



2016 HIPAA Audit Protocol List

<http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html>

HIPAA PRIVACY RULE

1. Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes
2. Deceased individuals
3. Confidential communications
4. Uses and disclosures consistent with notice
5. Disclosures by whistleblowers
6. Disclosures by workforce members who are victims of a crime
7. Business associate contracts
8. Requirements for group health plans
9. Requirements for a covered entity with multiple covered functions
10. Permitted uses and disclosures
11. Consent for uses and disclosures
12. Authorizations for uses and disclosures is required
13. Compound authorizations – Exceptions
14. Prohibition on conditioning of authorizations
15. Uses and Disclosures for which an Authorization is Required – Documentation and Content
16. Use and Disclosure for Facility Directories; Opportunity to Object
17. Uses and Disclosures for Facility Directories in Emergency Circumstances
18. Permitted uses and disclosures
19. Uses and disclosures with the individual present
20. Limited uses and disclosures when the individual is not present
21. Uses and disclosures for disaster relief purposes
22. Uses and disclosures when the individual is deceased
23. Uses and disclosures required by law
24. Uses and disclosures for public health activities
25. Disclosures about victims of abuse, neglect or domestic violence
26. Uses and disclosures for health oversight activities
27. Disclosures for judicial and administrative proceedings
28. Disclosures for law enforcement purposes
29. Disclosures for law enforcement purposes - for identification and location
30. Disclosures for law enforcement purposes-- PHI of a possible victim of a crime
31. Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct
32. Disclosures for law enforcement purposes: crime on premises
33. Disclosures for law enforcement purposes
34. Uses and disclosures about decedents
35. Uses and disclosures for cadaveric organ, eye or tissue donation
36. Uses and disclosures for research purposes -- Permitted Uses and Disclosures
37. Uses and disclosures for research purposes -- Documentation of Waiver Approval
38. Uses and disclosures for specialized government functions -- Military
39. Uses and disclosures for specialized government functions -- National Security and intelligence activities
40. Uses and disclosures for specialized government functions -- Medical Suitability Determinations
41. Uses and disclosures for specialized government functions -- Correctional institutions
42. Uses and disclosures for specialized government functions -- Providing public benefits
43. Disclosures for workers' compensation
44. Requirements for De-Identification of PHI & Re-Identification of PHI
45. Minimum Necessary - Disclosures of PHI
46. Minimum Necessary requests for protected health information
47. Minimum Necessary - Other content requirement

48. Limited Data Sets and Data Use Agreements
49. Uses and Disclosures for Fundraising
50. Uses and Disclosures for Underwriting and Related Purposes
51. Verification Requirements
52. Notice of Privacy Practices Content requirements
53. Provisions of Notice - Health Plans
54. Provisions of Notice - Certain Covered Health Care Providers
55. Provision of Notice - Electronic Notice
56. Joint Notice by Separate Covered Entities
57. Documentation
58. Right of an Individual to Request Restriction of Uses and Disclosures
59. Terminating a Restriction
60. Documentation
61. Confidential Communications Requirements
62. Right to access
63. Denial of Access
64. Unreviewable grounds for denial
65. Reviewable grounds for denial
66. Review of denial of access
67. Documentation
68. Right to Amend
69. Denying the Amendment
70. Accepting the Amendment
71. Denying the Amendment
72. Right to an Accounting of Disclosures of PHI
73. Content of the Accounting
74. Provision of the Accounting
75. Documentation
76. Personnel designations
77. Training
78. Safeguards
79. Complaints to the Covered Entity
80. Complaints to the Covered Entity
81. Mitigation
82. Refraining from Intimidating or Retaliatory Acts
83. Waiver of rights
84. Policies and Procedures
85. Documentation

HIPAA SECURITY RULE

86. General Requirements
87. Flexibility of approach
88. Security Management Process
89. Security Management Process -- Risk Analysis
90. Security Management Process -- Risk Management
91. Security Management Process -- Sanction Policy
92. Security Management Process -- Information System Activity Review
93. Assigned Security Responsibility
94. Workforce Security
95. Workforce security -- Authorization and/or Supervision
96. Workforce security -- Workforce Clearance Procedure
97. Workforce security -- Establish Termination Procedures
98. Information Access Management
99. Information Access Management -- Isolating Healthcare Clearinghouse Functions
100. Information Access Management -- Access Authorization
101. Information Access Management -- Access Establishment and Modification
102. Security Awareness and Training
103. Security Awareness and Training -- Security Reminders

104. Security Awareness, Training, and Tools -- Protection from Malicious Software
105. Security Awareness, Training, and Tools -- Log-in Monitoring
106. Security Awareness, Training, and Tools -- Password Management
107. Security Incident Procedures
108. Security Incident Procedures -- Response and Reporting
109. Contingency Plan
110. Contingency Plan -- Data Backup Plan
111. Contingency Plan -- Disaster Recovery Plan
112. Contingency Plan -- Emergency Mode Operation Plan
113. Contingency Plan -- Testing and Revision Procedure
114. Contingency Plan -- Application and Data Criticality Analysis
115. Evaluation
116. Business Associate Contracts and Other Arrangements
117. Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement
118. Facility Access Controls
119. Facility Access Controls -- Contingency Operations
120. Facility Access Controls -- Facility Security Plan
121. Facility Access Controls -- Access Control and Validation Procedures
122. Facility Access Controls -- Maintain Maintenance Records
123. Workstation Use
124. Workstation Security
125. Device and Media Controls
126. Device and Media Controls -- Disposal
127. Device and Media Controls -- Media Re-use
128. Device and Media Controls -- Accountability
129. Device and Media Controls -- Data Backup and Storage Procedures
130. Access Control
131. Access Control -- Unique User Identification
132. Access Control -- Emergency Access Procedure
133. Access Control -- Automatic Logoff
134. Access Control -- Encryption and Decryption
135. Audit Controls
136. Integrity
137. Integrity -- Mechanism to Authenticate ePHI
138. Person or Entity Authentication
139. Transmission
140. Transmission Security -- Integrity Controls
141. Transmission Security -- Encryption
142. Business Associate Contracts or Other Arrangements
143. Business associate contracts.
144. Business associate contracts.
145. Business associate contracts.
146. Other Arrangements
147. Business associate contracts with subcontractors
148. Requirements for Group Health Plans
149. Group Health Plan Implementation Specification
150. Group Health Plan Implementation Specification
151. Group Health Plan Implementation Specification
152. Group Health Plan Implementation Specification
153. Policies and Procedures
154. Documentation
155. Documentation -- Time Limit
156. Documentation- Availability
157. Documentation -- Updates

HIPAA DATA BREACH RULE

- 158. Administrative Requirements
- 159. Training
- 160. Complaints
- 161. Sanctions
- 162. Refraining from Retaliatory Acts
- 163. Waiver of Rights
- 164. Policies and Procedures
- 165. Documentation
- 166. Definitions: Breach – Risk Assessment
- 167. Definitions: Breach - exceptions Unsecured PHI
- 168. Notice to Individuals
- 169. Timeliness of Notification
- 170. Content of Notification
- 171. Methods of Notification
- 172. Notification to the Media
- 173. Notification to the Secretary
- 174. Notification by a Business Associate
- 175. Law Enforcement Delay
- 176. Burden of Proof

Confused? Afraid? Aren't Sure You Can Pass?

We can help.

www.semelconsulting.com

888-997-3635 x 202

rose@semelconsulting.com