 Psychotherapy Notes

A CE must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions granted to the CE that created the notes:

1. for treatment purposes.
2. for its own training purposes
3. to defend itself in legal proceedings brought by the individual
4. for HHS to investigate or determine the Covered Entity's compliance with the Privacy Rules
5. to avert a serious and imminent threat to public health or safety
6. to a health oversight agency for lawful oversight of the originator of the psychotherapy notes
7. for the lawful activities of a coroner or medical examiner or as required by law

4.1.1.6 Marketing

As per the Privacy Rule, "Marketing" is any communication about a product or service that encourages recipients to purchase or use the product or service. With limited exceptions, this Rule requires an individual's written authorization before a use or disclosure of their PHI can be made for marketing.

11 https://www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm

In this section, we will discuss the following three cases:

1. Communications that meet the definition of marketing in which authorization by the individual is **required**
2. Communications that meet the definition of marketing in which authorization by the individual is **not required**
3. Exceptions to the definition of marketing in which authorization by the individual is **not required**

Case 1 – Marketing communication where authorization is required

Generally, if the communication is "marketing", then the communication can only occur if the CE first obtains an individual's authorization.

For example,

- A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for $39, when the communication is not for the purpose of providing treatment advice
- A communication from a health insurer promoting a home and casualty insurance product offered by the same company

Marketing also is an arrangement between a CE and any other entity whereby the CE discloses PHI, in exchange for direct or indirect compensation, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. If compensation is involved, the authorization from the individual must acknowledge as such.

For example,

- A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors.

- A drug manufacturer receives a list of patients from a covered health care provided and provides compensation, then uses that list to send discount coupons for a new anti-depressant medication directly to the patient.

Case 2 – Marketing communication where authorization is not required

In the following cases, marketing communication does not require written authorization from an individual:

1. If a marketing communication involves face-to-face communications between a CE and an individual
2. For a CE's provision of promotional gifts of nominal value

For example,

- A hospital provides a free package of formula and other baby products to new mothers as they leave the maternity ward.
- An insurance agent sells a health insurance policy in person to a customer and proceeds to also market a casualty and life insurance policy as well.

Case 3 – Exceptions to the definition of marketing communication where authorization is not required

There are three categories of exceptions:

1. If it describes a health-related product, service or payment that is provided by or included in a benefits plan of the CE (for example, a hospital uses its patient list to announce the arrival of new equipment via email)
2. If it is in regard to the treatment of an individual (for example, a pharmacy mails prescription refill reminders to patients or contracts with a mail service to do so)
3. If it is in regard to case or care management for the individual (for example, a hospital social worker shares a health record with various nursing homes in the process of recommending a transfer)

4.2 Minimum Necessary Principle of Uses and Disclosures

The **Minimum Necessary** principle is a cornerstone of the Privacy Rule. It is based on confidentiality codes and practices in common use today. This standard requires CEs to evaluate their practices to ensure that PHI is not used or disclosed when it is not necessary to satisfy a particular purpose. It also requires CEs to implement safeguards to ensure that this standard is implemented (see **7 What are the Security Rule Safeguards?**).

Minimum Necessary principle

A CE must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

4.2.1 Requirements of the Minimum Necessary Principle

1. A CE must implement a PHI Use and Disclosure Policy that requires the following:
   a. Limits routine PHI uses and disclosures to the minimum necessary
   b. For non-routine disclosures and requests, CEs must develop reasonable criteria for determining and limiting the disclosure to the minimum necessary
   c. Identifies the persons or classes of persons within the CE who need access to the information to carry out their job duties, the categories or types of PHI needed and the conditions appropriate to such access (for example, a policy may be implemented that dentists, dental assistants, and dental hygienists all have access to the entire health record as needed without a case-by-case review)
2. The appropriate Security Rule Safeguards must be in place (see 7 What are the Security Rule Safeguards?)
3. An entire health record may not be able to be used or disclosed unless it can specifically justify the whole record as the amount reasonable needed for the specific purpose at hand

4. The responsibility to determine what the minimum necessary information is lies with the CE. If an external entity requests disclosure of PHI, In the following cases, a CE may choose to rely on their judgment:
   a. A public official or agency
   b. Another CE
   c. A professional who is a workforce member or BA of the CE
   d. A researcher from an Institutional Review Board (IRB) or Privacy Board

   Note: The CE always retains the discretion to make its own determination for minimum necessary disclosure.

4.2.2 Exceptions of the Minimum Necessary Principle

The minimum necessary requirement does not apply to the following situations:

1. disclosure to or a request by a health care provider for treatment
2. disclosure to an individual who is the subject of the information, or the individual's personal representative
3. use or disclosure made in line with an individual's authorization
4. disclosure to HHS for complaint investigation, compliance review or enforcement (see 9 How is HIPAA compliance enforced?)
5. use or disclosure that is otherwise required by law
6. use or disclosure required for compliance with the HIPAA Administrative Simplification Rules (see 10 What is the Administrative Simplification Rule?)

4.3 Administrative Requirements

The Privacy Rule requires certain administrative provisions be implemented in the practices of healthcare providers that are Covered Entities. These provisions are known as **Administrative Requirements** and are detailed in 45 CFR 164.530. This section details these requirements and what is required of Covered Entities in regard to these requirements.

Healthcare providers have the latitude to analyze their own needs and functions and to implement solutions that are reasonable and appropriate based on these factors.

4.3.1 Privacy Personnel [45 CFR 164.530(a)]

A Covered Entity must designate:

1. A Privacy Official who is responsible for the development and implementation of the privacy policies and procedures of the facility.
2. A contact person, office (or may be the Privacy Official) that is responsible for receiving complaints (see **5.9 Right to Make Complaints**) and may provide further information about the facility's privacy practices.

4.3.2 Workforce Training and Management [45 CFR 164.530(b)]

A Covered Entity must:

1. train its workforce members* on its privacy policies and procedures, as necessary and appropriate for them to carry out their job responsibilities

***Workforce members** include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).

4.3.3 Safeguards [45 CFR 160.530(c)]

A CE must maintain reasonable and appropriate administrative, technical, physical and organizational safeguards:

1. to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule (see 4.1 Use and disclosure of PHI)
2. to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure (see 4.1 Use and disclosure of PHI)

For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes.

The safeguards required by the Privacy Rule are the same as what is required by the Security Rule (see **7 What are the Security Rule Safeguards?**) with the exception that they apply to all types of PHI (written, electronic, and oral) while the Security Rule safeguards only apply to electronic Protected health information (ePHI). In fact, many healthcare providers will find that complying with the Security Rule safeguards also brings them into compliance with the Privacy Rule safeguards.

4.3.4 Complaints [45 CFR 164.530(d)]

A CE must:

1. have procedures for individuals to make complaints if they believe that the Privacy Rule is not being upheld (see **5.9 Right to Make Complaints**)
2. identify to whom individuals can submit complaints to at the Covered Entity and advise that complaints also can be submitted to the Secretary of HHS (see **5.9 Right to Make Complaints**)
3. explain those procedures in its Notice of Privacy Practices (see 5.3 Right to Designate a Personal Representative)

4.3.5 Sanctions [45 CFR 164.530(e)]

A CE must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.

4.3.6 Mitigation [45 CFR 164.530(f)]

A CE must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

4.3.7 Refraining from Retaliation [45 CFR 164.530(g)]

A CE may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule (see **5.9.2 Complaint Protections**).

4.3.8 Waiver of Rights [45 CFR 164.530(h)]

A CE may not require an individual to waive any of their rights under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

4.3.9 Privacy Policies and Procedures [45 CFR 164.530(i)]

A Covered Entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.

4.3.10 Documentation and Record Retention [45 CFR 164.530(j)]

A CE must maintain, until six years after the latter of the date of their creation or last effective date, its:

1. privacy policies and procedures
2. privacy practices notices
3. disposition of complaints
4. other actions, activities, and designations that the Privacy Rule requires to be documented

4.4 How State and Federal law intersect with regards to HIPAA

4.4.1 Preemption of Federal Law

The Privacy Rule provides a Federal floor of privacy protections for the PHI used and disclosed by CEs and their BAs. If and when a State law is contrary (see **4.4.2 Contrary State Laws**) to the Rule, this rule is preempted by the Federal requirements, unless a specific exception applies (see **4.4.3 Exceptions to Federal Preemption**). In these circumstances, a CE is not required to comply with a contrary provision of the Federal law.

4.4.2 Contrary State Laws

In general, State laws that are ***contrary*** to the Privacy Rule are preempted by the federal requirements, which means that HIPAA laws as stipulated at the federal level will apply.

For example, a State law that prohibits the disclosure of PHI to an individual who is the subject of the information may be contrary to the Privacy Rule, which requires such disclosure in certain circumstances.

The Privacy Rule provides exceptions to the preemption of Federal law in certain cases (see **4.4.3 Exceptions to Federal Preemption**).

Definition of "contrary" per the Privacy Rule

Contrary:

1. it would be impossible for a CE to comply with both the State and federal requirements.
2. the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA

4.4.3 Exceptions to Federal Preemption

Upon specific written request from a State or other entity or individual, HHS may determine that a contrary provision of State law that meets certain criteria will not be preempted by the Federal requirements. This is only if the Secretary or other HHS official determines that the State law:

1. is necessary to prevent fraud and abuse related to the provision of or payment for health care
2. is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation
3. is necessary for State reporting on health care delivery or costs
4. is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
5. has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substance, or that is deemed a controlled substance by State law.

The request for exception must explain how the State law in question is actually contrary to the Federal requirements (see **4.4.2 Contrary State Laws**), and how the contrary State law meets one or more of the specific criteria stated above.

When such an exception is granted, it will remain in effect until either the State law or the Federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists or the Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Unless an exemption exists in the HIPAA Rules, State laws that are contrary to the Privacy Rule access provisions – such as those that prohibit certain laboratories from disclosing test reports directly to an individual – are preempted by HIPAA. Thus, these State laws do not apply when an individual exercises his/her HIPAA right of access.

4.4.4 More Stringent State Laws

Occasionally, a more stringent provision of State law may be contrary to a HIPAA provision, in which case the Federal law provides an exception to preemption (in effect, making the State law prevail).

Where the more stringent State law and Privacy Rule are not contrary, however, CEs must comply with both laws.

In general, a State law is "more stringent" than the HIPAA requirements if it relates to the privacy of individually identifiable health information and provides greater privacy protections for individuals' identifiable health information, or greater rights to individuals with respect to that information, than the Privacy Rule does.

For example, a State law that provides individuals with a right to inspect and obtain a copy of their health records in a timelier manner than the Privacy Rule is "more stringent" than the Privacy Rule.

This page intentionally left blank

5 What are a patient's rights to their health information?

A patient's rights under the Privacy Rule and what you must do to afford those rights

The second mandate of the Privacy Rule is establishing a patient's rights over their health information. In order to afford patient's these rights, there are certain requirements of Covered Entities and Business Associates. This Chapter covers both aspects.

Providing individuals with easy access to their health information empowers them to be more in control and involved in their health care. For example, individuals with access to their health information are better able to monitor chronic health conditions, monitor and track their treatment progress and correct errors in their health records. Maintaining and increasing patient engagement is important with continued advances in health care.

The Department of Health and Human Services recognizes that Covered Entities and Business Associates range in size between small practices and large, multi-state practices. The Privacy Rule is designed to be flexible such that CEs may examine their own needs and implement policies that are appropriate for their size. What is appropriate depends on a CEs' size, resources and capabilities.

Bearing this in mind, let's examine the rights of patients to their health information and how CEs are expected to afford patients these rights per the HIPAA rules.

5.1 Right to authorize use and disclosure of PHI

An individual has the right to authorize the use and disclosure of their PHI that is **not** permitted by the Privacy Rule to be done without his or her express permission. The Privacy Rule permits the use and disclosure of PHI for the following purposes without an individual's express authorization - treatment, payment or health care operations (see **4.1.1 Permitted Uses and Disclosures**). For all other reasons, an individual's authorization is required.

Examples of disclosures that would require an individual's authorization include:

- disclosures to a life insurer for coverage purposes
- disclosures to an employer of the results of a pre-employment physical or lab test
- disclosures to a pharmaceutical firm for their own marketing purposes

The authorization itself requires specific elements. It must be written in plain language so that it is understandable to the individual and be transparent regarding the protected health information that may be used or disclosed, the entities that may receive and/or use the PHI, and the individual's rights regarding the information.

See the HIPAA Documentation Kit for a template for a Use and Disclosure Authorization Form.

5.2 Right to Access of PHI

An individual has the right to access their protected health information. According to the Privacy Rule, on request of the individual, CEs are required to provide individuals access to their PHI as part of one or more "designated record sets" (see **5.2.1 Designated Record Set**).

The Right to Access is covered under 45 CFR 164.524.

From an individual's perspective, the right to access has two components:

1. the right to inspect and/or obtain a copy of the PHI a requested format (see 5.2.2 Providing Access to PHI)
2. the right to direct the CE to send a copy of their PHI to another person or entity of their choice (see 5.3 Right to Designate a Personal Representative)

From a CE perspective, the right to access has the following two components:

1. a CE has the authority to require a request for access be made by the individual per a formal process (see 5.2.3 Making a Request for Access).
2. in certain circumstances, a CE or BA has the authority to deny a right to access (see 5.2.4 Authority for Denial of Access).

5.2.1 Designated Record Set[12]

Designed record set is defined in the regulations at in 45 CFR 164.501.

Individuals have the right to access the protected health information that is maintained in a "designated record set".

A designated record set is a group of records maintained by or for a CE that comprises the:

- Health records and billing records about individuals maintained by or for a covered health care provider
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
- Other records that are used, in whole or in part, by or for the CE that may be used to make healthcare related decisions about individuals whether or not those records had previously been used to make healthcare related decisions about the individual requesting access.

The term "record" refers to any item, collection, or grouping of information that includes PHI, which a CE maintains, collects, uses, or disseminates.

This means that an individual has a right to a wide range of his/her health information, including:

- health records
- billing and payment records
- insurance information
- clinical laboratory test results
- medical images, such as X-rays
- wellness and disease management program files
- and clinical case notes
- and any other information used to make decisions about an individual

In responding to a request for access, a CE is not required to create new information

12 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

(e.g. explanatory materials or analyses) that does not already exist in the designated record set.

5.2.2 Providing Access to PHI

5.2.2.1 Form and Format Access

When access to PHI is requested by an individual, the individual also has the right to request the information in their preferred form or format. This is so long as the CE is easily able to produce the PHI in the requested form or format. If not, the CE and individual should agree to the form and format the PHI will be provided.

"Form and Format" refer to how the PHI is conveyed to the individual – whether paper, electronically, and the type of file.

Table 4: Forms and Formats of PHI conveyed to an individual outlines some of the examples of formats an individual may request their PHI.

Format Requests	Action Required
Paper Copy	If an individual requests a paper copy of their PHI maintained by the CE, the latter is responsible to issue a paper copy regardless of whether the PHI is maintained in paper format or electronic format.
Electronic Copy	If an individual requests an electronic copy of their PHI maintained by the CE, the latter is responsible to issue an electronic copy: • If the PHI is maintained in a paper format, as a scan into an electronic format (if easily producible by the CE or BA) • If the PHI is maintained in an electronic format, the CE or BA must provide access in the same format or an agreed upon alternative electronic format

Format Requests	Action Required
	• If the individual does not agree to any easily producible electronic format, the CE or BA may provide a readable hard copy of the PHI.

Table 4: Forms and Formats of PHI conveyed to an individual

The Covered Entity also may provide the individual with a *summary* of the PHI requested, instead of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided in addition to that PHI, so long as the individual chooses in advance to receive the summary or explanation in the electronic or paper form being offered by the CE.

A fee may be charged to the individual for providing their PHI. For more information, see **5.2.2.5 Fees for Providing Access to PHI**.

5.2.2.2 Manner of Access

A Covered Entity must also provide access to PHI in the manner requested by the individual that is "readily producible" by the CE.

Manner refers to the form of transmission or the PHI from the Covered Entity or Business Associate to the individual.

Whether a particular mode of transmission or transfer is readily producible will be based on the capabilities of the CE and the level of security risk that the mode of transmission or transfer may introduce to the PHI on the CE's systems.

A CE is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access. Whether or not the individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the CE's Security Rule risk analysis (see **7 What are the Security Rule Safeguards?**).

Once the requested PHI has left the CE's system, they are not responsible for security risks to the PHI while in transit (though they are responsible to notify an individual of the potential safety risks and the individual must accept the risks associated with them, e.g. unencrypted e-mail).

Some of the ways an individual may choose to receive their PHI are in *Table 5: Manners*

in which an individual may request their PHI.

Manner of Access	Description
Physical pickup	A CE may arrange a convenient time and place for the individual to pick up or inspect their PHI if that is the manner of access requested by the individual. A CE may not mandate that an individual travels to the CE's physical location if they have the capability of either mailing or e-mailing a copy of the PHI to the individual.
Mail	It is expected that a CE has the capability to mail an individual a copy of their requested PHI.
E-mail	It is expected that a CE has the capability to mail an individual a copy of their requested PHI except in the case that e-mail cannot accommodate the size of the files requested.

Table 5: Manners in which an individual may request their PHI

A fee may be charged to the individual for providing their PHI. For more information, see **5.2.2.5 Fees for Providing Access to PHI**.

5.2.2.3 Timeliness in Providing Access

A CE must provide access to the requested PHI within 30 calendar days of the request. However, HHS expects and encourages that CEs respond as early as possible to such requests. This is especially true in cases of electronic access or format requests.

If a CE is unable to respond within a 30-calendar day period (for example, if the information is archived and hosted offsite), the CE is may extend the request fulfillment period by up to an additional 30 days. This extension must be requested in writing to the individual and must include the reason(s) for delay and date by which the CE will provide access. Only one extension is permitted per access request.

5.2.2.4 Duration of Right to Access

Individuals have the right to access their PHI for as long as the information is maintained by a CE regardless of:

- when or where the information was created
- the form or format the information is in
- where or how it is stored

5.2.2.5 Fees for Providing Access to PHI

The Privacy Rule permits a Covered Entity to impose a reasonable, cost-based fee to fulfill a request for access (whether that is providing an individual or their personal representative a copy of PHI, or forwarding a copy to a designated third party). This fee may only include the cost of:

- labor for copying the PHI requested by the individual, whether in paper or electronic form (e.g. photocopying paper, converting PHI formats, transferring PHI)
- supplies for creating the paper copy or electronic media (e.g. CD or USB drive) if the individual requests that the electronic copy be provided on portable media
- postage, when the individual requests that the copy, or the summary or explanation, be mailed
- preparation of an explanation or summary of the PHI, if requested and agreed to by the individual

The fee may not include costs associated with:

- ensuring only that information about the correct individual is included (see 5.2.3.3 Verification)
- labor searching for and retrieving the PHI
- maintaining a CE's systems
- a charge for a CE's data access, storage, or infrastructure

- other costs not listed above even if State law authorizes these costs unless an exception is provided (see 4.3 Administrative Requirements)
- providing access to PHI using Certified Electronic Health Record Technology (CEHRT)
- costs associated with utilizing a 3rd party service (a Business Associate) to fulfill requests for access

While it is permitted by the Privacy Rule to charge a nominal fee to fulfill a request for access, it is the recommendation of HHS that all requests for access be provided free of charge to individuals.

See *Table 6: Calculating fees to fulfill PHI access requests* for calculating the fee charged to an individual for fulfilling a request for access to PHI.

Methodology	Description
Actual costs	A CE or BA may calculate the actual costs including labor, postage, etc. and must inform the individuals in advance of the fee they may be charged to obtain a copy of their PHI.
Average costs	A CE or BA may develop a schedule for costs based on average labor costs, material costs, postage, etc.
Flat rate	A CE or BA may charge individuals a flat fee of no greater than $6.50 to provide individuals with a copy of their PHI (inclusive of all labor, supplies and postage). This option is for CEs and BAs that do not want to go through the process of calculating the actual or average costs.

Table 6: Calculating fees to fulfill PHI access requests

5.2.2.6 Confidential Communications Requirements.

Covered Entities and Business Associates must accommodate requests of individuals to receive communications of PHI by other means than those CEs or BAs typically employ in the case that the requested communication method is more confidential than

the typically method. For example, an individual may request communications be provided in a closed envelope rather than a post card or at an alternative phone number.

5.2.3 Making a Request for Access to PHI

5.2.3.1 Requiring a Written Request

A CE may require individuals to request access in writing, provided that it informs individuals of this requirement and there is no unreasonable barrier to the individual obtaining their PHI (see **5.2.3.2 Unreasonable Measures**). CEs may also offer individuals the option of using electronic means (e.g. e-mail, secure web portal) to make requests for access. In addition, a CE may require individuals to use the entity's own supplied form, provided use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to his/her PHI, as will be discussed below.

5.2.3.2 Unreasonable Measures

While CEs are allowed to require request for access in writing, and are required to verify an individual's identity prior to granting such access (see **5.2.3.3 Verification**), the CE may not impose unreasonable measures on an individual that serve as barriers to or delay the individual from obtaining access.

For example, a CE may not

- require an individual requesting access to his/her records to provide proof of identity *in person* when they are speaking on the phone
- *solely* use a web portal to access the information (since this type of system might not be accessible by all)
- require an individual to mail an access request (which would unreasonably delay the CE's receipt of the request and by extension, the individual's access)

CEs are encouraged to offer individuals multiple options for requesting access.

5.2.3.3 Verification

The Privacy Rule requires a CE to take reasonable steps to verify the identity of an

individual making a request for access to their PHI. While the verification method should be robust, it must not create an unreasonable barrier (see **5.2.3.2 Unreasonable Measures**) or delay for the individual to access their PHI.

It is up to the discretion and professional judgement of the CE to determine the verification process and measures.

Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access. For example:

- If the Covered Entity requires that access requests be made on its own supplied form, the form could ask for basic information about the individual that would enable the CE to verify that the person requesting access is the subject of the information requested or is the individual's personal representative.
- For those CEs providing individuals with access to their PHI through web portals, those portals should already be set up with appropriate authentication controls, as required by the Security Rule (see **7.3.1 Access Control**), to ensure that the person seeking access is the individual or his/her personal representative.

5.2.3.4 Exclusions from the Right of Access

There are certain types of PHI that are excluded from the Privacy Rule's Right to Access, and therefore, the individual's review.

- psychotherapy notes (see 4.1.1.5 Psychotherapy Notes)
- information compiled for legal proceedings
- laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access
- information held by certain research laboratories.
- Information which is <u>not</u> part of a Designated Record Set (see 5.2.1 Designated Record Set)
    - For example, a hospital's peer review files may be generated from and include an individual's PHI but might not be in the CE's designated record set and subject to access by the individual.

Additionally, Covered Entities are permitted, in certain limited circumstances, to deny an individual or their personal representative access to PHI. For more information, see **5.2.4 Authority for Denial of Access**.

5.2.3.5 Redirecting a Request for Access

If the CE does not maintain the PHI requested, but knows where the information is maintained, the CE must inform the individual where to direct the request for access.

5.2.4 Authority for Denial of Access

For PHI that is included within the Right of Access, in certain limited circumstances, CEs may deny an individual or their personal representative access. This section lists the grounds for which this denial may take place (see **5.2.4.1 Grounds for Denial**).

Additionally, in some of these cases, an individual has the right to have the denial reviewed by a licensed health care professional (designated by the Covered Entity) that did not participate in the original denial (see **5.2.4.3 Review of Denial**).

A CE may not require an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the CE, is not a permitted reason to deny access. In addition, a CE may not deny access because its BA, rather than the CE itself, maintains the PHI requested by the individual (e.g. the PHI is maintained by the CE's electronic health record vendor or is maintained by a records storage company offsite).

5.2.4.1 Grounds for Denial

There are two types of "grounds" for denial – *unreviewable* and *reviewable*.

5.2.4.1.1 Unreviewable Grounds for Denial[13]

If one of the following reasons is selected by the Covered Entity in denying an individual's request to access their PHI, the individual does not have the ability to request a review of the denial.

Unreviewable grounds for denial are explained further in 45 CFR 164.524(a)(2).

1. The request is for psychotherapy notes (see 4.1.1.5 Psychotherapy Notes).
2. The request is for information compiled for a legal proceeding
3. An inmate requests a copy of his/her PHI held by a CE that is a correctional institution, or health care provider acting under the direction of the institution, and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of correctional officers, employees, or other person at the institution or responsible for the transporting of the inmate. However, in these cases, an inmate retains the right to inspect his/her PHI.
4. The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g. clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access is reinstated upon completion of the research.
5. The requested PHI is in Privacy Act protected records (i.e., certain records under the control of a Federal agency, which may be maintained by a Federal agency or a contractor to one), if the denial of access is consistent with the requirements of the Act.
6. The requested PHI was obtained by someone other than a health care provider (e.g. a family member of the individual) under a promise of confidentiality, and providing access to the information would be reasonably likely to reveal the source of the information.

13 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

5.2.4.1.2 Reviewable Grounds for Denial[14]

If one of the following reasons is selected by the Covered Entity in denying an individual's request to access their PHI, the individual has the ability to request a review of the denial.

Reviewable grounds for denial are explained further in 45 CFR 164.524(a)(3).

If, in the exercise of professional judgement, a licensed health care professional has determined that:

1. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g. concerns that the individual will not be able to understand the information or may be upset by it).
2. The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
3. The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

5.2.4.2 Executing the Denial

For more information on Executing the Denial, see 45 CFR 164.524(d).

If a CE denies an individual's request for access to their PHI for one of the reasons listed in **5.2.4.1 Grounds for Denial**, they must notify the individual in writing within 30 calendar days of the initial request for access.

The denial must be in plain language and describe the basis for the denial. It must also explain whether or not the denial is reviewable or unreviewable and explain the process by which an individual may request a review, if applicable. It must also explain how an individual may submit a complaint to the CE or to the *Department of Health and Human Services Office for Civil Rights*.

14 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

The Documentation Kit contains a template for a PHI Access Request Denial Form.

The CE must, to the extent possible and within the above timeframes, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply.

5.2.4.3 Review of Denial

If the denial was based on a reviewable ground for denial and the individual requests review, the CE must promptly refer the request to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial. The CE must then promptly provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary to carry out the determination.

5.3 Right to Designate a Personal Representative

The Privacy Rule also establishes an individual's right to direct the CE to transmit the PHI about him/herself directly to another person or entity designated by the individual. This person is the individual's "personal representative". Under the Privacy Rule, a CE must treat the personal representative the same as the individual with respect to use and disclosure of the individual's PHI. All of the rights that apply for the individual apply to the personal representative as well in this case. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate.

The right to designate a personal representative is established in 45 CFR 164.502(g).

5.3.1 Designating a Personal Representative

The individual's request to direct the PHI to another person must be in writing, signed

by the individual, and clearly identify the designated person and where to send the PHI. A CE may accept an electronic copy of a signed request (e.g. PDF), as well as an electronically executed request (e.g. via a secure web portal) that includes an electronic signature. The same requirements for providing the PHI to the individual, such as the fee limitations and requirements for providing the PHI in the form and format and manner requested by the individual, apply when an individual directs that the PHI be sent to another person. See *Table 7: Examples of Personal Representatives* for examples of who may be designated as a Personal Representative.

5.3.2 Rights of a Personal Representative

An individual's personal representative also has the right to access PHI about the individual in a designated record set, as well as the right to direct the CE to transfer a copy of the PHI to a designated person or entity of the individual's choice, as long as such a request is in line with the scope of the representation.

In general, the scope of the personal representative's authority to act for the individual is based on his or her authority under applicable law to make health care decisions for the individual. Where the authority to act for the individual is limited or specific to particular health care decisions, the personal representative is to be treated as the individual only with respect to PHI that is relevant to that representation.

CEs should also consult State or local law to determine the authority of a personal representative to receive or access the individual's PHI.

5.3.3 Exception to a Personal Representative Designation

The Privacy Rule allows for an exception when a CE has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual in question.

The Privacy Rule also does not apply to the health information of an individual who has been deceased for more than 50 years; thus, a personal representative does not need to authorize disclosures of the decedent's health information nor does a personal representative have rights under the Privacy Rule with respect to such information.

5.3.4 Who may be recognized as a Personal Representative

Table 7: Examples of Personal Representatives lists some examples of who may be considered as a personal representative for different types of individuals.

If the Individual Is:	The Personal Representative Is:
An adult or an emancipated minor	A person with legal authority to make health care decisions on behalf of the individual Examples: • Health care power of attorney • Court appointed legal guardian • General power of attorney or durable power of attorney that includes the power to make health care decisions Exceptions: • when the CE suspects neglect or abuse
An unemancipated minor	A parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of the minor child Exceptions: • See 5.3.5 How unemancipated minors may designate a Personal Representative • And when the CE suspects neglect or abuse
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to persons with authority to make health care decisions) Examples: • Executor or administrator of the estate

If the Individual Is:	The Personal Representative Is:
	• Next of kin or other family member (if relevant law provides authority)

Table 7: Examples of Personal Representatives[15]

5.3.5 How unemancipated minors may designate a Personal Representative

Usually, parents, guardians or other persons acting in loco parentis (hereafter referred to as "parent") act as the personal representatives for their minor children. Therefore, in most cases, parents can exercise the minor's rights with regards to their healthcare, such as access to their health record.

However, there are certain exceptional cases where the parent is not considered an unemancipated minor's personal representative. In these situations, the parent does not control the minor's health care decisions, and thus under the Rule, does not control the PHI related to that care. The Privacy Rule defers to State and other law to determine the rights of parents to access and control the PHI of their minor children. If State and other law does not have provisions regarding parental access to the minor's PHI, a Covered Entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment.

Table 8: Examples of exceptions to Parent Personal Representation describes three examples in which a parent is not a minor's personal representative.

15 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html?language=es

Circumstance	Example
When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service	A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent's consent.
When someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent;	A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.
When a parent agrees to a confidential relationship between the minor and a health care provider.	A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

Table 8: Examples of exceptions to Parent Personal Representation[16]

The Privacy Rule defers to State or other applicable laws that expressly address the ability of the parent to obtain PHI about the minor child. In doing so, the Privacy Rule permits a CE to disclose to a parent, or provide the parent with access to, a minor child's PHI when and to the extent it is permitted or required by State or other laws (including relevant case law). Similarly, the Rule prohibits a CE from disclosing a minor child's PHI to a parent, or providing a parent with access to such information, when and to the extent it is prohibited under State or other laws (including relevant case law).

16 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html?language=es

5.4 Individual's right for Privacy Practice Notice

The Privacy Rule gives individuals the right to be informed of a Covered Entity's privacy practices as well as their rights to their protected health information. As such, Covered Entities are required to create and make available a notice detailing how an individual's PHI is used and what their rights are to their PHI. This notice is known as the Notice of Privacy Practices or NPP.

5.4.1 Content of the Notice of Privacy Practices

The below items are required to be covered in a Notice of Privacy Practices:

> See the Documentation Kit for a template of a Notice of Privacy Practices.

1. How a CE may use and disclose PHI (see 4.1 Use and disclosure of PHI)
2. An individual's rights to their PHI (see 5 What are a patient's rights to their health information?)
3. A CE's legal responsibilities with respect to PHI (including a statement that the privacy of PHI is required by law)
4. The contact information of the Covered Entity's HIPAA Compliance Officer (or from whom an individual can get further information about a CE's privacy policies)
5. Contact information of the Department of Health and Human Services Office for Civil Rights
6. The date the NPP became effective (i.e. the date the policy was instituted or last updated)

A CE is required to immediately update and distribute its NPP whenever it makes changes to its privacy practices. A CE is not required to resend an updated NPP to patients that have already received the NPP.

5.4.2 Notice of Privacy Practices Distribution.

The Privacy Rule also has stipulations regarding how the Notice of Privacy Practices is made available. These requirements are different for health plans and healthcare providers; the requirements of healthcare providers are listed below:

As of April 14, 2003, healthcare providers must provide the NPP:

1. To any person that requests it
2. As a posting prominently within the practice where it may reasonably be accessed and reviewed by patients (e.g. as a booklet in a waiting room and/or as a poster)
3. No later than the date of the first service delivery, in a manner aligned with the service provided. For example, if the first service was provided in a facility's physical location, a hard copy of the NPP may be provided. If the first service was electronic, then the healthcare provider must send an electronic NPP automatically and immediately.
4. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation

   Note: While it is not *required* of healthcare providers to post their NPP on any web site they maintain, it is highly recommended.

The Covered Entities in an Organized Health Care Arrangement (see **2.3.3 Organized Health Care Arrangement (OHCA)**) may use a joint privacy practices notice. In this case, the distribution of the joint NPP must happen at the first point that an OHCA member has the opportunity and obligation to provide it to the patient. If any one of the OHCA members provides the joint NPP to the individual, the requirement to provide an NPP is met for all members.

5.4.3 Acknowledgement of Notice Receipt.

The Privacy Rule requires healthcare providers that have a direct treatment relationship with individuals to make a "good faith" effort to receive a written acknowledgement from patients of receipt of the NPP. There is no specific phrasing or content required by the Privacy Rule for this acknowledgement. It is up to the discretion of the Covered Entity to determine in what format to obtain this acknowledgement.

You may consider receiving this acknowledgement:

- In the form of a signature on a form a patient fills in on their first visit
- Electronically by the patient checking a "checkbox" confirming that they received a copy of the NPP if they receive service electronically

See the Documentation Kit for a sample template for an NPP Acknowledgement Form.

Note: The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

5.5 Right to make Amendments

The Privacy Rule gives individuals (or other Covered Entities) the right to request that a Covered Entity correct any inaccurate or incomplete protected health information. The Rule specifies processes for requesting and responding to a request for amendment.

See the Documentation Kit for a PHI Amendment Request Form and PHI Amendment Response Form.

On receipt of a request to make an amendment to PHI, a Covered Entity has the ability to either accept or deny the request.

5.5.1 Accepting an Amendment Request

If a Covered Entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the Covered Entity knows might rely on the information.

5.5.2 Denying an Amendment Request

If the request is denied, Covered Entities must provide the individual with a written denial with rationale for the denial. It must also allow and provide guidance on how the individual to submit a statement of disagreement for inclusion in the record.

5.6 Right to Accounting of Disclosures

The Privacy Rule provides individuals a right to obtain an accounting of any disclosures made of their protected health information from their Covered Entity with certain exceptions.

The Rule does not stipulate specific language in making a request or in responding to a request. The Covered Entity may request that an individual complete a form to request an accounting of disclosures so long as it does not create an unreasonable barrier between an individual and their PHI (see **5.2.3.2 Unreasonable Measures**).

See the Documentation Kit for a sample Disclosure Accounting Request Form.

It is up to the discretion of the Covered Entity to provide an accounting of disclosures in a reasonable, agreeable format.

5.6.1 Duration to Maintain Disclosure Accounting

Covered Entities are required to maintain a log of any disclosures made of an individual's Protected health information for a period of six years to the date immediately preceding the accounting request.

Covered Entities are not obligated to have an accounting of disclosures made before coming into compliance with the Privacy Rule.

5.6.2 Exceptions[17]

Covered Entities are not obligated to maintain an account of any disclosures made for the following purposes:

1. for treatment, payment, or health care operations
2. to the individual or the individual's personal representative
3. for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories
4. if done so as part of an authorization by the individual or their personal representative
5. disclosures of information contained within a limited data set

17 https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

6. for national security or intelligence purposes
7. to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody
8. incident to otherwise permitted or required uses or disclosures.

Note: accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

5.6.2.1 Oral Communications

The Privacy Rule does not require Covered Entities to document any information, including oral information, that is used or disclosed for treatment, payment or health care operations.

However, if information disclosed must be documented as required by other standards or regulations, an accounting of disclosures must be maintained. For example, if a health care provider discloses a case of tuberculosis orally to a public health care authority orally, it must be documented in the accounting of disclosures.

5.7 Right to Restrictions

Individuals have the right to request that a Covered Entity restrict use or disclosure of protected health information. The restriction applies to PHI used for the following reasons:

- Treatment
- payment
- health care operations
- disclosure to persons involved in the individual's health care or payment for health care
- disclosure to notify family members or others about the individual's general condition, location, or death

5.7.1 Making a Restriction Request

The Rule does not stipulate specific language in making a request or in responding to a request. The Covered Entity may request that an individual complete a form to request a restriction of PHI so long as it does not create an unreasonable barrier between an individual and their PHI (see **5.2.3.2 Unreasonable Measures**).

See the Documentation Kit for a sample PHI Restriction Request Form.

5.7.2 Accepting or Denying a Restriction Request

A Covered Entity is under no obligation to agree to requests for restrictions. For example, an individual who has obtained a genetic test may request that the health care provider not use or disclose the test results. If the health care provider chooses to do so, they may deny the request to restrict this information when treating other family members who are seeking to identify their own genetic health risks if sharing the information is in regard to the treatment of the other family members.

A Covered Entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

5.8 Right to Confidential Communications

The Privacy Rule also requires CEs to take reasonable steps to ensure the confidentiality of communications with individuals. This includes permitting individuals to request an alternative means or location for receiving communications of protected health information by means other than the CE usually employs. For example, an individual can ask to be contacted at a designated phone number or address, instead of their home phone and address.

A Covered Entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

5.9 Right to Make Complaints

The Privacy Rule affords individuals the right to make a complaint to the Covered Entity and/or the Department of Health and Human Services Office for Civil Rights (OCR) should they believe that the Privacy Rule is not being upheld.

5.9.1 Communicating the Right to Complain

Covered Entities must identify to whom individuals can submit complaints to at both the Covered Entity itself and how to contact the Department of Health and Human Services. At the Covered Entity, it is recommended to direct complaints to the HIPAA Compliance Officer.

The Covered Entity must explain this policy in their Notice of Privacy Practices (see **5.3 Right to Designate a Personal Representative**).

5.9.2 Complaint Protections

Per the Privacy Rule, an individual is afforded protection while in the process of making a complaint if they believe, in good faith, their HIPAA rights are being violated. In any of the following cases, a Covered Entity may not retaliate in any form against a person while they are:

- making a complaint to the Covered Entity or HHS,
- assisting in an investigation by HHS or other authority
- opposing an act of practice that the person believes, in good faith, violates the Privacy Rule

5.9.3 Complaint Record Retention

A Covered Entity must maintain records regarding the initial complaint and disposition of the compliant for a period of six years after the date of the complaint creation.

5.9.4 Making a Complaint

The Rule does not stipulate specific language in making a complaint or responding to a complaint. The Covered Entity must maintain a record of the complaint (see **5.9.3 Complaint Record Retention**) so it is recommended that they request the individual to fill out a form outlining their complaint.

See the Documentation Kit for a sample Complaint Form.

6 What is the Security Rule?

Details of the standards to protect individuals' electronic personal health information

The *HIPAA Security Standards for the Protection of Electronic Protected Health Information* or *Security Rule* protects the electronic personal health information (ePHI) of individuals that is created, used, maintained or received by a Covered Entity (see **2.1 Covered Entities** for more on Covered Entities). The national standards established in the Security Rule require using appropriate administrative, physical and technical safeguards (see **6.3.3 Explanation of Safeguards** for more) to ensure that the ePHI retains its confidentiality, integrity, and security. The Security Rule in effect makes the protections outlined in the Privacy Rule practical by addressing these safeguards that can be adopted in order to protect individuals' ePHI.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

The Security Rule does not apply to the protected health information transferred orally or in writing; it only applies to ePHI.

See **6.1 Differences between the Privacy Rule and Security Rule** for the key differences between the Security Rule and Privacy Rule.

Before the adoption of HIPAA, there was no nationally accepted set of security standards or requirements for protecting health information. With the development of newer technologies and the health care industry's increased reliance on electronic systems to carry out administrative functions, security risks became more and more possible.

The Security Rule aims to protect the privacy and security of people's health information, while making it possible for Covered Entities to continue using technology to improve the efficiency of their work. An important feature of the Security Rule is that it is flexible for different situations, to account for the diversity of the health care industry. The security standards are also technology-neutral to accommodate changes

and avoid bounding CEs by specific systems and/or software that may become obsolete in the future. Because of these flexibilities, each CE can adopt the policies and safeguards that are appropriate for its specific needs.

The Security Rule establishes a set of national standards for confidentiality, integrity and availability (see *Table 10: Security Rule Definitions of Integrity, Availability, and Confidentiality*) of ePHI. Along with its enforcement of the Privacy Rule, the HHS Office for Civil Rights (OCR) administers and enforces the Security Rule standards and may investigate complaints and review compliance. Covered entities, except small health plans, must have been in compliance with the Security Rule by April 20, 2005. Small health plans had an additional year over said date to comply.

6.1 Differences between the Privacy Rule and Security Rule

The Security Rule establishes a set of national standards for confidentiality, integrity and availability of ePHI. Along with its enforcement of the Security Rule, the HHS Office for Civil Rights (OCR) administers and enforces the Privacy Rule standards and may investigate complaints and review compliance. Both the Privacy Rule and Security Rule have bearing on the uses and disclosures of PHI with certain key differences.

See *Table 9: Privacy Rule and Security Rule Key Differences* for a list of key differences between the Privacy Rule and Security Rule.

	Privacy Rule	Security Rule
Rule Description	The Privacy Rule defines and limits the circumstances in which an individual's PHI may be used and disclosed.	The Security Rule confidentiality requirements supports the Privacy Rules prohibition against improper uses and disclosures of ePHI. It also promotes the integrity and availability of ePHI.

	Privacy Rule	Security Rule
Applicable information	All forms of Protected health information – written, electronic and oral	Only electronic Protected health information
Required safeguards	Requires certain policies and procedures to be established – e.g. creating a Notice of Privacy Practices.	Much more comprehensive security requirements. Requires administrative, technical and physical safeguards to protect ePHI. Many CEs complying with the Security Rule may find they also comply with the terms of the Privacy Rule for this reason.
Regulatory Reference	45 CFR 160 and 45 CFR 164 Subparts A and E	45 CFR 164 Subparts A and C

Table 9: Privacy Rule and Security Rule Key Differences

6.2 Security Rule Flexibility

The Department of Health and Human Services (HHS) recognizes that Covered Entities can range widely in size. Therefore, the Security Rule was designed to be flexible to allow Covered Entities to analyze their specific needs and implement appropriate measures.

While the Security Rule does not require CEs to implement all measures (see **Figure 6: Relationship between safeguards, standards, and implementation specifications**

Required vs. Addressable Specifications), it does require CEs to consider certain factors when determining what measures to adopt. These deciding factors include:

- their size, complexity, and functions
- their technical (hardware and software) systems
- the costs of potential security measures (though cost may not be used as a factor to avoid implementing security safeguards that are determined to be required)
- the probability (likelihood) and severity (degree of impact) of potential risks to ePHI

For example, less sophisticated protections may not be as effective as larger or more complex measures.

Keep this flexibility in mind when implementing the Security Rule safeguards in your practice.

6.3 General Rules

The Security Rule outlines the requirements for CEs to adopt reasonable safeguards—administrative, physical, and technical—to protect ePHI. Under the Security Rule CEs must:

1. Enforce the integrity, availability and confidentiality of all the ePHI they create, maintain, receive or transmit (see 6.3.1 Security Rule Definitions of Integrity, Availability and Confidentiality)
2. Identify and protect against anticipated threats to the integrity and security of the ePHI (see 6.3.2 Risk Assessment and Management)
3. Identify and protect against anticipated improper uses or disclosures of ePHI (see 6.3.3 Explanation of Safeguards)
4. Ensure their staff is aware and in compliance with the Security Rule (see 6.3.4 Training)

6.3.1 Security Rule Definitions of Integrity, Availability and Confidentiality

Term	Definition
Integrity	ePHI is not destroyed or altered in an unauthorized manner
Availability	ePHI is accessible and can be used on demand at any time by an authorized individual.
Confidentiality	ePHI is not disclosed or available to unauthorized entities. In this way, the Security Rule's confidentiality requirements support the Privacy Rule's requirements against improper uses and disclosures of PHI. Additionally, Security rule aims to maintain the integrity and availability of ePHI.

Table 10: Security Rule Definitions of Integrity, Availability, and Confidentiality

6.3.2 Risk Assessment and Management

Per the Security Rule, CEs are *expected* and *required* to review the effectiveness of their ePHI security management safeguards and processes in the form of a **Risk Assessment**.

The Risk Assessment is intended to evaluate the probability (or likelihood) and severity (or impact) of potential risks to the privacy and security of the ePHI maintained by the CE.

A Risk Assessment is a formal process that is required to be documented per the HIPAA Security Rule.

See the Documentation Kit for a Risk Assessment Form.

6.3.2.1 Risk Assessment Activities

The Risk Assessment process includes the following activities:

1. Identify potential risks to the privacy and security of ePHI
2. Analyze the probability of the potential risks occurring
3. Analyze the severity of the impact should the potential risks occur
4. Determine and adopt appropriate measures to address the risks identified through the risk assessment analysis. This includes:
    a. Understanding the Security Rule, its standards and required specifications (see 6.3.3 Explanation of Safeguards)
    b. Assess the "addressable" specifications and determine whether each one is appropriate in the CE's environment (see Figure 6: Relationship between safeguards, standards, and implementation specifications
    c.
    d. Required vs. Addressable Specifications)
    e. Establish and implement the identified necessary protective measures
5. Document the chosen security measures and where appropriate the justification for choosing such measures
6. Maintain continuous, reasonable, and appropriate protections, and repeat this entire process periodically (see 6.3.2.2 When is a Risk Assessment Required?)

6.3.2.2 When is a Risk Assessment Required?

When doing an initial HIPAA compliance review, CEs are required to perform an initial Risk Assessment, identify necessary safeguards to implement, and perform another Risk Assessment (also called a residual Risk Assessment) to measure the effectiveness of the implemented safeguards in reducing risk.

Beyond the Risk Assessment performed as part of initial HIPAA compliance, HHS does not require repeat Risk Assessments to be performed at *specific* intervals – though it is required to regularly review these records. For this reason, it is recommended that CEs review their Risk Assessment evaluations:

1. On an annual basis
2. If there is a change to the Security safeguards currently in place, i.e. if any new safeguards or protections are added or if existing safeguards are removed or changed

As part of this review, evaluate the identified risks to determine whether any risks need to be added or removed and if there needs to be any change to the implemented safeguards.

6.3.3 Explanation of Safeguards

The core of the Security Rule is the establishment of safeguards to protect the privacy and security of ePHI. This section explains the concept of safeguards and some important terms to know when implementing safeguards in your practice.

6.3.3.1 Types of Safeguards

The Security Rule safeguards fall into the following types:

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards
4. Organizational, Policies, Procedures, and Documentation Requirements

Regulatory definitions of the safeguards can be found in the Security Rule at 45 CFR 164.304.

For more detailed information and instructions on how to implement safeguards in your practice, see **7 What are the Security Rule Safeguards?**.

6.3.3.2 Definition of Standards and Implementation Specifications

When discussing the Security Rule safeguards, the terms **Standard** and **Implementation Specification** are important. This section illustrates these terms.

As explained in **6.3.3.1 Types of Safeguards** there are different types of safeguards. Within each type of safeguard, there are a number of regulatory standards that adhered to by CEs. Compliance with these standards are through the consideration and

implementation of Implementation Specifications. Implementation specifications represent the security actual activities with regards to the Security Rule. They may be either "required" or "addressable". **Figure 6: Relationship between safeguards, standards, and implementation specifications** illustrates the relationship between safeguards, standards and implementation specifications with an example.

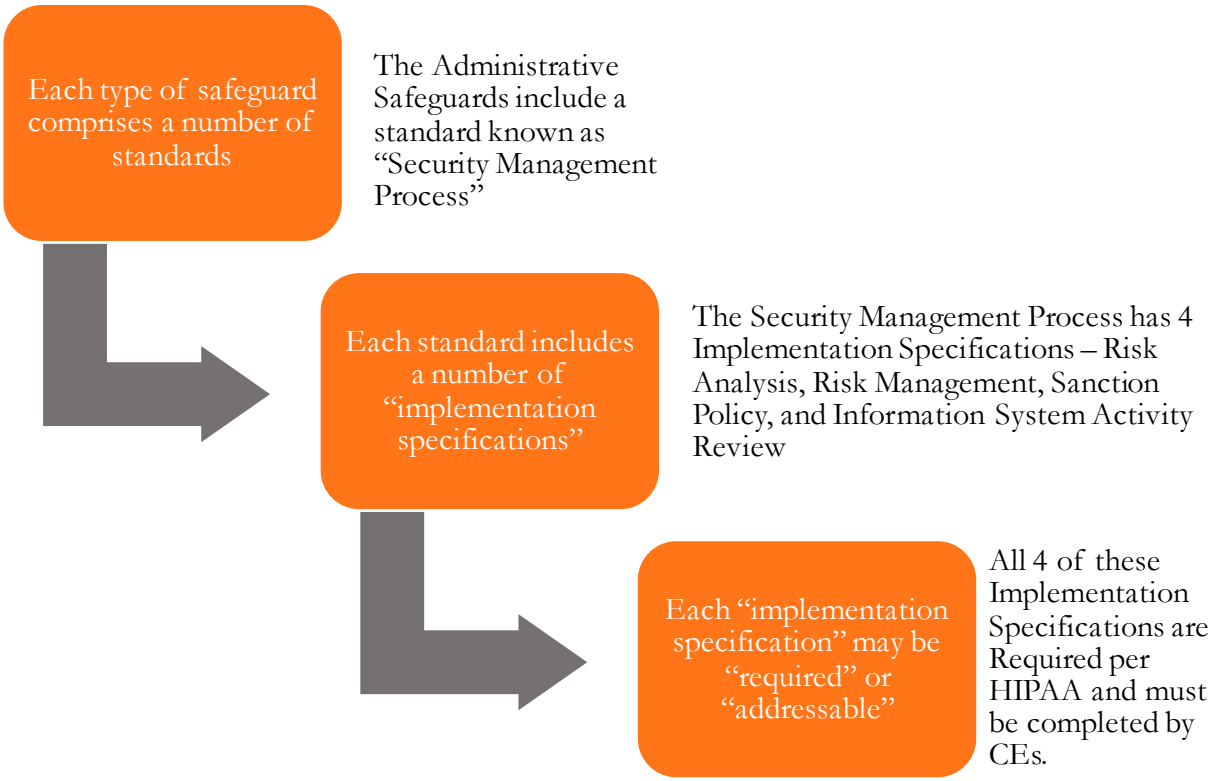

Figure 6: Relationship between safeguards, standards, and implementation specifications

6.3.3.3 Required vs. Addressable Specifications

Each set of safeguards for the Security Rule comprises a number of standards or requirements to comply with, each of which includes a number of **implementation specifications**.

Implementation specifications provide detailed instructions for how a Covered Entity should implement a particular standard.

While Covered Entities are required to comply with every standard, the Security Rule categorizes certain implementation specifications as "**required**" and others as "**addressable**."

- The **required** specifications must be adopted in every case.
- **Addressable** does not mean that an implementation specification is optional, but instead it means that a Covered Entity must determine whether adopting such a specification is reasonable and appropriate in its particular environment.

This process includes assessing the specification and determining its efficacy in protecting the entity's ePHI from reasonably anticipated security risks. If a CE determines that a certain specification is not appropriate and reasonable and decides against adopting it, the entity must document the reasoning and, when appropriate, implement an alternate reasonable and appropriate measure that achieves the purpose of the standard.[18]

In short, for each of the addressable implementation specifications, a Covered Entity must either:

- Implement the specification if it is reasonable and appropriate; or,
- If implementing the specification is not reasonable and appropriate:
  - Document the reasoning supporting the decision, and
  - Implement an alternate measure that is reasonable and appropriate and that would achieve the same purpose, or

18 (See C.F.R. 164.306(d)(ii)(B)(2) for more information.)

- Not implement the specification or an equivalent alternative measure, if the standard could still be met, and if implementing the specification or an equivalent would not be reasonable or appropriate.

A CE must consider options for implementing a particular addressable specification, if it is deemed to be reasonable and appropriate. The decision regarding which security measures need to be adopted to address the standards and implementation specifications depend on a variety of factors, namely:

- The CE's Risk Assessment (see 6.3.2 Risk Assessment and Management)
- The CE's currently implemented safeguards and protections
- The CE's financial capabilities

6.3.4 Training

The Security Rule requires that a CE's workforce undergo HIPAA training to ensure awareness of the different HIPAA requirements and practices to ensure PHI and ePHI privacy and security. For more information, see **4.3.2 Workforce Training and Management [45 CFR 164.530(b)]** and **7.1.5 Security Awareness and Training**.

6.4 Preemption of Federal Law over State Law

In a similar fashion to the Privacy Rule, in the case of the Security Rule, HIPAA "preempts" or applies over State law unless the State law is more stringent or, in cases of the State law being contrary to the Federal law, an exception is granted by HHS. For more information, see **4.3 Administrative Requirements**.

6.5 Compliance

The Department of Health and Human Services Office for Civil Rights (OCR) is responsible for administering and enforcing the standards of the HIPAA Security Rule. For more information, see **9 How is HIPAA compliance enforced?**.

7 What are the Security Rule Safeguards?

Administrative, Physical, Technical and Organizational safeguards to ensure integrity of ePHI under the Security Rule

As explained in **6 What is the Security Rule?**, the Security Rule establishes the requirements for certain safeguards to be implemented in the practices of Covered Entities.

This chapter lists and describes the different types of safeguards, standards and the implementation specifications. For each implementation specification, what Covered Entities must do to comply with the Security Rule requirements is explained.

The implementation specification section headers have a "- R" or "- A" if they are required or addressable respectively.

All standards are required to be implemented regardless of whether or not they contain implementation specifications.

Reference Tips

1. See the HIPAA Documentation Kit for Safeguard Worksheets your practice can use for implementation and documentation.
2. See 15 Security Safeguards Matrix for a listing of all safeguard types, their standards and implementation specifications.

7.1 Administrative Safeguards

The Security Rule defines administrative safeguards as administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE's workforce in relation to the protection of that information.

7.1.1 Security Management Process

As per this process, Covered Entities must implement policies and procedures to detect, prevent, contain and correct security violations. There are four implementation specifications in this standard, that outline what a Covered Entity needs to do in order to ensure compliance:

Section	Implementation Specifications R= Required, A=Addressable	
164.308(a)(1)	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R

7.1.1.1 Risk Analysis - R

- ✓ Conduct an accurate and complete assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
- ✓ Identify potential security risks and determine the probability (likelihood) of and severity (impact) of these risks.

7.1.1.2 Risk Management - R

- ✓ Address the findings from the risk analysis by implementing security measures that will sufficiently reduce risks and vulnerabilities to a reasonable and appropriate level.
- ✓ Consider the following factors with respect to implementing security measures:
  - size
  - complexity
  - capabilities
  - technical infrastructure
  - hardware, and software security capabilities
  - the cost of security measures
  - probability and criticality of potential risks to ePHI

Refer to the Documentation Kit for a Risk Assessment Form that can be used for documenting both the Risk Analysis and Risk Management Implementation Specifications.

Refer to **13 Basics of Risk Analysis and Management** for more information on performing Risk Analysis and Management.

7.1.1.3 Sanction Policy - R

- ✓ Establish appropriate sanctions so that workforce members understand the consequences of failing to comply with security policies and procedures, in order to deter noncompliance.
- ✓ Apply appropriate sanctions against workforce members who fail to comply with the entity's security policies and procedures.

7.1.1.4 Information System Activity Review - R

- ✓ Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

✓ Determine if any ePHI is used or disclosed in an inappropriate manner.

> The review procedures may be different for each Covered Entity, and should be customized to meet the Covered Entity's risk management strategy and take into account the capabilities of all information systems with ePHI.

7.1.2 Assigned Security Responsibility

Section	Implementation Specifications R= Required, A=Addressable	
164.308(a)(2)	None	N/A

This standard requires a CE to identify a security official who will be responsible for the development and implementation of the policies and procedures required by the Security Rule. Covered Entities should be aware of the following when assigning security responsibility:

- This requirement is comparable to the Privacy Rule standard of Personnel Designations (see 4.3.1 Privacy Personnel [45 CFR 164.530(a)]) which requires all Covered Entities to designate a Privacy Official.
- The Security Official and Privacy Official can be the same person, but are not required to be.
- While one individual must be designated as having overall responsibility, other individuals in the CE may be assigned specific security responsibilities (e.g. facility security or network security).

> For simplicity within your organization, we recommend that the Privacy and Security Official be the same person – referred to as the HIPAA Compliance Officer.

7.1.3 Workforce Security

The requirements of this standard are two-fold. According to this standard:

1. A Covered Entity is required to identify which workforce members require access to ePHI as part of their job functions and ensure they have the reliable access (see **7.1.4 Information Access Management**). This will also include identification of the computer systems and applications that provide access to the ePHI. The organization must provide only the minimum necessary access to ePHI that is required for a workforce member to do his or her job.

Section	Implementation Specifications R= Required, A=Addressable	
164.308(a)(3)	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A

2. A Covered Entity must prevent workforce members that do not require access to ePHI from obtaining such access.

Within Workforce Security there are three addressable implementation specifications:

7.1.3.1 Authorization and/or Supervision - A

- ✓ Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where ePHI are accessible.
- ✓ Determine whether a particular user (or a computer system) has the right to carry out a certain activity, such as reading a file or running a program.
- ✓ Consider the size and complexity of the workforce, and the information systems that contain ePHI.

For example, in a small provider office where all staff members may perform multiple functions, they may need to access all ePHI in their information system. In this case, the Covered Entity might document the reasons for implementing procedures and policies that allow for global access. If the documented reasoning is reasonable and appropriate, this approach may be deemed acceptable.

- ✓ Review the authorization and supervision policies already present in the organization's current operating environment, and where appropriate, reinforce these policies, make modifications for ePHI, and/or develop corresponding documentation.

7.1.3.2 Workforce Clearance Procedure - A

- ✓ Develop a procedure by which employees with access to ePHI receive an appropriate clearance level.
- ✓ Establish the clearance procedure as part of the Authorization/Supervision process (see 7.1.3.1 Authorization and/or Supervision - A) or at another appropriate time.

7.1.3.3 Termination Procedures - A

- ✓ Implement procedures to terminate access to ePHI when a workforce member's employment ends (voluntarily or involuntarily) or if the nature of their role requires more or less access to ePHI (see **7.1.3.2 Workforce Clearance Procedure - A**)

7.1.4 Information Access Management

This standard requires a Covered Entity to implement policies and procedures for authorizing access to ePHI in a manner consistent with the pertinent requirements of the Privacy Rule (see **4.1 Use and disclosure of PHI**).

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(a)(4)	Isolating Health Care Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A

As noted in **4.2 Minimum Necessary Principle of Uses and Disclosures**, the Privacy Rule's minimum necessary requirement mandates Covered Entities to restrict access to ePHI to the minimum necessary by evaluating their practices and enhancing their safeguards. A Covered Entity's compliance with the Information Access Management standard needs to be in line with the compliance with the Minimum Necessary Principle.

The Information Access Management standard has three implementation specifications:

7.1.4.1 Isolating Health Care Clearinghouse Functions - R

✓ If a healthcare clearinghouse is part of a larger organization, the former must implement policies and procedures that protect its ePHI from unauthorized access by the latter.

This specification is only required for **healthcare clearinghouses** that are a part of a larger organization, such that they must protect the ePHI they process.

It is not applicable to healthcare providers.

7.1.4.2 Access Authorization - A

✓ Based on whether a person or system has authorization, (see **7.1.3 Workforce Security**), implement policies and procedures to grant access to ePHI through means, such as a:

- workstation
- transaction
- program
- process
- any other mechanism
- Identify the entities with authority to grant access privileges,
- State the process for granting access.

7.1.4.3 Access Establishment and Modification - A

- Implement policies and procedures that are able to modify the access authorizations granted per 7.1.4.2 Access Authorization - A.
- Identify the person or persons with the responsibility of managing these access authorizations.

7.1.5 Security Awareness and Training

This standard states that a Covered Entity must implement a security awareness and training program for all members of its workforce.

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(a)(5)	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A

Training is required:

1. For all new staff members within 10 days of their hire
2. As environmental or operational changes take place that affect the security of ePHI, periodic retraining should also be given (**annual training is recommended**). Changes may include:
   i. new or updated policies and procedures
   ii. new or upgraded software or hardware
   iii. new security technology
   iv. changes in the Security Rule

The Security Awareness and Training standard has four implementation specifications:

7.1.5.1 Security Reminders - A

- ✓ Make periodic security updates/reminders such as:
- ✓ Printed and/or electronic notices
- ✓ Agenda items/discussion topics during meetings
- ✓ Formal retraining on security policies and procedures

7.1.5.2 Protection from Malicious Software - A

- ✓ Implement procedures and security software to detect, guard against, and report malicious software.
- ✓ Train the workforce on such programs since malicious software can enter a Covered Entity's system through email attachments or downloads from the internet.

Malicious software includes any program that can harm information systems like viruses, worms, etc.

7.1.5.3 Log-In Monitoring - A

- ✓ Implement procedures to monitor login attempts and report discrepancies.
- ✓ Make workforce members aware of inappropriate log-in attempts.
- ✓ Establish the capabilities of its system and train its workforce in using and monitoring it.

An **inappropriate login attempt** is typically when an individual enters multiple combinations of usernames and passwords in order to access the system,

Many information systems have the capability to identify, record, or prevent such attempts by requiring a password reset.

7.1.5.4 Password Management - A

- ✓ Implement procedures to create, change, and safeguard passwords.

- ✓ Train the workforce on safeguarding ePHI by creating passwords and changing them periodically.

7.1.6 Security Incident Procedures

This standard states that Covered Entities must implement policies and procedures to address security incidents. While implementing the Security Rule standards will reduce the type and amount of security incidents a Covered Entity encounters, security incidents may nonetheless occur for all Covered Entities, regardless of their size and capabilities.

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(a)(6)	Response and Reporting	R

A **security incident** occurs as a result of attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Examples of security incidents include:

- Inappropriately obtained passwords that are used to access ePHI
- Corrupted backup tapes that do not allow restoration of ePHI
- Malicious software attacks
- Physical break-ins leading to the theft of media with ePHI
- Unauthorized access to information systems with ePHI by a former employee

Security incident procedures must address how to identify these incidents and report them to the appropriate person(s).

A Covered Entity must rely on the information gathered in complying with the other Security Rule standards (like risk assessment and management procedures and the privacy standards) to define what constitutes a security incident in its own context, since the definition of a security incident, its documentation process and appropriate response depend on the entity's environment and the information involved.

There is one required implementation specification for this standard:

7.1.6.1 Response and Reporting - R

- ✓ Identify and respond to suspected or known security incidents
- ✓ Mitigate, to the extent practicable, any known harmful effects of security incidents
- ✓ Document security incidents and their outcomes
- ✓ Evaluate security incidents as part of ongoing risk management

7.1.7 Contingency Plan

This standard requires a Covered Entity to establish, and implement as needed, policies and procedures for responding to an emergency or other occurrence—for example, fire, vandalism, system failure, and natural disaster—that damages systems that contain ePHI. The goal is to ensure that organizations have their ePHI available when it is needed.

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(a)(7)	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedures	A
	Applications and Data Criticality Analysis	A

The Contingency Plan standard includes five implementation specifications:

7.1.7.1 Data Backup Plan - R

- ✓ Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

7.1.7.2 Disaster Recovery Plan - R

- ✓ Establish, and implement as needed, procedures to restore any loss of data.
- ✓ Review the existing general disaster recovery plan (if one exists) to ensure that it allows the recovery of ePHI.

7.1.7.3 Emergency Mode Operation Plan - R

- ✓ Establish, and implement as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode (such as a technical failure or power outage).

7.1.7.4 Testing and Revision Procedures - A

- ✓ Implement procedures for periodic testing and revision of all contingency plans including the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.
- ✓ In order to test the disaster recovery and emergency mode operations plans, a Covered Entity can use a scenario-based walk-through or perform complete live tests.
- ✓ Each Covered Entity must determine the comprehensiveness and sophistication of the testing and revision procedures depending on the complexity of its organization, its size and associated costs.

7.1.7.5 Applications and Data Criticality Analysis - A

- ✓ Assess the relative criticality of specific applications and data in support of other contingency plan components.

- ✓ Determine the importance of each software application to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plans.

7.1.8 Evaluation

A Covered Entity must implement ongoing monitoring and evaluation of its strategy and systems to ensure that the security requirements continue to adequately protect its ePHI within their organizations' operating environments. While this standard has no separate implementation specifications, it requires all Covered Entities to:

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(a)(8)	None	N/A

- ✓ perform a periodic technical and nontechnical evaluation:
  - based initially on the standards implemented under this rule
  - and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.
  - the ongoing evaluation should also be performed on a scheduled basis, e.g. annually or every two years.

7.1.9 Business Associate Contracts and Other Arrangements

Sections	Implementation Specifications R= Required, A=Addressable	
164.308(b)(1)	Written Contract or Other Arrangement	R

This standard states that a Covered Entity may permit a Business Associate to create, receive, maintain, or transmit ePHI on the Covered Entity's behalf only if the Covered Entity obtains satisfactory assurances that the Business Associate will appropriately safeguard the information in the form of a contract or other arrangement.

Covered Entities must enter into a contract or other arrangement with persons that meet the definition of Business Associate (see **2.2 Business Associates**). This standard is comparable to the Business Associate Contract standard in the Privacy Rule (see **2.2.1 Business Associate Contracts**) , but is specific to Business Associates that create, receive, maintain or transmit ePHI. To comply with this standard, Covered Entities must obtain satisfactory assurances from the business associate that it will appropriately safeguard ePHI.

> If a CE is acting as a BA of another CE, it is also subject to the requirements of this standard.

The organizational requirements related to this standard are discussed in more detail in **7.4 Organization, Policies and Procedures and Documentation Requirements**.

The standard has one required implementation specification, as outlined in the table above.

7.1.9.1 Written Contract or Other Arrangement

- ✓ Document the satisfactory assurances required by the Business Associate Contracts and Other Arrangements through a written contract or other arrangement with the Business Associate that meets the applicable requirements of the Organizational Requirements (see **7.4.1 Business Associate Contracts or Other Arrangements**).

7.1.9.2 When BA contracts are not needed

7.1.9 Business Associate Contracts and Other Arrangements addresses a few situations in which a BA contract is not needed.

- The transmission of ePHI by a CE to a health care provider regarding an individual's treatment.
- The transmission of ePHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of 164.314(b) and 164.504(f) apply and are met

The transmission of ePHI from or to other agencies providing the services at 164.502(e)(1)(ii)(C), when the Covered Entity is a health plan that is a government program providing public benefits, if the requirements of 164.502(e)(1)(ii)(C) are met."

7.2 Physical Safeguards

Physical safeguards are defined as physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

The physical safeguards standards require Covered Entities to evaluate their existing security controls, analyze risks, and determine and document solutions specific to their organization. When evaluating and implementing these standards, a Covered Entity must consider all physical access to ePHI, which may extend outside of an actual office (and could include workforce members' homes or other physical locations where they access ePHI).

7.2.1 Facility Access Controls

Sections	Implementation Specifications R= Required, A=Addressable	
164.310(a)(1)	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A

This standard requires a Covered Entity to implement policies and procedures to limit physical access to its electronic information systems and the **facility** or **facilities** in which they are housed, while ensuring that proper and authorized access is allowed.

A **facility** is defined as the physical premises and the interior and exterior of a building or buildings.

The Facility Access Controls standard has four implementation specifications:

7.2.1.1 Contingency Operations - A

- Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan (see **7.1.7.2 Disaster Recovery Plan - R**) and emergency mode operations plan (see **7.1.7.3 Emergency Mode Operation Plan - R**) in the event of an emergency.
    - Contingency operations may be set in motion during or immediately after a disaster or emergency situation. It is important to maintain physical security and appropriate access to ePHI during contingency operations, while allowing for data restoration activities.
    - Facility access controls during contingency operations will vary among Covered Entities. For example, a large organization may need to post guards at entrances to the facility or have escorts for individuals authorized to access the facility for data restoration purposes. For smaller to medium-sized practices, it may be sufficient to have all staff involved in the recovery process.

7.2.1.2 Facility Security Plan - A

- Implement policies and procedures to safeguard the facility and the equipment inside it from unauthorized physical access, tampering and theft.
- The Risk Assessment results (see 7.1.1.1 Risk Analysis - R and 7.1.1.2 Risk Management - R) should be used and referred to in order to create a facility security plan.

Examples of procedures to prevent unauthorized physical access, tampering, and theft are:

- Locked doors, signs warning of restricted areas, surveillance cameras, alarms
- Property controls such as property control tags, engraving on equipment
- Personnel controls such as identification badges, visitor badges and/or escorts for large offices

- Train workforce members on their roles in upholding facility security.
- Review and update the facility security plan when there are any significant changes to the facility or systems.

7.2.1.3 Access Control and Validation Procedures - A

- Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
- Align individual access to ePHI with each person's role or function within the organization (in line with 7.2.1.2 Facility Security Plan - A).

For example:

- In a larger organization, for example, it may be necessary to question each person's identity by checking picture ID before every visit,
- In a smaller office, it may be sufficient to verify identity once.

7.2.1.4 Maintenance Records - A

- Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors and locks).
- Documenting these device repairs, additions or removals may also be necessary to meet this specification.

For example:

- For a smaller office - a simple logbook of dates, reasons for repair or modification and person authorizing.
- For a larger organization - documenting repairs or modifications in more detail and maintaining them in a database.
- The most frequently implemented change may be changing door locks or combinations in the event of a staff termination.

7.2.2 Workstation Use

Sections	Implementation Specifications R= Required, A=Addressable	
164.310(b)	None	N/A

A **workstation** is defined in the rule as "an electronic computing device, for example, a laptop or desktop computer, and electronic media stored in its immediate environment." These workstations can either be within the Covered Entity's facilities, or off-site at employees' homes, satellite offices, or another facility.

While this standard has no implementation specifications, like all standards, it must be implemented (according to the below guidance):

- Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

- Specify the appropriate functions that electronic computing devices need to perform, since the inappropriate use of computer workstations can cause risks like virus attacks, compromise of information systems, and breaches of confidentiality.

For example, common practices that may already be in place include:

- logging off before leaving a workstation for an extended period of time
- using and continually updating antivirus software

7.2.3 Workstation Security

This standard requires that Covered Entities:

Sections	Implementation Specifications R= Required, A=Addressable	
164.310(c)	**None**	**N/A**

- Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. For example:
  - Keep workstations in a secure room with access only to authorized personnel
  - Password protect computers with ePHI
- Use the risk analysis to help determine which employees should have access to the workstations with ePHI.

7.2.4 Device and Media Controls

This standard requires a Covered Entity to implement policies and procedures that govern the receipt and removal of hardware and **electronic media** that contain ePHI, into and out of a facility, and the movement of these items within the facility.

This standard covers the proper handling of **electronic media**:

Sections	Implementation Specifications R= Required, A=Addressable	
164.310(d)(1)	Disposal	R
	Media Re-use	R
	Accountability	A
	Data Backup and Storage	A

> **Electronic media** means electronic storage media including hard drives and any removable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

7.2.4.1 Disposal - R

- Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
- When Covered Entities dispose of any electronic media that contains ePHI they should make sure it is unusable and/or inaccessible.

> Example of disposal methods:
>
> - Degaussing - a method whereby a strong magnetic field is applied to magnetic media to fully erase the data.
> - Physically damage it beyond repair, making the data inaccessible.

7.2.4.2 Media Re-use - R

- Implement procedures for removal of ePHI from electronic media before the media are made available for re-use (whether **internal or external**).

Internal vs. External Re-Use

- Internal re-use may include re-deployment of PCs or sharing CDs, DVDs or hard drives.
- External re-use may include donation of electronic media to charity organizations or local schools.

7.2.4.3 Accountability - A

- Maintain a record of the movements of hardware and electronic media and any person responsible for such movements.
    - If hardware and media containing ePHI are moved from one location to another, a record should be maintained as documentation of the move.
    - For example, tracking the serial numbers of portable workstations and media.

7.2.4.4 Data Backup and Storage - A

- Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.
    - This specification is similar to the **7.1.7.1 Data Backup Plan - R** implementation specification but is specifically regarding data backups prior to *moving* equipment. Both implementation specifications may be included in the same policies and procedures.
    - For example:
- Backup a hard drive before moving to prevent loss of ePHI when the existing data backup plan does not provide for local hard drive backups.

- Implement policies that require users to save all information on the network, thus eliminating the need for a hard drive back up prior to the move.

7.3 Technical Safeguards

The Security Rule defines technical safeguards as the technology, its policy and procedures that protect ePHI and control access to it.

With the recent technological advancements in the health care industry, technical safeguards are becoming increasingly more important. There are many technical security tools, products, and solutions that a Covered Entity may select, and determining the right security measure to implement is a decision that the entity must make based on what is reasonable and appropriate for its specific unique characteristics.

7.3.1 Access Control

Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files.

Sections	Implementation Specifications R= Required, A=Addressable	
164.312(a)(1)	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A

The Access Control standard requires a Covered Entity to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the **7.1.4 Information Access Management**.

The Security Rule defines **access** as the "ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."

This definition applies to "access" as used as related to the security rule.

Four implementation specifications are associated with the Access Controls standard:

7.3.1.1 Unique User Identification - R

- Assign a unique name and/or number for identifying and tracking user identity.
- Track specific user activity when that user is logged into an information system.
- Hold users accountable for functions performed on information systems with ePHI when logged into those systems.

There is no single format for user identification. Some examples include:

- Variation of name (e.g. jsmith)
- Random numbers and characters

7.3.1.2 Emergency Access Procedures - R

- Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
- Include the instructions and operational practices for obtaining access to necessary ePHI as part of the 7.1.7.3 Emergency Mode Operation Plan - R.

7.3.1.3 Automatic Logoff - A

- Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

7.3.1.4 Encryption and Decryption - A

- Implement a mechanism to encrypt and decrypt ePHI.
    - **Encryption** is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (i.e., type of procedure or formula).
    - **Decryption** (i.e., translation) is a method of taking encrypted text and converting it into plain, comprehensible text.
    - If information is encrypted, it lowers the probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to access it.

7.3.2 Audit Controls

This standard requires a Covered Entity to:

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Sections	Implementation Specifications R= Required, A=Addressable	
164.312(b)	None	N/A

    - These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred.
    - Most information systems provide some level of audit controls with a reporting method, such as audit reports.
    - The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed – this is at the discretion of the CE. Consider your risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.

7.3.3 Integrity

Integrity is defined in the Security Rule as the property that data or information have not been altered or destroyed in an unauthorized manner. Protecting the integrity of ePHI is a primary goal of the Security Rule (see *Table 10: Security Rule Definitions of Integrity, Availability, and Confidentiality*).

Sections	Implementation Specifications R= Required, A=Addressable	
164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	A

The Integrity standard requires a Covered Entity to implement policies and procedures to protect ePHI from improper alteration or destruction regardless of the source. Integrity of ePHI can be affected by both technical and non-technical sources. Such as:

- Non-technical: workforce members or Business Associates may make accidental or intentional changes that improperly alter or destroy ePHI
- Technical: data can be altered or destroyed by electronic media errors or failures

There is one addressable implementation specification in the Integrity standard:

7.3.3.1 Mechanism to Authenticate Electronic Protected Health Information - A

- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. For example:
  - Validation of digital signatures
  - Checksum verification

Checksum verification is a process of using an algorithm to verify the integrity of a computer file.

- Consider the various risks to the integrity of ePHI identified during the risk analysis.

7.3.4 Person or Entity Authentication

This standard requires a Covered Entity to:

Sections	Implementation Specifications R= Required, A=Addressable	
164.312(d)	**None**	**N/A**

- Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. This is similar to the requirement of CEs to perform **5.2.3.3 Verification** that the individual requesting access to PHI is either the individual that is the subject of the PHI or their personal representative
- A CE may require:
  - Something known only to that individual, such as a password or PIN.
  - Something that individuals possess, such as a smart card, a token, or a key.
  - Something unique to the individual such as a biometric, e.g. fingerprints, voice patterns, facial patterns or iris patterns.

7.3.5 Transmission Security

This standard requires a CE to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Sections	Implementation Specifications R= Required, A=Addressable	
164.312(e)(1)	Integrity Controls	A
	Encryption	A

In order to determine the technical security measures to implement to comply with this standard, Covered Entities must:

Review the current methods used to transmit ePHI. For instance, is ePHI transmitted through:

- email
- over the Internet
- some form of private or point-to-point network

Identify the available and appropriate means to protect ePHI as it is transmitted, select appropriate solutions, and document its decisions.

A CE should discuss reasonable and appropriate security measures with its IT professionals.

The Security Rule allows for ePHI to be sent over an electronic open network as long as it is adequately protected.

This standard has two implementation specifications:

7.3.5.1 Integrity Controls - A

- Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
    - Integrity (see **7.3.3 Integrity**) in this context refers ensuring that ePHI is not improperly modified during transmission.
- Utilize integrity controls such as:
    - network communications protocols
    - data or message authentication codes

7.3.5.2 Encryption - A

- Implement a mechanism to encrypt ePHI whenever deemed appropriate (see 7.3.1.4 Encryption and Decryption - A for more information on encryption).
- Consider the following factors:

- for encryption technologies to work properly when data is being transmitted, both the sender and receiver must be using the same or compatible technology
- discuss reasonable and appropriate security measures for the encryption of ePHI during transmission over electronic communications networks with its IT professionals
- the use of encryption for transmitting ePHI, particularly over the Internet where risk analysis shows such risk to be significant.

7.4 Organization, Policies and Procedures and Documentation Requirements

These standards require a Covered Entity to have contracts or other arrangements with Business Associates that will have access to the Covered Entity's ePHI. The standards provide the specific criteria required for written contracts or other arrangements.

7.4.1 Business Associate Contracts or Other Arrangements

This standard requires a Covered Entity to have contracts or other arrangements with business associates that will have access to the Covered Entity's ePHI. As long as the requirements are addressed, the actual language used can be customized to the needs of each Covered Entity.

Sections	Implementation Specifications R= Required, A=Addressable	
164.314(a)(1)	Business Associate Contracts	R
	Other Arrangements	R

In general, a business associate is a person or entity outside of the Covered Entity's workforce that performs functions or activities on behalf of the Covered Entity, or provides specified services to the Covered Entity, that involve the use or disclosure of PHI. A business associate may also be another Covered Entity.

For more information on Business Associates, see **2.2 Business Associates.** For more information on Business Associate contracts, see **2.2.1 Business Associate Contracts**

This standard has two implementation specifications:

7.4.1.1 Business Associate Contracts - R

- CEs must create a Business Associate contract that:
- Ensures that the BA will appropriately and reasonably implement the requirements of the HIPAA Security Rule with regards to ePHI it uses or discloses on behalf of the CE
- Ensures that if the BA provides ePHI to another third party, that party too implements the requirements of the HIPAA Security Rule with regards to ePHI it uses or discloses
- Reports any security incident of which it becomes aware to the Covered Entity
- Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the business associate has violated a material term of the contract.

> Note: this implementation specification may not apply to many healthcare providers. If it is not applicable, it can be documented as such in the **Documentation Kit**.

7.4.1.2 Other Arrangements - R

If a Covered Entity and its Business Associate are both **government entities**, the Covered Entity may comply with the standard in either of two alternative ways:

1. if it enters into a memorandum of understanding (MOU) with the Business Associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section above
2. if other law (including regulations adopted by the Covered Entity or its business associate) contain requirements applicable to the Business

Associate that accomplish the objectives of the Business Associate contract. If statutory obligations of the Covered Entity or its Business Associate do not permit the Covered Entity to include in its other arrangements authorization of the termination of the contract by the Covered Entity, the termination authorization may be omitted.

7.4.2 Requirements for Group Health Plans

Sections	Implementation Specifications R= Required, A=Addressable	
164.314(b)(1)	Implementation Specifications	R

The standard requires a group health plan to ensure that its plan documents require the plan sponsor to reasonably and appropriately safeguard ePHI that it creates, receives, maintains or transmits on behalf of the group health plan. Specific exceptions to this requirement are provided when the only ePHI disclosed to a plan sponsor is disclosed pursuant to permitted disclosures under the HIPAA Privacy Rule, see **4.1.1 Permitted Uses and Disclosures**.

The standard includes the following required implementation specification:

7.4.2.1 Implementation Specifications - R

The plan documents of the group health plan must incorporate provisions to require the plan sponsor to:

1. Implement the HIPAA Security Rule safeguards in a manner that is reasonable and appropriate to protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan
2. Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
3. Report to the group health plan any security incident of which it becomes aware."

4. If the plan sponsor of a group health plan has access to ePHI beyond summary information and enrollment information or to ePHI, the plan documents must contain language similar to that already required by the Privacy Rule.

7.4.3 Policies and Procedures

This standard required Covered Entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

Sections	Implementation Specifications R= Required, A=Addressable	
164.316(a)	None	N/A

A Covered Entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

The Security Rule does not define either "policy" or "procedure." *Table 11: Explanation of Policy and Procedure* provides further explanation on what is considered a "policy" and "procedure".

Policy	Procedure
Generally, policies define an organization's approach. **For example, most business policies establish measurable objectives and expectations for the workforce, assign responsibility for decision-making, and define enforcement and consequences for violations.**	Procedures describe *how* the organization carries out that approach. Procedures set forth explicit, step-by-step instructions that implement the organization's policies.

Table 11: Explanation of Policy and Procedure

7.4.4 Documentation

The Documentation standard requires Covered Entities to:

Maintain the policies and procedures implemented to comply with the Security Rule in written or electronic form.

Maintain a written or electronic record of the action, activity, or assessment if required by the Security Rule to be documented.

Sections	Implementation Specifications R= Required, A=Addressable	
164.316(b)(1)	Time Limit	R
	Availability	R
	Updates	R

The Documentation standard has three implementation specifications:

7.4.4.1 Time Limit - R

- Retain the documentation described in **7.4.4 Documentation** for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

- This six-year period must be considered the minimum retention period for required documentation under the Security Rule.
- You may choose to keep their documentation longer based on state law, requirements of accreditation organizations, or other business reasons.

7.4.4.2 Availability - R

- Make documentation available (in written or electronic form) to those persons responsible for implementing the procedures to which the documentation pertains.

7.4.4.3 Updates - R

- Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.
- The Security Rule does not stipulate a set review cycle.
- The review frequency depends on the volume of the CE's environmental or operational changes that affect the security of ePHI.

It is recommended that CEs review their HIPAA policies and procedures on an annual basis.

This page intentionally left blank

8 What is the Breach Notification Rule?

What to do in the event of a data breach

This Chapter details what healthcare providers must do in the event there is an unauthorized use or disclosure of protected health information or electronic health information that compromises the information's privacy and/or security. Such an event is known as a **"breach"** (see **8.1 What is a Breach?**). The steps that a healthcare provider must take in the event of a breach are outlined in **8.2 Breach Notification Requirements**. There are some cases in which a breach of protected health information does not require a Covered Entity to take breach notification steps. These cases are outlined in **8.1.1 Disqualification of a breach**, **8.1.2 Exceptions to the definition of a breach** and **8.1.3 Unsecured PHI and Guidance.**

.

8.1 What is a Breach?

A breach is usually an impermissible use or disclosure of PHI that compromises the PHI's privacy and/or security. An impermissible use or disclosure of PHI is one that occurs in a manner that is not permitted by the Privacy Rule (see **4.1.1 Permitted Uses and Disclosures**).

In certain circumstances, an impermissible use or disclosure of PHI may be *disqualified* as a breach or an *excepted* from the definition of a breach. These cases are explained in **8.1.1 Disqualification of a breach** and **8.1.2 Exceptions to the definition of a breach**.

8.1.1 Disqualification of a breach

A breach may be disqualified as such if the CE or BA (as applicable) demonstrates that there is a low probability that the PHI has been compromised. This is achieved by performing a risk assessment with at least the following factors:

See the Documentation Kit for a worksheet that can be used to complete a risk assessment in the event of a breach.

1. The nature and extent of the PHI in question, including
    a. the types of identifiers within it (see 3.1.2.2 Safe Harbor)
    b. the probability of re-identification (see 3.1.2.3 Re-identification)
2. The unauthorized individual who used the PHI or to whom the PHI was disclosed
3. Whether the PHI was in fact acquired or viewed
4. How much the risk to the PHI has been mitigated

If Covered Entities and/or Business Associates decide to forgo the process of evaluating whether a breach may be disqualified and perform the Breach Notification activities, a risk assessment is not required.

8.1.2 Exceptions to the definition of a breach

There are exceptions to what constitutes a breach:

1. the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. the inadvertent disclosure of PHI by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the CE or BA, or organized health care arrangement (see **2.3.3 Organized Health Care Arrangement (OHCA)**) in which the CE participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
3. the CE or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.
4. the breach does not involve unsecured PHI (see 8.1.3 Unsecured PHI and Guidance)

8.1.3 Unsecured PHI and Guidance

CEs and BAs are only required to provide notifications if the breach involved **unsecured PHI**.

Unsecured PHI is PHI that has not been rendered *unusable, unreadable, or indecipherable* to unauthorized individuals using a methodology or technology that the HHS Secretary specified.

PHI will be considered *unusable, unreadable, or indecipherable* to unauthorized individuals if one or more of the following applies:

1. ePHI has been encrypted and such confidential process or key that might enable decryption has not been breached (see 7.3.1.4 Encryption and Decryption - A).
    a. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.
    b. Refer to the Welcome Kit for valid encryption processes consistent with the National Institute of Standards and Technology
        i. NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices
        ii. NIST Special Publications 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
        iii. NIST Special Publications 800-77: Guide to IPsec VPNs
        iv. NIST Special Publications 800-113: Guide to SSL VPNs
        v. Others which are Federal Information Processing Standards (FIPS) 140-2 validated

    Refer to the Welcome Kit for these special publications from NIST.

    c. It is highly recommended that Covered Entities consult with their IT representative in regard to encrypting PHI.

2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
    a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or reconstructed. Redaction is specifically not considered an appropriate means of data destruction.
    b. Electronic media have been cleared, purged, or destroyed such that PHI cannot be retrieved (see 7.2.4.1 Disposal - R).
        i. Refer to the Welcome Kit for media disposition processes consistent with NIST (NIST Special Publication 800-88: Guidelines for Media Sanitization).

Refer to the Welcome Kit for these special publications from NIST.

8.2 Breach Notification Requirements

Should a breach occur, a Covered Entity is required to notify the following parties:

1. The affected individuals (see 8.2.1 Notice to the Individual)
2. The Secretary of the Department of Health and Human Services (see 8.2.2 Notice to the HHS Secretary)
3. The media (see 8.2.3 Notice to the Media) (in certain cases)

State law may also require additional parties be notified. Refer to your Documentation Kit for details.

Additionally, Business Associates must notify their Covered Entities should a breach occur at or by the BA (**8.2.4 Notification by a BA**).

8.2.1 Notice to the Individual

8.2.1.1 Responsible parties

In the event of a breach, CEs are responsible for providing notice to the affected individuals. If a breach occurs at or by a BA, the CE is ultimately responsible for

ensuring individuals are notified, but the CE can also delegate this responsibility to the BA. Depending on the circumstances, including which organization has the relationships in place, the CE and BA can determine which entity is best equipped to provide the appropriate notice.

8.2.1.2 Manner of providing notice

CEs are required to provide notice to affected individuals in the following ways:

1. Written form by first-class mail, or by email if the individual in question has agreed to receive such notices electronically.
2. If the CE does not have access to sufficient or recent contact information for 10 or more affected individuals, it is required to provide another form of notice by either posting it on its website's main page for at least 90 days or providing the notice in major print or broadcast media where the individuals probably live.
3. The CE must also include a toll-free number for at least 90 days for individuals to call in order to learn if their information was involved in the breach.
4. If there are less than 10 individuals with insufficient or out-of-date contact information, the CE may provide substitute notice by an alternative form of written notice, by telephone, or other means.

8.2.1.3 Timeframe to provide notice

All such notices must be provided within a reasonable timeframe and never over 60 days after the discovery or a breach. The notifications must include, as much as possible:

1. A brief description of the breach and the types of information involved in it
2. What steps individuals need to take to protect themselves from any potential harm
3. What the CE is doing to investigate the breach, manage the harm, and prevent further breaches
4. Contact information for the CE or BA when applicable

8.2.2 Notice to the HHS Secretary

8.2.2.1 When to notify the HHS Secretary

CEs must notify the HHS Secretary in the event of a breach in the following manner:

1. If the breach affects **fewer than 500 individuals**, the CE may provide an annual notice of breaches to the Secretary. These reports are due to the Secretary no later than 60 days after the end of the calendar year in which the breach was discovered.
2. If the breach affects **over 500 individuals**, the CE must notify the Secretary without unreasonable delay and no later than 60 days following the breach.

If the CE is uncertain of the number of individuals affected by a breach at the time that the breach was discovered, they may make an initial estimate and act accordingly with the number estimated. The, if at a later time, the number changes, they should update their response accordingly.

8.2.2.2 How to notify the HHS Secretary

All notifications to the HHS Secretary of breaches must be submitted using the Department of Health and Human Services Office for Civil Rights web portal. A notice must be submitted for each instance of a breach.

1. For breaches affecting fewer than 500 individuals, submit a notice here[19].
2. For breaches affecting over 500 individuals, submit a notice here[20].

19 https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

20 https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

8.2.2.3 HHS responsibility to post breaches

Section 13402(e)(4) of the HITECH Act requires the HHS Secretary to post a list of breaches of unsecured PHI affecting 500 or more individuals. This list may be viewed here[21].

8.2.3 Notice to the Media

8.2.3.1 When to notify the media

If a breach affects more than 500 residents of a State or jurisdiction, the CE is required to provide notice to prominent media outlets serving that area as well as the affected individuals.

8.2.3.2 How to notify the media

Notification to the media must include the same information that is provided in the notice to the affected individuals and may be in the form of a press release.

8.2.3.3 Timeframe to notify the media

Notification must be without unreasonable delay and never later than 60 days after the discovery of a breach.

8.2.4 Notification by a BA

If a breach occurs at or by a BA, it must provide notice to the CE of the breach.

8.2.4.1 Timeframe to notify the CE

The BA must provide notice to the CE after the discovery of such a breach without unreasonable delay and never later than 60 days after.

21 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

8.2.4.2 How to notify the CE

The BA should provide the CE with the identification of each affected individual and any other available information the CE would need to provide individuals in its notifications.

8.2.4.3 Additional notification responsibilities

If a breach occurs at or by a BA, the **CE** is ultimately responsible for ensuring individuals are notified, but the CE can also delegate this responsibility to the BA. Depending on the circumstances, including which organization has the relationships in place, the CE and BA can determine which entity is best equipped to provide the appropriate notice.

8.2.5 Burden of Proof

CEs or BAs (when applicable) have the burden of proof in regard to breach notifications. This means that:

1. They must demonstrate that all required notices have been provided and provide documentation as such
2. *Or* that the use or disclosure of unsecured PHI did not constitute a breach and provide documentation to demonstrate that notification was not required (see **8.1.1 Disqualification of a breach** and **8.1.2 Exceptions to the definition of a breach**)

8.2.6 Administrative Requirements

CEs must comply with certain administrative requirements regarding breach notification. For example, CEs must:

1. have written policies and procedures in place regarding breach notification (see 7.4.3 Policies and Procedures)
2. must train their workforce about these policies and procedures (see 7.1.5 Security Awareness and Training)

3. must develop and apply appropriate sanctions for those not complying with these policies and procedures (see 7.1.1.3 Sanction Policy - R)

This page intentionally left blank

9 How is HIPAA compliance enforced?

HIPAA enforcement activities by the Office for Civil Rights

CEs and BAs are expected to give an honest effort to comply with HIPAA regulation. However, the Department of Health and Human Services Office for Civil Rights (OCR), has the responsibility and authority to administer and enforce the HIPAA requirements. The process that OCR follows to enforce HIPAA is detailed in **9.1 HIPAA Enforcement Process**. Should a CE fail to comply with HIPAA standards voluntarily, they may be subject to penalties (see **9.3 Penalties**).

The OCR's authority, HIPAA Enforcement Process, and penalties are driven from the HIPAA Enforcement Rule (45 CFR Part 160, Subparts C, D, and E).

HR 7898 (now Public Law No: 116-321) amended the HITECH Act to allow enforcement discretion on the length/outcome of audits, amounts of fines, or extent of penalties if a healthcare entity has adopted cybersecurity best practices. While this change does not prevent OCR from imposing fines/penalties, entities that find themselves the subject of an audit/investigation should see advantages if they have already adopted recognized cybersecurity best practices.

9.1 HIPAA Enforcement Process

OCR enforces HIPAA requirements in one of the following manners:

1. investigating complaints that are filed (see 9.1.1 Complaints)
2. conducting compliance audits of CEs and BAs (see 9.1.2 Compliance Audits)
3. conducting compliance reviews of CEs and BAs (see 9.1.3 Compliance Reviews)

OCR also coordinates education and outreach programs to promote HIPAA awareness and compliance.

If the CE does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose penalties (see **9.3 Penalties**).

9.1.1 Complaints

Any individual may file a health information privacy and security complaint with the (OCR) if they feel that a CE or BA violated his/her or someone else's health information privacy rights or committed another violation of the Privacy, Security or Breach Notification Rules (see **5.9 Right to Make Complaints**).

OCR processes complaints according the flowchart in **Figure 7: HIPAA OCR Complaint Handling Process**.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to the Department of Justice (DOJ) for investigation.

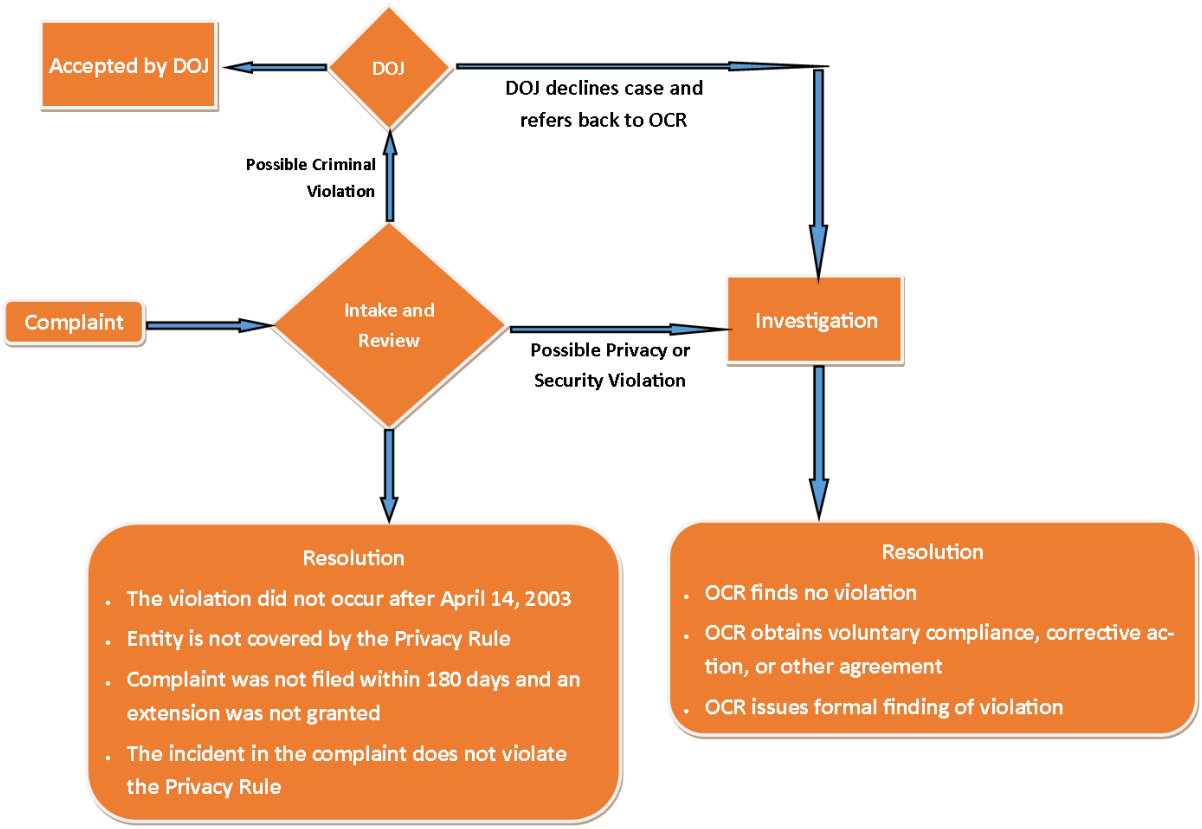

Figure 7: HIPAA OCR Complaint Handling Process[22]

Let's examine the different stages of this process.

9.1.1.1 Complaint Intake and Review

By the Complaint Intake and Review process, OCR reviews all the complaints it receives. However, under HIPAA, OCR may only take action on complaints that meet certain conditions:

1. The alleged action must have taken place after the dates the Rules took effect.

22 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

a. Compliance with the Privacy Rule was not required until **April 14, 2003**.
b. Compliance with the Security Rule was not required until **April 20, 2005**.
c. OCR cannot investigate complaints about actions that took place before these dates.

2. The complaint must be filed against a CE or BA that is legally required to comply with HIPAA regulation.
   a. HIPAA regulations must apply to the entity in question (see 1.3 Governing Bodies)
   b. For example, the following entities may not be required to comply by law:
      i. life insurers
      ii. employers
      iii. workers compensation carriers
3. The incident that is the subject of the complaint must violate HIPAA regulations.
   a. For example, OCR generally could not investigate a complaint that alleged that a physician sent a person's demographic information to an insurance company to obtain payment, because the Privacy Rule generally permits doctors to use and disclose such information to bill for their services.
4. Complaints **must be filed within 180 days** of when the person submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule.
   a. OCR may waive this time limit if it determines that the person submitting the complaint shows good cause for not submitting the complaint within the 180-day time frame.

9.1.1.2 Complaint Investigation

If OCR accepts a complaint for investigation, it will notify the person who filed the complaint and the CE named in it. Then the complainant and the CE are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. CEs are required by law to cooperate with complaint investigations.

> Due to the complexity of some cases, and the evidence needed to understand and/or prove indications of noncompliance, most investigations can take multiple years to investigate and resolve.

OCR reviews the information or evidence that it gathers in each case. In some cases, it may determine that the CE did not violate HIPAA requirements. However, if the evidence indicates that the CE was not in compliance, OCR will attempt to resolve the case with the CE by obtaining:

1. Voluntary compliance
2. Corrective action
3. Resolution agreement

Most Privacy and Security Rule investigations are concluded to the satisfaction of OCR through these types of resolutions. OCR provides notification of the resolution result to both the complainant and the CE.

9.1.1.3 Complaint Closure

The process that OCR follows to close cases is detailed in **9.2 OCR Closure of Cases**.

9.1.2 Compliance Audits

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires the OCR to conduct periodic audits of Covered Entities and Business Associates.

> OCR has developed protocols and informational material regarding their audit process. See the Welcome Kit for these documents.

The purpose of the audit program is to:

1. assess the HIPAA compliance of the entities covered by HIPAA
2. examine the mechanisms for compliance
3. identify best practices
4. discover risks and vulnerabilities to PHI and ePHI

Ultimately, the audit program is an important part of OCR's overall health information privacy, security, and breach notification compliance activities.

This section details OCR's audit process and provides other information regarding the audit program.

9.1.2.1 Eligibility for Audit

Any Covered Entity or Business Associate may be audited. CEs or BAs that are selected to be audited will receive an audit notification letter from OCR via email. OCR will not audit entities that have an open complaint investigation or who are currently undergoing a compliance review.

9.1.2.2 Basis for Audit Selection

OCR selects entities to audit from a wide range of health care providers, health plans, clearinghouses and Business Associates. This is to better assess HIPAA compliance across the industry by viewing a range of size, type and operations of the audit candidates. Sampling criteria includes:

- Size and type of the entity
- Affiliation with other healthcare organizations
- Whether the organization is public or private
- Geographic factors

9.1.2.3 Selection Process

OCR will may request a potential auditee's contact information or use publicly available information. Audit candidates are then asked to complete a questionnaire designed to gather data about the size, type and operations of the CE or BA. This data is used by OCR to develop pools of potential auditees.

See the Welcome Kit for a sample audit questionnaire.

OCR asks CEs to identify their BAs. We recommend maintaining the Business Associate Listing (see **2.2.2 Business Associate Listing**)

Note: if an entity does not respond to the questionnaire or to a request from OCR for information, OCR will use publicly available information about the entity. The entity may still be subject to an audit.

9.1.2.4 Audit Process

OCR conducts both desk and onsite audits for CEs and BAs.

- **Desk audits** involve audited entities submitting documents online via OCR's secure audit portal.
- **Onsite audits** involve in-person auditors who will review the CE's or BA's compliance with the Privacy, Security and Breach Notification Rules.

IMPORTANT:

1. The scope of the audit program does not include State-Specific Privacy and Security Rules. State specific rules are enforced by the relevant state agency.
2. HHS is responsible for the costs of the audit programs; CEs and BAs are not required to bear this cost.

After both types of audits, auditors will develop and share draft findings with the auditee. The entity will then have the opportunity to review and respond to these findings; their written responses will be included in the final audit report along with a description of how the audit was conducted.

9.1.2.5 Audit Timeline

1. OCR expects CEs that are the subject of an audit to respond to OCR's requests for information via the secure audit portal within 10 business days of the date of the request.
2. If auditees would like to provide a response to an auditor's audit findings to be included in the final audit record, they have 10 business days from the time the first draft of findings is made available to them.
3. The auditor will complete a final audit report for each audited entity within 30 business days after receiving the auditee's response.
4. An onsite audit will be conducted over 3 to 5 days onsite, depending on the size of the entity.

9.1.2.6 Post-Audit

OCR reviews and analyzes information from final audit reports to better understand CE's and BA's compliance efforts. They use this information to determine what type of technical assistance (tools and informational guidance) to develop and what types of corrective action are most helpful.

OCR does not post any listing of audited entities or findings of individual audits that clearly identifies the audited entity. However, under the Freedom of Information Act (FOIA), if a request is made by the public, OCR may be required to release audit notification letters or other information about the audit.

Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review (see **9.1.3 Compliance Reviews**) to further investigate or close the case per **9.2 OCR Closure of Cases**.

9.1.3 Compliance Reviews

Compliance Reviews are a step above an audit. Through a compliance review, OCR reviews a CE's or BA's HIPAA policies in more detail to evaluate compliance. A compliance review may be initiated as a result of a complaint or if a serious compliance issue is revealed through an audit.

Issues raised during a Compliance Review are closed per **9.2 OCR Closure of Cases**.

9.2 OCR Closure of Cases[23]

OCR closes cases of HIPAA non-compliance in the following ways depending on how the issue was raised and the nature of the issue:

9.2.1 Complaint resolved after intake & review

After initial review of the complaint, OCR may close the case if it determines it does not have jurisdiction or if it will otherwise not be investigated. Examples of this situation include:

- the entity in question is not a CE or BA
- no PHI and ePHI is involved in the complaint
- the complainant does not consent for their information to be disclosed as part of the investigation
- OCR otherwise determines not to investigate the complaint

9.2.2 Complaint technical assistance provided

OCR provides technical assistance to the CE and/or BA, and the complainant and resolves the complaint prior to needing investigation.

9.2.3 No Violation

OCR investigates and does not find any violations of the HIPAA Rules.

23 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html

9.2.4 Corrective Action Obtained

OCR requires the CE or BA to make changes regarding HIPAA policies, procedures, training, or safeguards. In some cases, technical assistance is provided after investigation without requiring specific corrective action, for example, when the covered entity or business associate has already taken corrective action during the investigation or within the 60-day window prior to notifying OCR of the breach incident.

Corrective action closures also include those cases in which OCR enters into a settlement agreement with a CE or BA (see **9.2.4.1 Resolution Agreements**).

9.2.4.1 Resolution Agreements

A resolution agreement is a settlement agreement signed by HHS and a CE or BA in which the entity in question agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS also monitors the CE's compliance with its obligations.

See the Welcome Kit for Sample Resolution Agreement and Corrective Action Plan.

A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the CE's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity (see **9.3 Penalties**).

To promote systemic reform that benefits the greatest number of individuals, in such case:

- OCR settles for a *percentage* of any applicable civil money penalties OCR could impose
- requires entities to reinvest in their enterprises to correct the underlying root causes for the noncompliance through a corrective action and monitoring plan

9.2.5 Other closures of cases

OCR may decide not to investigate a case further if:

1. It is referred to the Department of Justice for prosecution.
2. It involved a natural disaster.
3. It was pursued, prosecuted, and resolved by state authorities.
4. The CE or BA has taken steps to comply with the HIPAA Rules and OCR determines enforcement resources are better/more effectively deployed in other cases.

NOTE: multi-year monitoring of a CE's or BA's HIPAA practices may be required by OCR.

9.3 Penalties

9.3.1 Civil Money Penalties

CEs may be faced with civil money penalties if they fail to comply with a requirement of the HIPAA regulation. Penalties depend largely on the date of the violation, whether the CE knew or should have known of the failure to comply, or if the CE's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement. See *Table 12: Civil Money Penalties Structure* for the different types of violations and their penalties.

HIPAA Violation	Minimum Penalty Amount
For violations occurring prior to 2/18/2009	
All	• Minimum: Up to $100 per violation • Calendar year cap: $25,000
For violations occurring on or after 2/18/2009 (below amount plus adjustment for inflation)	
Unknowing	• Minimum: $100 per violation • Annual maximum: $25,000 for all violations of an identical provision
Reasonable cause can be justified	• Minimum: $1,000 per violation • Annual maximum: $100,000 for all violations of an identical provision
Willful neglect but violation is corrected within the required time period	• Minimum: $10,000 per violation • Annual maximum: $250,000 for all violations of an identical provision
Willful neglect and is not corrected within the required time period	• Minimum: $50,000 per violation • Annual maximum: $1,500,000 for all violations of an identical provision

Table 12: Civil Money Penalties Structure

A penalty will not be imposed in certain situations, including:

- the failure to comply was not caused by willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR)
- the Department of Justice has imposed a criminal penalty for the failure to comply (see 9.3.2 Criminal Penalties)

Complainants do not receive a portion of Civil Money Penalties collected from Covered Entities; the penalties are deposited in the U.S. Treasury.

[continued on next page]

Additionally, if the OCR determines that the failure to comply was due to reasonable cause and that the penalty would be excessive for such noncompliance, it may choose to reduce the penalty.

Before a penalty is imposed, a CE will be notified and given the opportunity to provide written evidence of circumstances that might reduce or avoid a penalty. OCR must receive this evidence within 30 days of the CE's receipt of the notice. A CE also has the right to request an administrative hearing to appeal the proposed penalty after it receives notice that a penalty may be imposed.

9.3.2 Criminal Penalties

- If a person knowingly obtains or discloses PHI in violation of HIPAA regulation, he/she may face a criminal penalty of up to $50,000 and up to one-year imprisonment.
- If the wrongful conduct involves false pretenses, the criminal penalties increase to $100,000 and up to five years imprisonment.
- If the wrongful conduct involves the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the criminal penalties increase to $250,000 and up to 10 years imprisonment.

9.4 Enforcement Statistics

See **16 Enforcement Statistics** for enforcement data.

10 What is the Administrative Simplification Rule?

HIPAA administrative standards for your practice

In addition to the Privacy Rule (see **4 What is the Privacy Rule?**), Security Rule (**6 What is the Security Rule?**), Breach Notification Rule (**8 What is the Breach Notification Rule?**) and Enforcement Rule (**9 How is HIPAA compliance enforced?**), HIPAA also includes a number of other *administrative* rules known as the Administrative Simplification Rules.

This Chapter highlights these rules and what healthcare providers are required to do to comply.

10.1 Transactions Standard

10.1.1 What is a transaction?

A **transaction** is an *electronic* exchange of information between two parties to carry out financial or administrative activities related to health care. For example, a health care provider will send a claim to a health plan to request payment for medical services.

10.1.2 Standard Transactions

Under HIPAA, the Department of Health and Human Services (HHS) adopted certain standard transactions for the electronic exchange of health care data. These transactions include:

- Claims and encounter information
- Payment and remittance advice
- Claims status
- Eligibility
- Enrollment and disenrollment

We recommend consulting with an IT professional to ensure that your transactions comply with these HIPAA required standards.

- Referrals and authorizations
- Coordination of benefits
- Premium payment

CEs (including healthcare providers) who conduct any of these transactions electronically must use an adopted standard from **10.1.2.1 ASC x12N** or **10.1.2.2 NCPDP** (for certain pharmacy transactions). For example, if a healthcare provider submits a claim to a health insurance company to request payment for medical services, they must follow these standards for electronic transactions.

10.1.2.1 ASC x12N

In 1979, the American National Standards Institute (ANSI) chartered the Accredited Standards Committee (ASC) X12 to develop uniform standards for interindustry electronic exchange of business transactions-electronic data interchange (EDI).[24]

10.1.2.2 NCPDP

As an ANSI-accredited Standards Development Organization (SDO), NCPDP uses a consensus-building process to create national standards for real-time, electronic exchange of healthcare information. Their primary focus is on information exchange for prescribing, dispensing, monitoring, managing and paying for medications and pharmacy services crucial to quality healthcare.[25]

24 http://www.x12.org/about/faqs.cfm#b1

25 https://www.ncpdp.org/About-Us

10.2 Codes Set Standard

Under HIPAA, HHS adopted specific code sets for diagnoses and procedures used in all transactions.

10.2.1 About Code Sets

They inform diverse health care functions, from billing to tracking public health. Code sets classify:

- Diagnoses
- Procedures
- Diagnostic tests
- Treatments
- Equipment and supplies

10.2.2 HIPAA Code Sets

Code sets outlined in HIPAA regulations include:

10.2.2.1 International Classification of Diseases, 10th edition (ICD-10)

The International Classification of Diseases, Tenth Edition (ICD-10) is a clinical cataloging system that went into effect for the U.S. healthcare industry on Oct. 1, 2015. Accounting for modern advances in clinical treatment and medical devices, ICD-10 codes offer many more classification options compared to those found in its predecessor, ICD-9.

The World Health Organization (WHO) owns, develops and publishes ICD codes, and national governments and other regulating bodies adopt the system.

10.2.2.2Health Care Common Procedure Coding System (HCPCS)

The regulation that CMS published on August 17, 2000 (45 CFR 162.10002) to implement the HIPAA requirement for standardized coding systems established the

HCPCS level II codes as the standardized coding system for describing and identifying health care equipment and supplies in health care transactions that are not identified by the HCPCS level I, CPT codes. The HCPCS level II coding system was selected as the standardized coding system because of its wide acceptance among both public and private insurers. Public and private insurers were required to be in compliance with the August 2000 regulation by October 1, 2002.[26]

10.2.2.3 Current Procedure Terminology (CPT)

Current Procedural Terminology (CPT) is a medical code set that is used to report medical, surgical, and diagnostic procedures and services to entities such as physicians, health insurance companies and accreditation organizations. CPT codes are used in conjunction with ICD-9-CM or ICD-10-CM numerical diagnostic coding during the electronic medical billing process.

CPT is a registered trademark of the American Medical Association.

10.2.2.4 Code on Dental Procedures and Nomenclature (CDT)

The purpose of the CDT Code is to achieve uniformity, consistency and specificity in accurately documenting dental treatment. One use of the CDT Code is to provide for the efficient processing of dental claims, and another is to populate an Electronic Health Record.

On August 17, 2000 the CDT Code was named as a HIPAA standard code set. Any claim submitted on a HIPAA standard electronic dental claim must use dental procedure codes from the version of the CDT Code in effect on the date of service. The CDT Code is also used on paper dental claims, and the ADA's paper claim form data content reflects the HIPAA electronic standard.[27]

26 https://www.cms.gov/Medicare/Coding/MedHCPCSGenInfo/HCPCSCODINGPROCESS.html

27 http://www.ada.org/en/publications/cdt

10.2.2.5 National Drug Codes (NDC)

The Drug Listing Act of 1972 requires registered drug establishments to provide the Food and Drug Administration (FDA) with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution. (See Section 510 of the Federal Food, Drug, and Cosmetic Act (Act) (21 U.S.C. 360)). Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as a universal product identifier for drugs. FDA publishes the listed NDC numbers and the information submitted as part of the listing information in the NDC Directory which is updated daily.[28]

10.3 Employer Identifier Standard

HIPAA requires that healthcare providers have, their National Provider Identifier (NPI), identify them on standard transactions.

NPI is a unique 10-digit number used to identify healthcare providers. All healthcare providers who are HIPAA CEs, whether individuals or organizations, must obtain an NPI.

An NPI remains the same, even if a provider has a change of name, address or other information.

Applications for an NPI can be made through the Centers for Medicare & Medicaid Services (CMS) National Plan and Provider Enumeration System (NPPES).[29]

28 https://www.fda.gov/Drugs/InformationOnDrugs/ucm142438.htm

29 https://nppes.cms.hhs.gov/#/

This page intentionally left blank

11 Conclusion

This manual addresses federal HIPAA requirements for covered healthcare providers including medical, dental, pharmaceutical, chiropractic offices and more. It contains comprehensive information that can be used to train your workforce. Training is required both on making a new hire and over time. It also lists the required policies, procedures and safeguards that healthcare providers must implement in their practice to be in compliance with HIPAA.

Although compliance with HIPAA can seem daunting, it is simpler than it seems. By adopting a culture of protecting your patients' health information, putting in a good faith effort and implementing measures where required by HIPAA, you can rest assured knowing that you're protected from citation by OCR and protecting your patients' information as well. **Our Five Stage Process for HIPAA Compliance** will help guide you.

Here at Gamma Compliance Solutions, we strive to provide you with HIPAA compliance solutions that are simple, accurate, comprehensive, and current. If we have omitted any aspect of the regulations or if you have any other feedback, please feel free to contact us.

Thank you for selecting us to assist you in implementing HIPAA compliance in your practice. We look forward to working with you.

The Gamma Compliance Solutions Team

This page intentionally left blank

12 Our Five Stage Process for HIPAA Compliance

This chapter describes our five-stage process that you can adapt and use to implement HIPAA compliant practices in your organization. Each stage will have several **actions** for you to take to complete that stage.

This plan is intended to be adaptable to the size and nature of your organization. When executing this process, be mindful of the factors impacting your compliance process:

1. The size, complexity, and capabilities of your organization
2. Your technical infrastructure, hardware, and software security capabilities,
3. The cost of security measures
4. The probability and severity of potential risks to ePHI

The five stages to HIPAA Compliance are:

1. 12.1 Stage 1: Identify your team and set your objectives & scope
2. 12.2 Stage 2: Assess your current system & policies and identify gaps
3. 12.3 Stage 3: Determine corrective and preventative actions
4. 12.4 Stage 4: Implement new processes, policies and systems
5. 12.5 Stage 5: Evaluate, monitor and update as needed

12.1 Stage 1: Identify your team and set your objectives & scope

In order to start your journey to HIPAA compliance, an understanding of the regulations is important. Fortunately, if you have become familiar with the content in this manual, you are already halfway there. However, HIPAA regulations can be complex, and you may need assistance. The actions in Stage 1 are:

1. 12.1.1 Action 1A: Appoint a HIPAA Compliance Officer and their team
2. 12.1.2 Action 1B: Define the roles and responsibilities of each member in the HIPAA compliance team
3. 12.1.3 Action 1C: Create a HIPAA documentation repository

4. 12.1.4 Action 1D: Promote a culture of protecting patient privacy and securing health Information

12.1.1 Action 1A: Appoint a HIPAA Compliance Officer and their team

Your HIPAA Compliance Officer will be your go to resource for developing, implementing and maintaining processes, procedures, policies and systems in order to meet HIPAA requirements. Depending on the size of your organization you may consider having multiple people in this role and/or splitting the role into Privacy Compliance Officer and Security Compliance Officer.

Privacy Compliance Officer: Responsible for ensuring that PHI and ePHI is used and disclosed in a HIPAA compliant manner.

Security Compliance Officer: Responsible for ensuring that appropriate security safeguards are in place for ePHI.

The HIPAA Compliance Officer is a required role but may need to coordinate with other members of your staff in order to conduct his/her/their duties including but not limited to the:

1. practice manager
2. information technology (IT) administrator or consultant
3. other staff

Identify these personnel as part of your information Privacy and Security team.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.1.2 Action 1B: Define the roles and responsibilities of each member in the HIPAA compliance team

1. Record all team assignments in a permanent documentation file (this file should focus on HIPAA compliance efforts). This file will be part of your objective evidence for HIPAA compliance.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

a. [Important: ultimately, the responsibility of HIPAA compliance falls on the entire organization, not just the HIPAA compliance officer(s)].

2. Ensure that the designated officer(s) (and team if applicable) is trained to develop a full understanding of the HIPAA Rules so they can succeed in their roles.

- TIP: The HIPAA Training Program covers all the information your HIPAA compliance officer and other workforce staff need to know to comply with HIPAA.

12.1.3 Action 1C: Create a HIPAA documentation repository

As you move through the process outlined in this document towards HIPAA compliance, you will be generating documentation and processes. These records must be organized in an easily accessible and secure repository for use by your Privacy and Security team and other members in your organization. Additionally, these records are essential if you are ever audited by the Office for Civil Rights (OCR).

- TIP: We recommend saving all HIPAA documentation electronically in a location accessible to staff and/or in the HIPAA Documentation Kit.

12.1.4 Action 1D: Promote a culture of protecting patient privacy and securing health Information

Privacy and security are best achieved when the overall atmosphere in your office emphasizes confidentiality and protecting of patient information. Culture sets the tone that will:

1. Consistently communicate your expectations that all members of your workforce protect patients' health information
2. Guide your workforce's efforts to comply with, implement, and enforce your privacy and security policies and procedures
3. Remind staff why securing patient information is important to patients and the medical practice

12.2 Stage 2: Assess your current system & policies and identify gaps & risks

Once you have your team identified, set the objectives for your team and have committed to promoting a culture of protecting patient information privacy and security, it is time to inventory your organization's current state. HIPAA regulations have requirements that certain analyses be performed. The actions in Stage 2 include:

1. 12.2.1 Action 2A: Document your current process and archive your records
2. 12.2.2 Action 2B: Perform and document an Initial Risk Analysis

12.2.1 Action 2A: Document your current process and archive your records

The goal of this action is:

1. to identify your current policies and procedures to protect the privacy and security of PHI and ePHI
2. collect all such policies and procedures as well as any training materials and archive them in the HIPAA documentation repository created in **12.1.3 Action 1C: Create a HIPAA documentation repository**
3. identify any missing elements of HIPAA compliance

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.2.2 Action 2B: Perform and document an Initial Risk Analysis

The risk assessment process identifies potential risks to the privacy and security of protected health information. The findings from this assessment will form the basis of your corrective actions strategy in **12.3 Stage 3:**

IMPORTANT: Ensure that you are familiar with the terms threat, vulnerability and risk as defined in **13 Basics of Risk Analysis and Management**. A good understanding of these concepts is required for a successful risk assessment.

Determine corrective and preventative actions.

Documentation of a risk analysis is a requirement under the HIPAA Security Rule (see **7.1.1.1 Risk Analysis - R**). The intent of the documentation is to show:

- the *process* by which the security risk analysis was conducted,
- the risks that are identified along with their probability (likelihood) and severity (impact) of occurrence
- how you implemented safeguards and mitigations to address these risks.

Your HIPAA compliance officer is a mandatory participant in the Risk Assessment. The HIPAA compliance team may also participate as necessary.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete the initial risk analysis.
- TIP: See 13 Basics of Risk Analysis and Management for more information on performing a risk analysis.

12.3 Stage 3: Determine corrective and preventative actions

After completing **12.2 Stage 2: Assess your current system & policies and identify gaps & risks,** you will have identified the missing elements of HIPAA compliance as well as a list of risks prioritized by risk level. In Stage 3, you will consider measures to:

1. resolve these gaps in HIPAA compliance
2. mitigate the identified risks from your risk analysis by taking measures that will reduce the risk to an acceptable level

These corrective and preventative actions (together termed: CAPAs) are designed to eliminate risks to the privacy and security of PHI and ePHI as well as prevent such risks from arising in the future.

HIPAA provides flexibility in achieving compliance based on the characteristics of your organization – you have the latitude to select measures that are reasonable and appropriate for your practice provided that they are effective in reducing risk to PHI and ePHI.

The actions in Stage 3 are:

1. 12.3.1 Action 3A: Develop an Action Plan
2. 12.3.2 Action 3B: Develop a Risk Management Plan
3. 12.3.4 Action 3C: Evaluate Residual Risk Level

12.3.1 Action 3A: Develop an Action Plan

The purpose of the Action Plan is to resolve the gaps in HIPAA policies and procedures.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.3.2 Action 3B: Develop a Risk Management Plan

Through the initial risk assessment, you should have a list of risks and their prioritization. The purpose of the risk management plan is to evaluate corrective and preventative actions (CAPAs) to reduce the risk to acceptable levels.

CAPAs should be performed similar to any other project in your organization i.e. having a defined scope, timeline and budget. There may also be opportunities to combine with other existing projects and initiatives (for example the implementation of a new information system).

The HIPAA compliance officer is responsible for creating the risk management plan but may enlist the participation of the HIPAA compliance team.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.
- TIP: See 13 Basics of Risk Analysis and Management for more information.

12.3.3 Tips for CAPAs

Any single risk may require a combination of safeguards to address it because there may be multiple potential threats and vulnerabilities. For example, ensuring appropriate and continuous access to electronic health records may require:

1. A physical safeguard of installing a power surge protection strip
2. Locating the server in a secure location
3. Ensuring backups are performed on a regular basis

Conversely, a single CAPA may mitigate multiple risks. For example, a new information system may mitigate:

1. Unauthorized access to PHI by requiring login credentials
2. Insecure information communication by encrypting information

12.3.4 Action 3C: Evaluate Residual Risk Level

Simply identifying CAPAs to reduce the identified risks is not sufficient. It is important to evaluate the effectiveness of the proposed CAPA before implementing it to ensure that the risk is actually reduced to an acceptable level. This is done by performing another risk level assessment (i.e. the residual risk assessment) now accounting for the risk after the proposed CAPA. By re-assessing the probability, severity and risk level after the CAPA (this is a projection based on if the CAPA was instituted), the HIPAA compliance officer and team can make the determination whether to approve the CAPA for implementation.

- If the resulting risk assessment shows the risk is projected to be at an acceptable level after the CAPA, then the CAPA is deemed an effective mitigation and can be implemented in **12.4 Stage 4: Implement new processes, policies and systems**.
- If the resulting risk assessment shows the risk is projected to be at an unacceptable level even after the CAPA, the CAPA is not sufficient to reduce the risk to an acceptable level. In this event, either the CAPA should be rejected or additional CAPA(s) will be required to reduce the risk to an acceptable level.

- ✓ TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.
- ✓ TIP: See 13 Basics of Risk Analysis and Management for more information.

Let's illustrate this process with an example.

Let's say the risk being evaluated is "Portable electronic devices are not tracked or logged when not in use". The current probability and severity are both evaluated to be "Medium" and therefore the risk level is "Medium" (per a pre-defined risk level matrix defined by the HIPAA compliance officer and team (see *Table 14: Risk Level Matrix*).

- Risk: Portable electronic devices are not tracked or logged when not in use
- Probability: Medium
- Severity: Medium
- Current risk level: Medium
- Result: Unacceptable (as determined by the HIPAA Compliance Officer)

The HIPAA compliance team evaluates this risk and considers implementing a check in / check out system in which:

- All portable devices are marked with a unique identifier (e.g. a serial number)
- The devices are stored in a locked cabinet with bins marked for each device
- A process is developed such that the devices must be returned to the cabinet by the end of the business day
- A daily check is done to ensure that all devices are in the cabinet
- If a device is found not to be in the cabinet, the HIPAA Compliance Officer is notified, and a tracking system is used to locate the device

Considering the initial risk level and this proposed CAPA, the HIPAA Compliance Officer reassesses the risk level and determines:

- Probability: Low
- Severity: Low
- Resulting risk level: Low
- Result: Acceptable (as determined by the HIPAA Compliance Team)

Since the resulting risk level is determined to be acceptable, the CAPA is approved for implementation (see **12.4 Stage 4: Implement new processes, policies and systems**).

12.4 Stage 4: Implement new processes, policies and systems

Once you have a list of policies to implement and CAPAs that you have evaluated to be effective and have been approved by the HIPAA compliance officer and team, it's time to initiate those actions.

Additionally, HIPAA regulations **require** certain policies and safeguards to be implemented, such as:

1. Business Associate contracts (see 2.2.1 Business Associate Contracts)
2. Policies protecting patient rights (see 5 What are a patient's rights to their health information?)
3. Certain security rule safeguards (see 7 What are the Security Rule Safeguards?)

Note: This is not an all-inclusive list; it specifically mentions the actions for which healthcare providers have been cited in the past for not implementing. The HIPAA Manual and Documentation Kit cover these items extensively and comprehensively and should be completed in its entirety in order to be HIPAA compliant.

The actions in Stage 4 are:

1. 12.4.1 Action 4A: Implement Written Policies and Procedures
2. 12.4.2 Action 4B: Implement your Corrective and Preventative Actions
3. 12.4.3 Action 4C: Educate and train your workforce
4. 12.4.4 Action 4D: Communicate your Privacy and Security Practices
5. 12.4.5 Action 4E: Update your Business Associate Contracts and Listing

12.4.1 Action 4A: Implement Written Policies and Procedures

HIPAA requires the existence and utilization of documented policies in procedures within your practice to guide your workforce operation in a manner that ensures the privacy and security of PHI and ePHI. Your practice policies and procedures should accomplish the following, at minimum (not exhaustive):

  - Establish protocols for the Security Rule Safeguards (see 7 What are the Security Rule Safeguards?)
  - Contain instructions for what to do in the event of a breach of PHI or ePHI privacy and security and a sanction policy for such violations (see **8 What is the Breach Notification Rule?**)
  - Detail your control measures to ensure that PHI and ePHI are used and disclosed compliantly
- TIP: As you create and update these policies in procedures, maintain a revision history in the HIPAA Documentation Repository created in 12.1.3 Action 1C: Create a HIPAA documentation repository. HIPAA requires at least six years of history (see **7.4.4.1 Time Limit - R**). State and private-sector requirements may specify a longer time period for retention.
- TIP: The HIPAA Documentation Kit contains templates for HIPAA mandated and recommended policies and procedures that can be used to complete this action.

12.4.2 Action 4B: Implement your Corrective and Preventative Actions

As discussed in **12.3 Stage 3: Determine corrective and preventative actions**, your CAPAs should address the risks identified as part of the initial risk assessment and reduce them to an acceptable level. Implementing CAPAs should also account for the Security Rule safeguards (see **7 What are the Security Rule Safeguards?**)

Ensure that you have the appropriate documentation demonstrating that the CAPAs have been implemented, are performing per expectations and are therefore effectively mitigating the identified risks.

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.4.3 Action 4C: Educate and train your workforce

Workforce education and training that covers privacy of patients and security of their information are required aspects of HIPAA. All of your workforce members including

employees, volunteers, trainees and contractors need to be familiar with HIPAA, your organization's privacy and security practices and what their responsibilities are to safeguard PHI and ePHI.

Your training program should contain the following elements:

- The different roles within your organization and their specific responsibilities in safeguarding patients' health information and complying with the HIPAA Rules
- Your HIPAA-related policies
- Your procedures, including processes to monitor security and steps for breach notifications

✓ TIP: The HIPAA Training Program covers all the information your HIPAA compliance officer and other workforce staff need to know to comply with HIPAA.

12.4.3.1 Frequency of Workforce Training

There are three triggers for workforce training:

1. A new workforce member is brought on staff (training recommended within 10 days)
2. "Refresher" training – HIPAA does not stipulate the frequency of refresher training, but industry best practice suggest training on an annual basis
3. Changes to HIPAA policies, procedures or systems, infrastructure etc. (training recommended within 10 days)

12.4.3.2 Updating Workforce Training

Training material itself should be routinely assessed for completeness and correctness. There are three triggers to update training material:

1. Changes to HIPAA policies, procedures or systems, infrastructure etc.

2. Changes to the organizational structure that impact the HIPAA compliance officer and/or team
3. Recurring training review - HIPAA does not stipulate the frequency of updating training material but it is recommended to re-assess any training material on an annual basis

12.4.4 Action 4D: Communicate your Privacy and Security Practices

As demonstrated in **1.1 Importance of Privacy and Security**, a patient's attitude towards the privacy and security of their health information is directly correlated to their support of the use of EHR. It is important that your organization has in place a mechanism to communicate with patients to explain the safeguards you have in place for their PHI and ePHI as well as the benefits of utilizing EHRs.

The Notice of Privacy Practices (see **5.3 Right to Designate a Personal Representative**) as well as making available your practice's HIPAA policies available to patients (we recommend notifying them of the existence of the completed Documentation Kit and that it is available for their review) will assist in effective communication with your patients.

You should also designate someone to respond to any patient's questions or concerns about your HIPAA practices or their rights. This is typically the HIPAA compliance officer but can be any other qualified member of workforce staff (see **5.4.1 Content of the Notice of Privacy Practices**).

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.4.4.1 Tips when communicating with patients

Below are some tips to consider when communicating with patients. This is not an exhaustive list but just a few highlights:

- Consumer communications should be culturally appropriate. Consider the various languages, communication needs, and trust levels of different patient populations.

- Be prepared to discuss and answer the questions that concerned patients and their caregivers may have.
- When communicating with patients via online platforms (e.g. via email, texting, social media or some other online patient portal), you must adhere to the HIPAA Security Rule and safeguards (see **7 What are the Security Rule Safeguards?**)
- Be mindful of the patient's rights to their health information (see 5 What are a patient's rights to their health information?)

12.4.5 Action 4E: Update your Business Associate Contracts and Listing

After instituting new HIPAA compliant policies, procedures and systems in your organization, be sure to update your Business Associate agreements to comply (see **2.2.1 Business Associate Contracts**). At a minimum, such agreements should require your BAs to:

- Fully comply with relevant safeguards for PHI that they get from your practice
- Train their workforce
- Adhere to additional requirements for patient rights and breach notification

Additionally, be sure to update and maintain a listing of all Business Associates affiliated with your practice (see **2.2.2 Business Associate Listing**).

- TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.5 Stage 5: Evaluate, monitor and update as needed

HIPAA compliance is an on-going process and requires routine evaluation of your HIPAA practices and security measures.

Stage 5 includes the following actions:

1. 12.5.1 Action 5A: Evaluate the effectiveness of your Privacy and Security infrastructure

2. 12.5.2 Action 5B: Monitor how your PHI and ePHI are used
3. 12.5.3 Action 5C: Update Privacy and Security practices as necessary

12.5.1 Action 5A: Evaluate the effectiveness of your Privacy and Security infrastructure

Your organization is responsible to ensure that the CAPAs you implement are effective in reducing risk to the privacy and security of PHI and ePHI. While this effectiveness check was done in **12.3 Stage 3: Determine corrective and preventative actions**, it is important to routinely re-assess to confirm that the CAPAs implement continue to be effective.

Work with your HIPAA compliance officer and team to ensure that your system's risks are effectively mitigated. This is achieved by conducting routine internal assessments of your privacy and security infrastructure.

12.5.1.1 Considerations for an internal assessment

- Utilize the Risk Analysis worksheet to perform this internal assessment
- Identify if there were any organizational or technology changes that would affect your HIPAA practices or safeguards (e.g. new staff or a new computer system)
- Identify trigger indicators — or signs that ePHI could have been compromised and further investigation is needed
- Establish a schedule for routine assessments (HIPAA does not stipulate a timeline on which routine audits need to be performed but you may consider an annual or on a biennial (once every two years) basis).

✓ TIP: The HIPAA Documentation Kit contains a template that can be used to complete this action.

12.5.2 Action 5B: Monitor how your PHI and ePHI are used

The HIPAA Security Rule requires that you have systems in place – i.e. hardware, software, and/or procedures – in place that allow for the examination of information

systems that contain or use PHI and ePHI and that a regular examination is done of those systems.

Requirement for Information system activity review	Requirement for Audit Controls
7.1.1.4 Information System Activity Review - R requires procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	**7.3.2 Audit Controls** requires audit controls i.e. hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

12.5.2.1 Considerations for monitoring capabilities:

- Electronic health record (EHR) systems must be set up to maintain a history of the below data for a period of at least 6 years (as measured from the creation of the EHR)
- Who – specific user
- What – what ePHI was accessed
- When – when did the access occur
- Where – e.g. what device was used to access ePHI
- How – e.g. was information reviewed or exported and for what purpose
- Work with your HIPAA compliance officer and team and EHR administrator to ensure that these capabilities are set up within your EHR system and that reports (audit logs) can be generated
- Your audit controls should be scaled to your organization's size

12.5.3 Action 5C: Update Privacy and Security practices as necessary

As stipulated in the associated Stages and actions, certain practices should be on a recurring basis if there is a change affecting the practice or on a pre-determined frequency. The practices to be revisited are:

1. Risk Analysis and Management (see 12.2.2 Action 2B: Perform and document an Initial Risk Analysis and 12.3.2 Action 3B: Develop a Risk Management Plan)
2. Corrective and Preventative Actions (see 12.3.3 Tips for CAPAs and 12.4.2 Action 4B: Implement your Corrective and Preventative Actions)
3. Workforce Training (see 12.4.3.2 Updating Workforce Training)

12.6 Conclusion

The actions represented in this five-stage plan are the foundation of the practices required by HIPAA. Execution of these actions and the completion of the required documentation will ensure that your organization is both compliant with HIPAA regulations and is utilizing health information in a safe manner. It will also protect against any reasonably anticipated risks to the security and integrity of PHI and ePHI. Fundamentally, this ensures the availability, integrity and confidentiality of PHI and ePHI, and ultimately, better outcomes for the patient.

This page intentionally left blank

13 Basics of Risk Analysis and Management

The purpose of this chapter is to explain the main concepts of Risk Analysis and Risk Management and implementation as required by the HIPAA Security Rule. Risk analysis and management can be difficult due to the level of detail, different processes that may be followed and variations in types of Covered Entities. We recommend focusing on the concepts and processes detailed in this chapter and adapting them as reasonable and appropriate for your practice.

13.1 Important Definitions to Understand

To better understand risk analysis and risk management processes, Covered Entities should be familiar with several important terms. These terms may not be specifically defined by the Security Rule, but are provided to put the Risk Analysis and Risk Management discussion in context.

Term	Definition
Vulnerability	A flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the CE's policy. e.g. non-existent policies or software flaws in security systems.
Threat	The potential for a person or thing to accidentally trigger or intentionally exploit a specific vulnerability. e.g. floods or malicious software.
Probability	The likelihood of a given threat triggering or exploiting a vulnerability.
Severity	The resulting impact on the CE and their patients.

Term	Definition
Risk	The net mission impact considering the *probability* that a *threat* will accidentally trigger or intentionally exploit a *vulnerability* and the *severity* if this should occur.
Risk Analysis	Assessing the level of risk to the privacy and security of health information within the organization.
Risk Management	Evaluating and implementing measures to reduce the level of risk to the privacy and security of health information within the organization to acceptable levels.

Table 13: Risk Analysis and Management Important Terms and Definitions

13.2 Risk Analysis Process

As previously stated, the Security Rule requires Covered Entities to conduct an accurate and thorough risk analysis (see **7.1.1.1 Risk Analysis - R**). This section provides an example approach to risk analysis which may be used by Covered Entities.

The risk analysis process includes the following steps:

> Note: There are numerous methods of performing risk analysis and risk management. There is no single method or "best practice" that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps.

1. **13.2.1 Identify the scope of the analysis**
2. **13.2.2 Gather data**
3. **13.2.3 Identify and document potential risks**
4. **13.2.4 Assess current security measures**
5. **13.2.5 Determine the probability and severity of risk occurrence**
6. **13.2.6 Determine the Level of Risk**

13.2.1 Identify the scope of the analysis

The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that a Covered Entity creates, receives, maintains, or transmits (see **3 What information is protected by HIPAA?**).

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a Covered Entity's risk analysis should consider all its ePHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its ePHI.

13.2.2 Gather data

Once the scope of the risk analysis is identified, the Covered Entity should gather relevant data on EPHI. For example, a Covered Entity must identify where the EPHI is stored, received, maintained or transmitted. A Covered Entity could gather relevant data by:

- reviewing past and/or existing projects
- performing interviews
- reviewing documentation
- using other data gathering techniques

13.2.3 Identify and document potential risks

Once the Covered Entity has gathered and documented relevant data on ePHI, the next step is to identify potential risks to the confidentiality, availability and integrity of the ePHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining risk.

13.2.4 Assess current security measures

The next step is to assess the *current* security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to ePHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures implemented to reduce risk will vary among Covered Entities. For example, small Covered Entities tend to have more control within their environment. Small Covered Entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard ePHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of ePHI in a small Covered Entity may differ from those that are appropriate in large Covered Entities.

Security measures can be both technical and non-technical.

Technical measures are part of information systems hardware and software and include:

- access controls
- identification and authentication
- encryption methods
- automatic logoff

Non-technical measures are management and operational controls, such as:

- policies and procedures
- standards and guidelines
- accountability and responsibility
- physical and environmental security measures

13.2.5 Determine the probability and severity of risk occurrence

Once the first four steps in the risk analysis process are complete, the Covered Entity has the information needed to determine probability and severity of the risk occurrence. The purpose of this step is to assist the Covered Entity in determining the level of risk and prioritizing risk mitigation efforts.

When determining the probability and severity of risk occurrence, you may consider using one of two different types of rating systems.

13.2.5.1 Qualitative Rating

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the probability and severity of risk. This method allows the Covered Entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale (you may rate this risk as medium severity and low probability).

13.2.5.2 Quantitative Rating

In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks.

For simplicity, we recommend employing a Qualitative Rating system when performing a risk analysis.

However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

13.2.6 Determine the Level of Risk

Next, Covered Entities should determine the level of risk to ePHI. As discussed earlier, risk is a function determined by the probability and severity of occurrence.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence.

A **risk level matrix** can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a probability value of "high"

combined with a severity value of "low" may equal a risk level of "low." Or a probability value of "medium" combined with a severity value of "medium" may equal a risk level of "medium."

Probability / Severity	*None*	*Low*	*Medium*	*High*
None	No Risk	No Risk	No Risk	No Risk
Low	No Risk	Low Risk	Low Risk	Low Risk
Medium	No Risk	Low Risk	Medium Risk	Medium Risk
High	No Risk	Low Risk	Medium Risk	High Risk

Table 14: Risk Level Matrix

Risk levels may be deemed to be acceptable, non-acceptable or require further review to make that determination. In *Table 14: Risk Level Matrix*,

- Green and yellow are acceptable
- Red is not-acceptable and requires a mitigation to reduce the risk
- Orange requires further review to determine if a mitigation is needed or not

The risk level will be used in to inform your Risk Management process (**13.3 Risk Management**).

13.3 Risk Management Process

Once the Covered Entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule (see **7.1.1.2 Risk Management - R**), includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of ePHI, protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, and protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under HIPAA.

The risk management process includes the following steps:

- 13.3.1 Develop and Implement a Risk Management Plan
- 13.3.2 Implement Security Measures
- 13.3.3 Evaluate and Maintain Security Measures

13.3.1 Develop and Implement a Risk Management Plan

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the Covered Entity's evaluation, prioritization, and implementation of risk-reducing security measures.

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the Covered Entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- Risks identified in the risk analysis
- Security measures selected to reduce the risks and required by HIPAA
- Implementation project priorities, such as:
    - required resources
    - assigned responsibilities
    - start and completion dates
    - maintenance requirements

The implementation component of the risk management plan may vary based on the circumstances of the Covered Entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement.

Note: certain risks may require multiple mitigations to sufficiently address – for example, securing ePHI in the event of a power outage may involve a generator system and data backup. Also, a single mitigation may address multiple risks – for example, providing each employee with a unique user ID to access electronic health records allows you to both secure the EHR system as well as monitor and audit access to the system.

Cost is one of the factors a Covered Entity must consider when determining security measures to implement.

However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the Covered Entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the Covered Entity's actual implementation of security measures to reduce risks to ePHI to reasonable and appropriate levels.

13.3.2 Implement Security Measures

Once the risk management plan is developed, the Covered Entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the Covered Entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget. Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A Covered Entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the Covered Entity is responsible for its compliance with the Security Rule.

13.3.3 Evaluate and Maintain Security Measures

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment.

- The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes.
- The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among Covered Entities. Some Covered Entities may perform these processes annually or as needed (e.g. bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation.

For example, if the Covered Entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain ePHI, the potential risk to these devices must be analyzed to ensure the ePHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the Covered Entity to reduce the associated risks to reasonable and appropriate levels.

13.4 In Summary

Risk analysis and risk management are the foundation of a Covered Entity's Security Rule compliance efforts. Risk analysis and risk management are ongoing processes that will provide the Covered Entity with a detailed understanding of the risks to ePHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of ePHI, protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, and protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under HIPAA.

14 Acronyms and Abbreviations

#	Acronym / Abbreviation	Definition
1	AHIMA	American Health Information Management Association
2	AIDS	Acquired Immune Deficiency Syndrome
3	BA	Business Associate
4	BAA	Business Associate Agreement
5	CD	Compact Disc
6	CE	Covered Entity
7	CEHRT	Certified Electronic Health Record Technology
8	CFR	Code of Federal Regulations
9	CHPS	Certified in Healthcare Privacy and Security
10	CMS	Centers for Medicare & Medicaid Services
11	CPHIMS	Certified Professional in Healthcare Information and Management Systems
12	CPOE	Computerized Provider Order Entry
13	DVD	Digital Video Disc
14	EHR	Electronic Health Record
15	EP	Eligible Professional
16	ePHI	Electronic Protected Health Information
17	FAQ	Frequently Asked Questions
18	FERPA	Family Educational Rights and Privacy Act
19	FR	Federal Register
20	GINA	Genetic Information Nondiscrimination Act
21	Health IT	Health Information Technology
22	HHS	U.S. Department of Health and Human Services

#	Acronym / Abbreviation	Definition
23	HIE	Health Information Exchange
24	HIMSS	Healthcare Information and Management Systems Society
25	HIO	Health Information Organization
26	HIPAA	Health Insurance Portability and Accountability Act
27	HITECH	Health Information Technology for Economic and Clinical Health
28	HIV	Human Immunodeficiency Virus
29	IT	Information Technology
30	NIST	National Institute of Standards and Technology
31	NPP	Notice of Privacy Practices
32	NPRM	Notice of Proposed Rulemaking
33	OCR	Office for Civil Rights
34	ONC	Office of the National Coordinator for Health Information Technology
35	PHI	Protected Health Information
36	PHR	Personal Health Record
37	REC	Regional Extension Center
38	RHI	Reproductive Healthcare Information
39	SRA	Security Risk Assessment
40	SUD	Substance Use Disorder
41	USC	United States Code

Table 15: Acronyms and Abbreviations

15 Security Safeguards Matrix

15.1 Administrative Safeguards

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	R
		Risk Management	R
		Sanction Policy	R
		Information System Activity Review	R
Assigned Security Responsibility	164.308(a)(2)		R
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A
		Workforce Clearance Procedure	A
		Termination Procedures	A
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions	R
		Access Authorization	A
		Access Establishment and Modification	A
Security Awareness and Training	164.308(a)(5)	Security Reminders	A
		Protection from Malicious Software	A
		Log-in Monitoring	A

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
		Password Management	A
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R
Contingency Plan	164.308(a)(7)	Data Backup Plan	R
		Disaster Recovery Plan	R
		Emergency Mode Operation Plan	R
		Testing and Revision Procedures	A
		Applications and Data Criticality Analysis	A
Evaluation	164.308(a)(8)		R
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	R

15.2 Physical Safeguards

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	A
		Facility Security Plan	A

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
		Access Control and Validation Procedures	A
		Maintenance Records	A
Workstation Use	164.310(b)		R
Workstation Security	164.310(c)		R
Device and Media Controls	164.310(d)(1)	Disposal	R
		Media Re-use	R
		Accountability	A
		Data Backup and Storage	A

15.3 Technical Safeguards

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
Access Control	164.312(a)(1)	Unique User Identification	R
		Emergency Access Procedure	R
		Automatic Logoff	A
		Encryption and Decryption	A
Audit Controls	164.312(b)		R

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	A
Person or Entity Authentication	164.312(d)		R
Transmission Security	164.312(e)(1)	Integrity Controls	A
		Encryption	A

15.4 Organizational, Policies, Procedures and Documentation Requirements

Standards	Regulatory Reference	Implementation Specifications R = Required, A = Addressable	
Business Associate Contracts or Other Arrangements	164.314(a)(2)(i)	Business Associate Contracts	R
	164.314(a)(2)(ii)	Other Arrangements	R
Policies and Procedures	164.316(a)		
Documentation	164.316(b)(2)(i)	Time Limit	R
	164.316(b)(2)(ii)	Availability	R
	164.316(b)(2)(iii)	Updates	R

16 Enforcement Statistics

Note: All the enforcement statistics in this section are taken from the Health and Human Services website (HHS.gov).

16.1 Enforcement Highlights

(As of October 31, 2024)[30]

Since the compliance date of the Privacy Rule in April 2003, OCR has received over 374,321 HIPAA complaints and has initiated over 1,193 compliance reviews. We have resolved ninety-nine percent of these cases (370,578).

OCR has investigated and resolved over 31,191 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Corrective actions obtained by OCR from these entities have resulted in change that is systemic and that affects all the individuals they serve. OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity or their business associate. To date, OCR settled or imposed a civil money penalty in 152 cases resulting in a total dollar amount of $144,878,972.00. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

In another 15,561 cases, our investigations found no violation had occurred.

Additionally, in 67,873 cases, OCR intervened early and provided technical assistance to HIPAA covered entities, their business associates, and individuals exercising their rights under the Privacy Rule, without the need for an investigation.

In the rest of our completed cases (255,953), OCR determined that the complaint did not present an eligible case for enforcement. These include cases in which:

30 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

- OCR lacks jurisdiction under HIPAA. For example, in cases alleging a violation by an entity not covered by HIPAA;
- The complaint is untimely, or withdrawn by the filer; and
- The activity described does not violate the HIPAA Rules. For example, in cases where the covered entity has disclosed protected health information in circumstances in which the Privacy Rule permits such a disclosure.

From the compliance date to the present, the compliance issues most often alleged in complaints are, compiled cumulatively, in order of frequency:

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Lack of administrative safeguards of electronic protected health information; and
5. Use or disclosure of more than the minimum necessary protected health information.

The most common types of covered entities that have been alleged to have committed violations are, in order of frequency:

1. General Hospitals;
2. Private Practices and Physicians;
3. Pharmacies;
4. Group Health Plans; and
5. Outpatient Facilities

16.2 Referrals to DOJ

(As of October 31, 2024)[31]

OCR refers to the Department of Justice (DOJ) for criminal investigation appropriate cases involving the knowing disclosure or obtaining of protected health information in violation of the Rules. As of the date of this summary, OCR made 2,419 such referrals to DOJ.

16.3 Complaints Received by Calendar Year

This bar graph represents annual numbers of complaints received from the 2011 through 2021.[32]

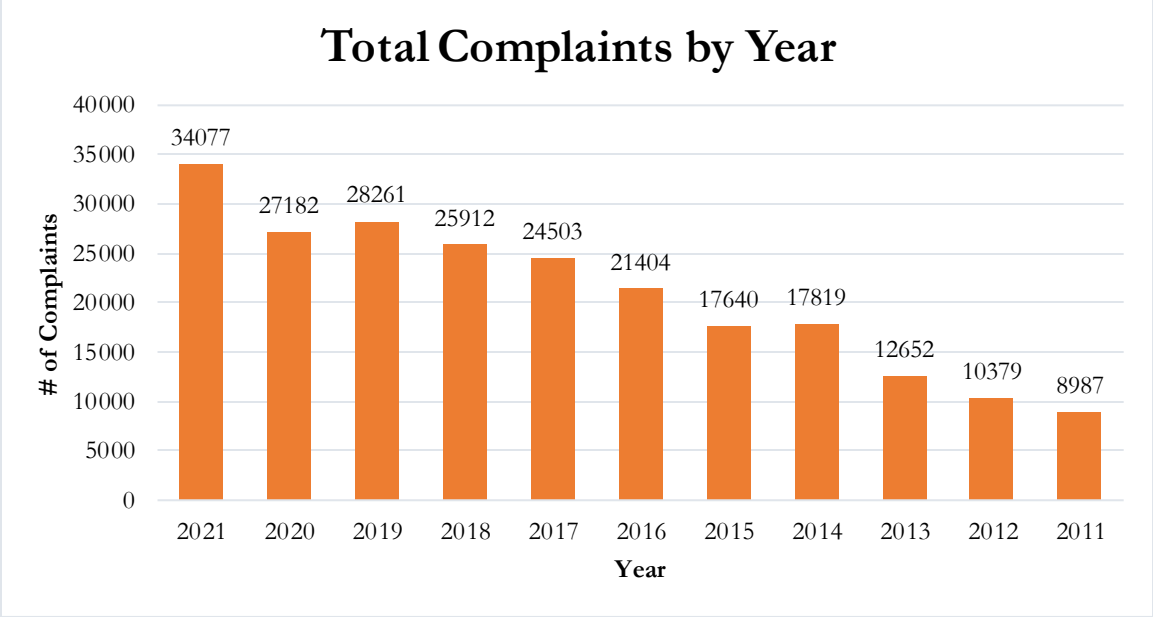

Figure 8: Total Complaints by Year

31 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

32 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html

16.4 Status of All Complaints

(April 14, 2003 – October 31, 2024)[33]

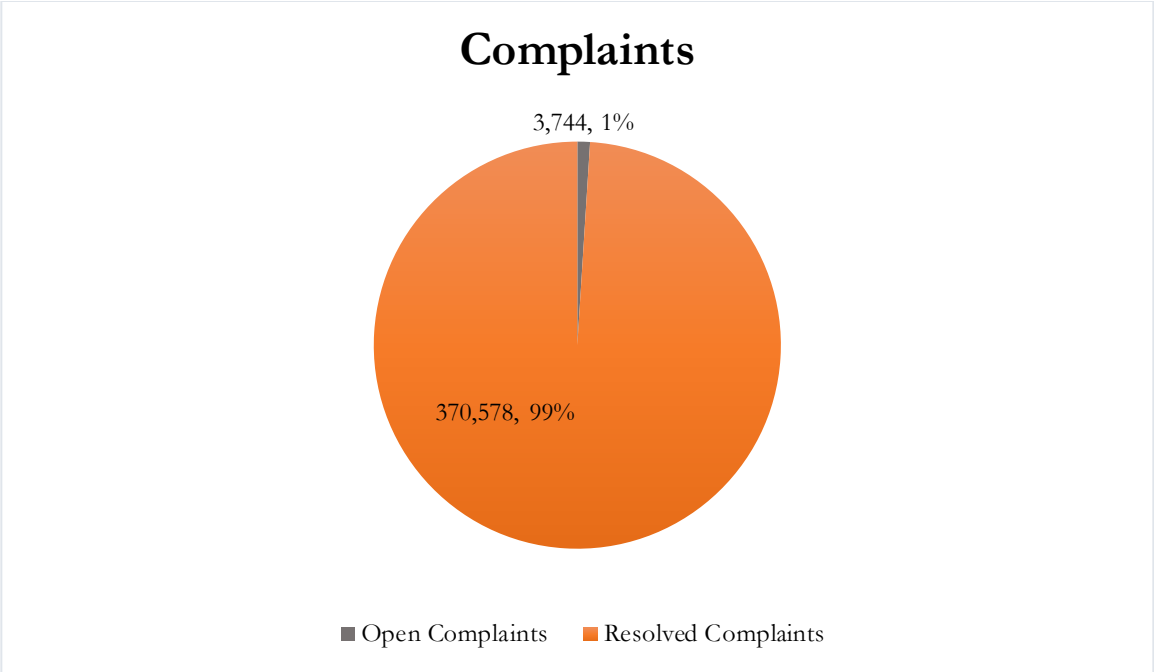

Figure 9: Status of All Complaints

33 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

16.5 Total Investigated Resolutions

(April 14, 2003 – October 31, 2024)[34]

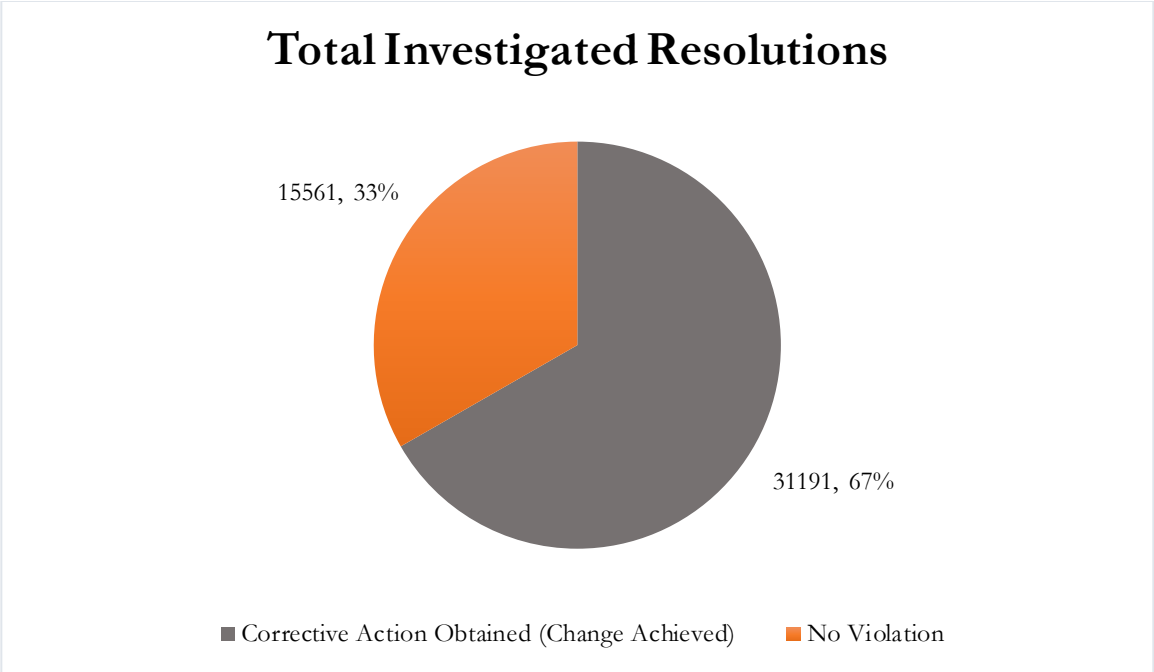

Figure 10: Total Investigated Resolutions

34 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

16.6 Investigated Resolutions by Year

(April 14, 2003 - December 31, 2015)[35]

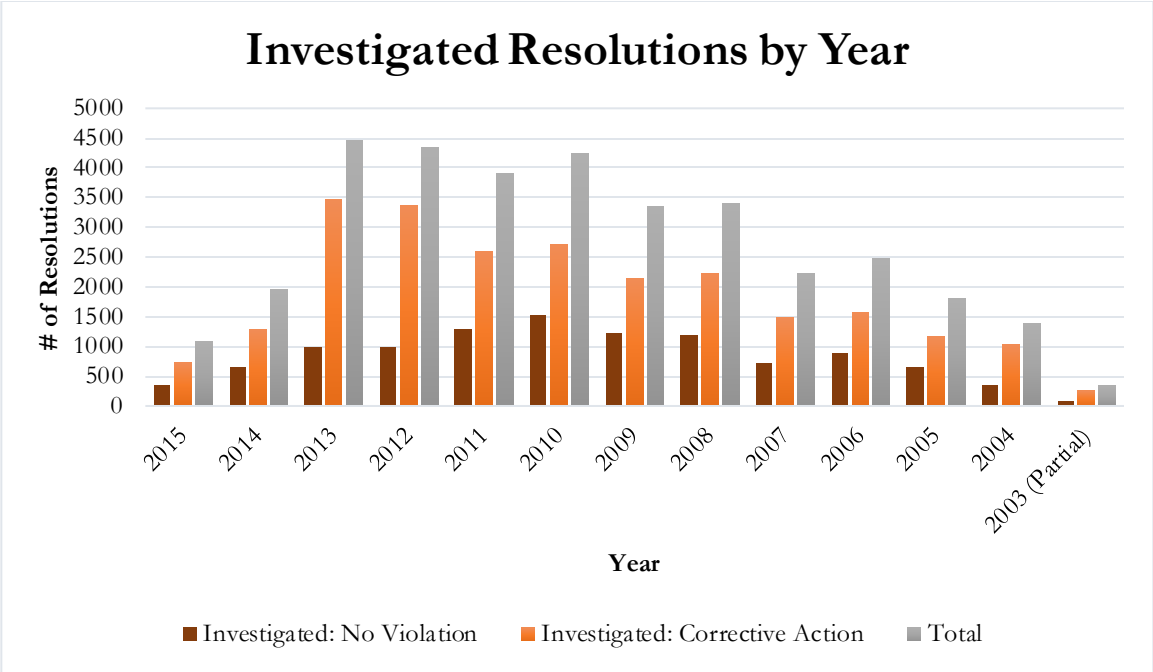

Figure 11: Investigated Resolutions by Year

16.7 Audit Results by Year

This section shows audit results by year according to the type of closure – whether there was no violation, corrective was obtained, etc. Data is separated for whether the incident was or was not determined to be a breach.

35 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

16.7.1 Non-Breach Audit Results

(January 1, 2013 – December 31, 2015)[36]

YEAR	INVESTIGATED: NO VIOLATION		INVESTIGATED: CORRECTIVE ACTION OBTAINED		RESOLVED AFTER INTAKE AND REVIEW		OTHER		TOTAL RESOLUTIONS
2013	1	4%	21	84%	3	12%	0	0%	25
2014	2	7%	27	90%	0	0%	1	3%	30
2015	7	19%	24	67%	2	6%	3	8%	36

16.7.2 Breach Audit Results

(January 1, 2013 – December 31, 2015)[37]

YEAR	RESOLVED AFTER INTAKE AND REVIEW		INVESTIGATED: NO VIOLATION		INVESTIGATED: CORRECTIVE ACTION OBTAINED		OTHER		TOTAL RESOLUTIONS
2013	6	4%	21	14%	121	80%	4	3%	152
2014	7	3%	6	3%	216	90%	10	4%	239
2015	8	5%	9	6%	126	85%	5	3%	148

36 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/results-by-year-compliance-reviews/index.html?language=en

37 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/results-by-year-compliance-reviews/index.html?language=en

16.8 Enforcement Results by State

This table, for each state, represents the enforcement results for the period from April 14, 2003 through December 31, 2021.[38]

STATE	INVESTIGATED: NO VIOLATION	RESOLVED AFTER INTAKE AND REVIEW	INVESTIGATED: CORRECTIVE ACTION
Alaska	5%	66%	29%
Alabama	5%	70%	26%
Arkansas	7%	67%	26%
Arizona	4%	66%	30%
California	4%	71%	25%
Colorado	5%	68%	27%
Connecticut	7%	67%	26%
District of Columbia	5%	70%	24%
Delaware	7%	65%	28%
Florida	4%	68%	27%
Georgia	4%	70%	26%
Hawaii	3%	69%	28%
Iowa	3%	74%	23%
Idaho	4%	68%	28%
Illinois	5%	67%	28%

38 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-state/index.html?language=en

STATE	INVESTIGATED: NO VIOLATION	RESOLVED AFTER INTAKE AND REVIEW	INVESTIGATED: CORRECTIVE ACTION
Indiana	5%	70%	25%
Kansas	4%	73%	23%
Kentucky	5%	71%	24%
Louisiana	5%	70%	25%
Massachusetts	8%	63%	29%
Maryland	6%	65%	29%
Maine	8%	67%	24%
Michigan	5%	69%	26%
Minnesota	4%	70%	26%
Missouri	4%	70%	26%
Mississippi	5%	73%	22%
Montana	7%	70%	23%
North Carolina	5%	68%	27%
North Dakota	7%	67%	26%
Nebraska	3%	75%	22%
New Hampshire	8%	65%	28%
New Jersey	4%	67%	29%
New Mexico	5%	68%	27%
Nevada	3%	72%	25%
New York	4%	70%	26%

STATE	INVESTIGATED: NO VIOLATION	RESOLVED AFTER INTAKE AND REVIEW	INVESTIGATED: CORRECTIVE ACTION
Ohio	4%	69%	27%
Oklahoma	6%	67%	27%
Oregon	4%	68%	28%
Pennsylvania	6%	67%	27%
Rhode Island	11%	54%	36%
South Carolina	5%	69%	27%
South Dakota	6%	68%	26%
Tennessee	5%	68%	28%
Texas	5%	69%	26%
Utah	5%	68%	27%
Virginia	6%	67%	27%
Vermont	8%	69%	24%
Washington	4%	67%	30%
Wisconsin	5%	68%	27%
West Virginia	7%	71%	22%
Wyoming	6%	66%	27%

Table 16: Enforcement Results by State

16.9 Top 5 Issues in Investigated Cases Closed with Corrective Action by Year

(January 1, 2005 - December 31, 2021)[39]

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2021	Impermissible Uses & Disclosures	Access	Safeguards	Administrative Safeguards	Breach – Notice to Individual
2020	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Technical Safeguards
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2017	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2016	Access	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Technical Safeguards
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards

39 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2014	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2013	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2012	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Minimum Necessary
2011	Impermissible Uses & Disclosures	Safeguards	Access	Notice to Individuals	Minimum Necessary
2010	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints
2009	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints
2008	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints
2007	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2006	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2005	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation

Table 17: Top 5 Issues in Investigated Cases Closed with Corrective Action by Year

17 HIPAA and Reproductive Health

17.1 HIPAA Privacy Rule and Reproductive Health Care Provisions

Access to comprehensive reproductive health care services has long been recognized as essential to individual health and well-being. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule helps safeguard this access by assuring individuals that their protected health information (PHI), including information related to abortion and other reproductive care, will be kept private and used only as permitted by law.

The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) administers and enforces the Privacy Rule. This rule establishes the standards that covered entities—such as health plans, most healthcare providers, and their business associates—must follow when using or disclosing PHI. Disclosures without an individual's authorization are limited to specific purposes allowed under the Privacy Rule, including certain public health and law enforcement situations, and are designed to balance privacy protections with necessary information sharing.

In April 2024, HHS issued a Final Rule titled "HIPAA Privacy Rule to Support Reproductive Health Care Privacy." The new provisions aimed to strengthen patient confidentiality by prohibiting the use or disclosure of PHI for investigations or proceedings related to the provision or receipt of lawful reproductive health care, such as abortion or fertility services. Covered entities would have been required to obtain signed attestations before disclosing reproductive health information (RHI) in certain contexts, ensuring that PHI was not used to penalize patients or providers for care that was legal in the state where it occurred.

However, on June 18, 2025, the U.S. District Court for the Northern District of Texas vacated these reproductive health provisions nationwide, holding that HHS exceeded its statutory authority in issuing the rule. As a result, the reproductive health protections introduced in the 2024 Final Rule are currently unenforceable. Covered entities should therefore continue to follow the standard HIPAA Privacy Rule requirements and applicable state laws when handling reproductive health–related PHI.

The information in this chapter describes the reproductive health privacy provisions as they were finalized in 2024 before being vacated by the U.S. District Court for the Northern District of Texas on **June 18, 2025**.

These provisions—intended to restrict the use and disclosure of PHI related to lawful reproductive health care and require signed attestations—are **not currently enforceable**.

This section is provided for informational purposes only to help covered entities and workforce members understand the background and intent of the rule, pending any future legal developments. Until further notice, entities should follow **standard HIPAA Privacy Rule requirements and applicable state laws** for handling reproductive health–related PHI.

17.2 Definitions

17.2.1 Reproductive Health Care

Like the definition of "health care," the definition of reproductive health care is intended to be broad. "Reproductive health care" is defined as "health care that affects the health of the individual in all matters relating to the reproductive system and to its functions and processes." HHS added a clarifying statement that the definition should not be construed to establish a standard of care for or regulate what constitutes clinically appropriate reproductive health care.

HHS provided a non-exclusive list of examples that fit within the definition:

- contraception, including emergency contraception;
- preconception screening and counseling;
- management of pregnancy and pregnancy-related conditions, including pregnancy screening, prenatal care, miscarriage management, treatment for preeclampsia, hypertension during pregnancy, gestational diabetes, molar or ectopic pregnancy, and pregnancy termination;

- fertility and infertility diagnosis and treatment, including assisted reproductive technology and its components (e.g., in vitro fertilization (IVF));
- diagnosis and treatment of conditions that affect the reproductive system (e.g., perimenopause, menopause, endometriosis, adenomyosis); and
- other types of care, services, and supplies used for the diagnosis and treatment of conditions related to the reproductive system (e.g., mammography, pregnancy-related nutrition services, postpartum care products).

17.2.2 Reproductive Health Information

"Reproductive health information" means protected health information potentially related to reproductive health care.

17.2.3 Lawful

"Lawful" means that the reproductive health care is either:

Condition	Example
Lawful under the circumstances in which such health care is provided and in the state in which it is provided.	If a resident of one state traveled to another state to receive reproductive health care, such as an abortion, that is lawful in the state where such health care was provided.
OR	
Protected, required, or authorized by Federal law, including the United States Constitution, regardless of the state in which such health care is provided.	If the use of reproductive health care, such as contraception, is protected by the Constitution.

17.2.4 Seeking, obtaining, providing, or facilitating

"Seeking, obtaining, providing, or facilitating" would include, but not be limited to, expressing interest in, inducing, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same.

17.3 Does the Final Rule apply to all healthcare providers?

The new requirements apply to any covered entity (and its business associates) that maintains protected health information (PHI) which includes reproductive health information (RHI) – whether the RHI was created by the covered entity or not. However, RHI is defined very broadly (see the definitions of Reproductive Health Care and Reproductive Health Information).

RHI could become part of a medical or dental patient record if the patient history includes questions about:

- pregnancy status,
- medications taken (which could include birth control pills),
- date of last period,
- menopause status,
- past surgeries (which could include tubal ligation, vasectomy, hysterectomy, etc.), or
- if visit notes mention pregnancy status, etc.

So, while the answer is theoretically "yes, the new requirements are only applicable to entities that maintain RHI", this is likely a broad swath of providers. A provider should be very careful when evaluating if it maintains any RHI anywhere in its patient records.

If the provider determines that they truly do not ever maintain reproductive health information of any patient, then this Final Rule would not apply. However, patients may expect to see how RHI will be handled, so they may wish to add a statement to their Notice of Privacy Practices (NPP) that they do not maintain RHI in their patient records. Also, to ensure they don't inadvertently add RHI, they may need to train their

team on what RHI is and impress on them the need to avoid adding RHI to a patient record.

17.4 Guidelines for Permissible Use/Disclosure

In addition to the guidelines in the Final Rule, uses and disclosures of RHI must still comply with the Privacy Rule, including the minimum necessary standard (see the Protected Health Information Use and Disclosure Policy in the Documentation Kit).

The Final Rule continues to permit covered health care providers, health plans, or health care clearinghouses (or business associates) to use or disclose PHI for purposes otherwise permitted under the Privacy Rule where the request for the use or disclosure of PHI is not made to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

For example:

- A covered healthcare provider could continue to use or disclose PHI to defend themselves in an investigation or proceeding related to professional misconduct or negligence where the alleged professional misconduct or negligence involved the provision of reproductive health care.
- A covered health care provider, health plan, or health care clearinghouse (or business associates) could continue to use or disclose PHI to defend any person in a criminal, civil, or administrative proceeding where liability could be imposed on that person for providing reproductive health care.
- A covered health care provider, health plan, or clearinghouse (or their business associates) could continue to use or disclose PHI to an Inspector General where the PHI is sought to conduct an audit for health oversight purposes.

17.5 Prohibited Uses and Disclosures

Covered Entities and Business Associates are prohibited from using or disclosing PHI for either of the following activities:

- To conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided, or
- The identification of any person for the purpose of conducting such investigation or imposing such liability.

This includes a wide range of activities related to reproductive health care, such as expressing interest in, using, performing, paying for, and disseminating information about reproductive health services.

Before sharing reproductive health PHI, the regulated entity must determine whether a request is for a non-prohibited purpose and whether the reproductive healthcare was lawfully provided. The regulated entity's determination must be reasonable. (See Responding to a Request for Reproductive Health Information.)

17.6 Responding to a Request for Reproductive Health Information

Responding to a request for Reproductive Health Information involves the following steps:

- Evaluating the legal basis for the request and verifying that the request is not for a prohibited purpose.
- Obtaining a valid attestation if the request for RHI is for:
    - health oversight activities,
    - judicial or administrative proceedings,
    - law enforcement purposes, or
    - disclosures about decedents to coroners and medical examiners.
- Determining whether the reproductive health care was lawfully provided.
- Making the disclosure in a manner that otherwise complies with the HIPAA Privacy Rule so long as 1) a prohibition does not apply, or 2) reproductive health care was not provided lawfully.

17.6.1 Determining Legal Basis of a Request

The regulated entity should develop procedures for reasonably determining whether the legal basis for a request for reproductive health information is for a prohibited purpose. (See the Protected Health Information Use and Disclosure Policy in the Documentation Kit for more information on determining the legal basis of a request.)

17.6.2 Obtaining a Valid Attestation

To assist in effectuating this prohibition, HHS also requires regulated entities to obtain an attestation in the circumstances listed below from the person requesting the use or disclosure stating that the use or disclosure is not for a prohibited purpose (see Prohibited Uses and Disclosures). A person (including a regulated entity or someone who requests PHI) who knowingly and in violation of the Administrative Simplification provisions obtains or discloses PHI relating to another individual would be subject to potential criminal liability. Compliance with the attestation requirement applies to both CEs and BAs that receive disclosure requests.

17.6.2.1 Circumstances where attestation is required

- Health oversight activities (45 CFR 164.512(d))
- Judicial and administrative proceedings (45 CFR 164.512(e))
- Law enforcement purposes (45 CFR 164.512(f))
- Coroners and medical examiners (45 CFR 164.512(g)(1)

17.6.2.2 Attestation form requirements

Regulated entities may not require the attestation to include any elements not required by the statute.

The attestation must include a statement that the information will not be used for prohibited activities and be signed by the person requesting the information, among other elements.

Regulated entities must review the attestation and any supporting documentation provided by the requester in making their determination as to whether the purpose of the request is prohibited or not.

(See the Welcome Kit > Documentation Kit > Reproductive Health Information for an Attestation Form template).

17.6.2.3 Restrictions

If an attestation is required and not provided, then the regulated entity must omit reproductive records in responding to a request.

If an attestation is required and the provided attestation is defective, then the regulated entity must omit reproductive records when responding to a request.

Minimum necessary also still applies, so if the reproductive health information is not necessary to fulfill the purpose of the request, then it should not be provided.

Even if a required attestation is provided, the regulated entity must still go through the steps to reasonably determine that the purpose of the request is not prohibited (in other words, the attestation is not defective and the stated purpose is not pretextual) and/or the care provided was unlawful; and the use or disclosure must also otherwise be permitted by the Privacy Rule.

An attestation will be limited to the specific use or disclosure. Accordingly, each use or disclosure request for PHI will require a new attestation.

17.6.3 Determining Lawfully Provided Care

If the regulated entity determines that the purpose of the request is prohibited (see Prohibited Uses and Disclosures), then the regulated entity must make a reasonable determination whether the reproductive healthcare was unlawful under the circumstances it was provided.

17.6.3.1 Rule of Applicability i.e. who makes the determination

With respect to whether the care was lawful or not, under the Rule of Applicability, the regulated entity that received the disclosure request is who determines whether the reproductive health care was lawful under the circumstances it was provided.

Under the revised conditions for that determination, the circumstances in which the prohibition applies are determined by the law of the state in which the health care is/was provided.

17.6.3.2 Reasonability Determination

The regulated entity's determination that the care was lawfully provided must be reasonable. Thus, a regulated entity that receives the request for PHI must decide whether it would be reasonable for a similarly situated regulated entity to determine, as provided in the Rule of Applicability, that the reproductive health care is lawful under the circumstances in which such health care is provided.

Consistent with the Privacy Rule's requirements regarding the evaluation of requested disclosures of PHI, in order to make the reasonableness determination, that is, to determine whether it would be reasonable for a similarly situated regulated entity to determine that one or more of the conditions of the Rule of Applicability applies, a regulated entity receiving the request for PHI must evaluate the facts and circumstances under which the reproductive health care was provided. Such facts and circumstances include but are not limited to the individual's diagnosis and prognosis, the time such health care was provided, the location where such health care was provided, and the particular health care provider who provided the health care.

17.6.3.3 Presumption

If the regulated entity that received the request is not the entity that provided the reproductive health care, then there is a regulatory presumption that the care provided was lawful under the circumstances.

This presumption can be overcome where the regulated entity has either actual knowledge, or factual information supplied by the person requesting the use or

disclosure, that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

Example of actual knowledge	Example of factual information
An individual discloses to their doctor that they obtained reproductive health care from an unlicensed person, and the doctor knows that the specific reproductive health care must be provided by a licensed health care provider.	A law enforcement official provides a health plan with evidence that the information being requested is reproductive health care that was provided by an unlicensed person, whereas the law requires that such health care be provided by a licensed health care provider.

If the regulated entity is not who provided the reproductive health care, then it is not reasonable to rely, without additional information, on a statement in an attestation from the person requesting the use or disclosure, that the request is not made for a prohibited purpose or that the underlying reproductive health care was unlawful.

17.6.4 Fulfilling a Request

If the regulated entity reasonably determines that the prohibition does not apply or that the reproductive care was unlawfully provided, then the disclosure may be made as long as it otherwise complies with the Privacy Rule (that is, the request meets the requirements of an applicable permission and is accompanied by a valid attestation where required).

Note:

Since reproductive health care information is not easily segregable from the rest of the medical record the way that psychotherapy notes are, the regulated entity should think about whether it may be easier to require attestations for all PHI requests for the four non-healthcare purposes rather than just for reproductive health PHI. Doing so would reduce the risk that the regulated entity fails to identify whether the PHI is potentially related to reproductive health care, or that the regulated entity is un able to

easily remove or redact information regarding reproductive health care from the medical records.

17.7 Disclosures to Law Enforcement

The Privacy Rule permits uses or disclosures of PHI without an individual's authorization only where such uses or disclosures are expressly permitted or required by the Privacy Rule. As explained in OCR guidance, the Privacy Rule permits, but does not require, certain disclosures to law enforcement and others, subject to specific conditions. Thus, covered healthcare providers, health plans, and healthcare clearinghouses (and business associates), including their workforce members, are only permitted to disclose PHI for law enforcement purposes where they suspect an individual of obtaining reproductive health care (lawful or otherwise) if the covered entity or business associate is required by law to do so and all applicable conditions are met. Accordingly, under the Final Rule, such disclosure is only permitted where all three of the following conditions are met:

- The disclosure is not subject to the prohibition.
- The disclosure is required by law.
- The disclosure meets all applicable conditions of the Privacy Rule permission to use or disclose PHI as required by law.

17.8 Clarification of Personal Representative Qualifications

The changes in the Final Rule clarify that it is not reasonable to elect not to treat a person as an individual's personal representative because the person provides or facilitates reproductive health care for and at the individual's request.

In abuse, neglect, or endangerment situations, notwithstanding a State law or any requirement of the federal implementation requirements to the contrary, a regulated entity may elect not to treat a person as the personal representative if the regulated entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or that treating such person as the personal representative could endanger the individual. The clarification that was added states that it is not a reasonable belief if the basis for the belief is the provision or

facilitation of reproductive health care by such person for and at the request of the individual.

(See the Protected Health Information Use and Disclosure Policy in the Documentation Kit for more information on Personal Representative qualifications.)

17.9 Accounting of Disclosures

Language in policies regarding accounting of disclosures must reflect that disclosures made pursuant to one of the permissions under 45 CFR 164.512(d), (e), (f), or (g) must be included in the accounting, including when they are made pursuant to an attestation. (See the Protected Health Information Accounting of Disclosures Policy in the Documentation Kit for a template of this policy.)

17.10 Breach Notification

Language in policies defining a breach or setting forth notice procedures should be updated to reflect that a disclosure made based on an attestation that contains material misrepresentations or other defects becomes an impermissible disclosure requiring applicable breach notices once the regulated entity becomes aware of the misrepresentation or defect. (See the HIPAA Contingency and Security Incident Policy in the Documentation Kit for a template of this policy.)

17.11 Business Associates

Some Business Associate Agreements or Contracts (BAAs) may also need to be updated to reflect a determination by the parties regarding their respective responsibilities when they receive requests for disclosure when attestation is required—e.g., to add a requirement to notify the other party when they have knowledge that a request is for an unlawful purpose and allocation responsibilities for handling these less frequent requests with respect to reproductive health PHI. (See the Welcome Kit > Documentation Kit > Business Associates for a BAA template.)

18 HIPAA and Part 2

18.1 What is Part 2?

The regulations at 42 CFR part 2 ("Part 2") protect the confidentiality of substance use disorder (SUD) treatment records. These are "records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States." Confidentiality protections help address concerns that discrimination and fear of prosecution deter people from entering treatment for SUD.

The U.S. Department of Health & Human Services (HHS), through the Office for Civil Rights (OCR) in coordination with the Substance Abuse and Mental Health Services Administration (SAMHSA), announced a Final Rule modifying the confidentiality of Substance Use Disorder (SUD) Patient Records regulations at 42 CFR part 2 ("Part 2"). This Final Rule implements requirements of section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act (enacted March 27, 2020), which requires the Secretary to align certain aspects of Part 2 with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

18.2 What entities must comply with Part 2 requirements?

The Part 2-related changes are only required for entities that meet Part 2's definition of a "program". These are:

- federally assisted programs that provide substance abuse education, prevention, training, treatment, rehabilitation, or research;
- if a provider is not a general medical care facility, an individual or entity that holds itself out as providing and provides alcohol or drug abuse diagnosis, treatment, or referral for treatment; and

- medical personnel or other staff in a general medical facility who are identified as providers whose primary function is to provide diagnosis, treatment, or referral for treatment for a SUD.

If a provider is not a Program, these Part 2 related changes do not apply.

18.3 Part 2 Requirements

Patient notice requirements and Notice of Privacy Practices (NPP) requirements have been modified to provide consistent notices with respect to records that are PHI, Part 2 records, or both. The primary changes Part 2 providers will need to make in relation to Part 2 are to the NPP. Patient consent forms will also likely need to be updated.

The key changes are as follows:

18.3.1 Patient consent

A single patient consent is now allowed for all future uses and disclosures for treatment, payment, and health care operations. The updated Part 2 rule also allows covered entities and business associates that receive records under the single consent to redisclose the records in accordance with the HIPAA regulations. However, the updated Part 2 rule does not allow combining patient consent for the use and disclosure of records for civil, criminal, administrative, or legislative proceedings with a patient consent for any other use or disclosure. Separate patient consents are required for the use and disclosure of substance use disorder counseling notes. Also, each disclosure made with patient consent must include a copy of the consent or a clear explanation of the scope of the consent. A patient's right to access their own SUD records has also been expanded.

18.3.2 Other uses and disclosures

The updated Part 2 rule permits disclosure of patient records without patient consent to public health authorities, as long as the records disclosed are de-identified according to HIPAA standards. Part 2 records and testimony relaying them may not be used in civil, criminal, administrative, and legislative proceedings against patients without patient consent or a court order.

18.3.3 Safe harbor for investigative agencies

The updated Part 2 rule creates a "safe harbor" that limits civil or criminal liability for investigative agencies that act with reasonable diligence to determine whether a provider is subject to Part 2 before making a demand for records in the course of an investigation. In order to demonstrate "reasonable diligence" before requesting records, an investigative agency must look for a provider in SAMHSA's online treatment facility locator or similar state database where available, and check a provider's website or physical location to determine whether it provides Part 2 services, and viewing the Patient Notice or HIPAA NPP if available online.

18.3.4 Segregation of information

The updated Part 2 rule includes an express statement that segregating or segmenting Part 2 records is not required. This means that Part 2 records can be maintained as part of an electronic health record or other comprehensive patient record system. However, the rule also adds a new definition, SUD Counseling Notes, for a clinician's notes analyzing the conversation in a counseling session that the clinician voluntarily maintains separately from the rest of the patient's treatment and medical record. These SUD Counseling Notes require specific consent from an individual and cannot be used or disclosed based on a broad consent for treatment, payment and healthcare operations. This is analogous to the HIPAA protections for psychotherapy notes. A provider may, therefore, be required to redact or exclude SUD Counseling Notes from a use or disclosure.

18.3.5 Specific changes to the NPP required for Part 2 programs

There are newly required references to Part 2 in mentioning "other applicable law" and a new paragraph adding a notice requirement for regulated entities creating or maintaining Part 2 records. The requirement to provide an NPP in plain English is now not just required by the Privacy Rule but also Part 2.

Regulated Entities that that participate in organized health care arrangements (OHCAs) may issue a joint NPP if certain requirements are met, including a new paragraph (d)(4) adding a clarification with respect to Part 2 obligations that a joint notice doesn't remove obligations or duties of each Part 2 entity or remove any patient rights.

Part 2 records or testimony relaying their content shall not be used in civil, criminal, administrative, or legislative proceedings against the individual without their written consent or a court order after notice and an opportunity to be heard.

If Part 2 records will be used for fundraising for the regulated entity's benefit, the individual must be provided with a clear and conspicuous opportunity to opt out.

18.3.6 Penalties

Enforcement and penalties have been aligned with HIPAA, so violators of Part 2 will now be subject to the same potential civil and criminal penalties as covered entities and business associates for HIPAA violations. The same mitigating factors and consideration of level of culpability will apply to Part 2 enforcement as well. DOJ will continue to have enforcement authority for criminal penalties and state attorneys general may bring civil suits on behalf of state residents.

18.3.7 Breach Notification

The Final Rule applies the same requirements of the HIPAA Breach Notification Rule to breaches of records under Part 2.