ComplianceProSolutions™

List of Documents That May be Requested for OCR Phase 2 Audits (2016)

Editorial Comments: This list has been created from the actual language of the OCR breach protocols that has been cleaned up and at times been rendered more readable. The intent was to capture all of the possible requests generated by action verbs within the OCR 'Audit Inquiry' column within the protocol line items, at least in a somewhat summarized form. The intent is to have generated a easily useable list that can work with the more detailed spreadsheets Kelly McLendon and CompliancePro has produced to look up the more exact language and supporting information such as elements to consider during review that yield higher understanding of what might be expected in an OCR audit. Also note that OCR themselves may ask for documents in a slightly different manners than listed here, again the idea is to be close and predictable about what might be asked for, the exact details will only be known when produced and delivered for response by OCR.

None of this is guaranteed accurate nor should it be construed as any type of legal advice. This information is for reference purposes only.

Yellow highlighting indicates actual OCR audit document requests that were made for the desk audits in summer 2016 from 167 sites. The actual language of the request may not exactly meet the original text from the OCR website and summary thereof provided by CompliancePro, but it'll be close.

Total number of discrete requests as estimated by this document: Breach 45, Privacy 137, Security 187. These are the numbers the rules say could be requested, but with consolidation and paraphrasing they use to create the requests who knows how many documents would have to be provided in a full scope privacy, security and breach rule audit. These sheer volume of requests they could make as illustrated by this document call for deep preparation for an audit of this kind, undoubtedly given OCR's language to date there will be more comprehensive audits in the future much wider than the 7 controls examined in the July desk audits. So prepare and be ready by becoming familiar with whether your entity could provide the items requested as listed in the protocols and within this document.

The number in parenthesis at the end of each line item e.g. (BNR16) corresponds to the OCR protocols numbers we finally were made aware of (the prefixes - BNR=Breach Rule, P=Privacy Rule & S=Security Rule). If multiple numbers are in parenthesis e.g. (BNR1) (BNR7) (BNR7) (BNR9)(BNR12) this indicates a line item that is repeated and addressed within multiple protocols addressed. Look for ';' acting as separators denoting the areas consolidated in the text of the line item from several original pieces of information.

ComplianceProSolutions™

Contents

Breach Audit Request Documents

1. P&P related to Breach, including language regarding training; complaints to CE; sanctions; refraining from retaliatory acts; waiver of rights and documentation; notification (individuals & media)l; and other areas (BNR1) (BNR7)(BNR12) (BNR13) (BNR14) (BNR15) (BNR16) (BNR16) (BNR18)
2. Copy of the content of training (BNR2)
3. Evidence of training (e.g. sign-in sheets) (BNR2)
4. Breach complaint process in place (BNR3)
5. List of complaints received in the specified period and the disposition of such complaints (BNR3)
6. Use sampling methodologies to select complaints to be reviewed (BNR3)
7. Documentation of actions taken by the CE or BA to investigate and resolve the potential breach (BNR3)
8. List of sanctions; include type of action led to sanction and other relevant info (BNR4)
9. Use sampling methods to choose sanctions to be reviewed (BNR4)
10. P&P related to refraining from retaliatory acts (BNR5)
11. Obtain any patient or health plan member intake forms to ensure they contain waiver of rights language (BNR6)
12. P&P for requiring BA to report an impermissible use or disclosure of PHI to the CE and the CEs process for handling such reports (BNR7)
13. Documentation that the CE maintains its P&P, in written or electronic form, until 6 years after the later of the date of their creation or the last effective date (BNR8)
14. Documentation that the CE maintains all other documentation required by 164.530(j)(1) until 6 years after the later of the date of their creation or the last effective date (BNR8)
15. Process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised (BNR9)
16. If there's not a process for breach assessment, does the CE have a P&P that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI (BNR9)
17. Review the CE's risk assessment P&P, if the CE does not have a P&P that treats all potential breaches as requiring notifications without conducting a risk assessment (BNR9)
18. List of risk assessments, if any, conducted within the specified period where the CE determined there was a low probability of compromise to the PHI (BNR9)
19. Use sampling methodologies to select documentation of risk assessments (BNR9)

20. List of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification (BNR9)
21. Use sampling methodologies to select documentation of risk assessments (BNR9)
22. Documentation of a determine that one of the regulatory exceptions to the definition of breach at §164.402(1) applies (to a potential breach), if any (BNR10)
23. Use sampling methodologies to select and review documentation of one of the regulatory exceptions to the definition of breach (BNR10)
24. Obtain documentation is a CE or BA determine that the breach did not require notification, because the PHI was not unsecured PHI (BNR10)
25. Use sampling methodologies to select and review documentation determining that the breach did not require notification, because the PHI was not unsecured PHI (BNR10)
26. Question from July 2016 audit: Upload documentation of five breach incidents for the previous calendar affecting fewer than 500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification (BNR12)(BNR16)
27. Question from July 2016 audit: If the entity used a standard template or form letter, upload the document (BNR13)
28. Obtain a list of breaches, if any, in the specified period and documentation indicating (BNR12)
29. Question from July 2016 audit: upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year (BNR13)(BNR15)(BRN16)
30. Question from July 2016 audit: Upload a copy of a single written notice sent to affected individuals for each breach incident (BNR13)
31. List of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach (BNR13)
32. Use sampling methodologies to select notifications sent to individuals to be reviewed (BNR13)
33. Documentation of any breaches within the specified period that required substitute notice (BNR14)
34. Documentation of a conspicuous posting on the home page of the covered entity's web site or a copy of conspicuous notices in major print or broadcast media and documentation of a toll-free phone number that remained active for at least 90 days (BNR14)
35. Use sampling methodologies to select notifications to be reviewed (BNR14)
36. Documentation to verify that the media notifications included the elements required (BNR15)
37. Documentation of notifications provided to the Secretary (BNR16)
38. Sampling methodologies to select notifications to be reviewed (BNR16)
39. Documentation of notifications provided to the Secretary (BNR16)
40. Sampling methodologies to select notifications to be reviewed (BNR16)
41. Copies of the notification(s) sent by the BA (or subcontractor) to the CE (or BA for breaches by subcontractors) (BNR17)
42. Use sampling methodologies to select notifications sent by the BA (or subcontractor) to the CE (or BA for breaches by subcontractors) to be reviewed (BNR17)
43. Documentation of any such law enforcement statement about delayed notification of a breach of unsecured PHI (BNR18)
44. Use sampling methodologies to select notifications to be reviewed (BNR18)

45. Documentation to prove CE or BA took correct action (BNR19)

Privacy Audit Request Documents

1. Underwriting policies and procedures related to use and disclosure of genetic information (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials) (P1)
2. P&P regarding use and disclosure of PHI including, deceased individual's PHI, Personal Representative (P2) (P3)
3. Sample for compliance where Personal Representative request was recognized by the entity (P3)
4. Sample for compliance where PR request was not recognized by the entity (P3)
5. P&P regarding requests for confidential communications (P4)
6. Sample of confidential communications requests made by individuals (P4)
7. Sample of communications to individuals where a conf communications request was accepted (P4)
8. P&P regarding PHI uses & disclosures, evaluate if constant with NPP (P5)
9. Documentation of disclosures by a workforce member not otherwise permitted by the Privacy Rule that the entity determined to meet the requirements of this standard (whistleblower) (P6)
10. P&P related to disclosure of PHI by workforce members who are a victim of a crime (P&)
11. P&P related to Identification and engagement of Business Associates and establishment of BAAs (P8)
12. Sample of BAA to evaluate compliance with PC and P&P (P8)
13. BAA between CE and BA to include provisions for subsequent BAs/subcontractors to provide adequate assurances (P8)
14. Documentation of any material breach with BAs (P8)
15. Documentation of reports from BA to CE of uses or disclosures not provided in its contract (P8)
16. Group health plans documents for restrictions on uses and disclosure of PHI in compliance with PC (P9)
17. P&P restrict use of PHI to appropriate function being performed (e.g. provider, health plan, clearinghouse) (P10)
18. P&P related to uses and disclosures of PHI for TPO (P11)
19. Sample of completed consents, if any and patient intake materials (P12)
20. P&P for obtaining a valid authorization as required by the standard, including seeking authorizations from individuals) (P13) (P15)
21. Sample of a standard covered entity authorization (P13)
22. Sample of authorizations obtained (by a patient or 3rd party) to permit disclosures (P13)
23. For providers only: All relevant patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any (P13)
24. Sample of a compound authorizations (research related), if any (P14)
25. P&P related to seeking authorizations from individuals (P15)
26. Sample of conditioned authorizations (probably health plan or research related) (P15)
27. Sample of conditioned authorizations to assess exceptions (P15)
28. Sample of authorizations used as a basis for disclosure (P16)
29. Sample of the directory on a certain date along with an individual's objections (P17)

30. P&P for use and disclosures, including address determining if individual has objected to use and disclosure for facility directory and documentation of such determination; to disclose directory in emergency, those to family members, relatives, close friends or others identified by the individual; determining or inferring individual agreement or lack objection to disclosure of PHI with individual present; disclosing only relevant info to persons when individual is not present; disclosure of PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts; documenting the individual's prior expressed preference and relationship of family members and other persons to the individual's care or payment for care; uses and disclosures for victims of abuse neglect or domestic violence pursuant to judicial or administrative proceedings and law enforcement purposes; Neglect or domestic violence pursuant to judicial or administrative proceedings and law enforcement purposes; how the CE determines whether and how to make disclosure about victims of abuse, neglect or domestic violence; using or disclosing PHI for health oversight activities; disclosures during administrative or judicial proceeding; disclosures of PHI for law enforcement purposes; to disclosures of PHI to law enforcement officials for identification and location purposes; disclosing PHI to a possible victim of a crime in response to a law enforcement request; disclosures of PHI to law enforcement officials that address the requirement for an individual who has died as a result of suspected criminal conduct; disclosures of PHI about an individual who may have committed a crime on the premises to law enforcement officials; disclosures of what information about a medical emergency is necessary to disclose to alert law enforcement of PHI to law enforcement officials; disclosures of PHI to coroners and medical examiners and funeral directors; disclosures of PHI for purposes of cadaveric organ, eye, or tissue donation; disclosures for military and veterans purposes; disclosures for national security and intelligence activities and purposes; disclosure of PHI for protective services; use and disclose PHI Medical Suitability Determinations if the CE is a component of the Department of State; correctional institution or individual in custody; disclosures of PHI for Workers Comp or other similar programs (P17) (P18) (P19) (P20) (P21) (P22) (P23) (P24) (P25) (P26) P27) (P28) (P29) (P30) (P31) (P32) (P33) (P34) (P35) (P36) (P39) (P40) (P41)(P42)(P43) (P45)
31. Sample of Public Health uses and disclosures, to include uses and disclosures to an employer about an individual who is a member of the workforce of the employer (P25)
32. Sample of disclosure made for health oversight activities (P27)
33. If CE is a health oversight agency, the P&P for using PHI for health oversight activities (P27)
34. Sample of uses made for health oversight activities (P27)
35. Sample of disclosures and the corresponding court orders, subpoenas, or discovery requests (P28)
36. Sample of disclosures and the corresponding court orders, subpoenas, disclosure requests, etc (P29)
37. Sample of responses to law enforcement officials request for PHI for identification and location purposes (P30)
38. Samples of responses to law enforcement related to disclosing PHI to a possible victim of a crime in response to a law enforcement request (P31)
39. Sample of documentation of a disclosure for an individual who has died as a result of suspected criminal conduct disclosure (P32)
40. Sample documentation related to disclosures of PHI about an individual who may have committed a crime on the premises to law enforcement officials (P33)

41. Sample documentation related to disclosures of what information about a medical emergency is necessary to disclose to alert law enforcement of PHI to law enforcement officials (P34)
42. Sample documentation of disclosures of PHI to coroners and medical examiners and funeral directors (P35)
43. Sample of disclosures of PHI to organ procurement organizations (P36)
44. P&P for CE to disclose PHI for research purposes (P37)
45. Authorization, or waiver of the authorization, has been approved by an IRB or appropriately configured privacy board (P37)
46. From the researchers the required representations regarding reviews preparatory to research on decedents (P37)
47. Entity obtained the necessary authorization and/or waiver to conduct the research (P37)
48. Board approval of a waiver of authorization (P37)
49. Use or disclosure is solely to review PHI as necessary to prepare a research protocol (P37)
50. Representation that the use or disclosure is solely for research on the PHI of decedents (P37)
51. P&P to determine what documentation of approval or waiver for research purposes is needed to permit a use or disclosure and to apply that determination (P38)
52. Sample documentation of any approval or waiver for research purposes that contains all the information necessary to permit a use or disclosure (P38)
53. List of uses and disclosures for military and veterans activities (P39)
54. Sample documentation related to correctional institution or individual in custody (P43)
55. P&P related to uses and disclosures if a CE is a health plan that is a government program providing public benefits, or is it a government agency administering a government program providing public benefits (P44)
56. Sample documentation of uses and disclosures if a CE is a health plan that is a government program providing public benefits, or is it a government agency administering a government program providing public benefits (P44)
57. Sample documentation related to disclosures of PHI for Workers Comp or other similar programs (P45)
58. P&P related to De-Identification of PHI & Re-Identification of PHI (P46)
59. P&P related to limiting access to PHI (P47)
60. Sample documentation of workforce members access to PHI for their corresponding job title and description (P47)
61. P&P related to minimum necessary use or disclosure of PHI and; to limit the PHI requested to the amount minimally necessary to achieve the purpose of the disclosure; to minimum necessary uses and disclosures or requests for entire medical record (P48) (P49) (P50)
62. Sample of protocols for disclosures made on a routine and recurring basis and determine if they limit PHI (P48)
63. Sample of requests made on a routine and recurring basis to determine if minimum necessary followed (P41)
64. Sample documentation related to the use, disclosure or request for an entire medical record (93)
65. P&P related to Limited Data Sets and Data Use Agreements if there any data use agreements in place between CE and it's recipients (P51)

66. A sample data use agreement (P51)
67. A sample limited data set (P51)
68. P&P and notice of privacy practices (NPP) for disclosures of PHI to BA or institutionally related foundations (P52)
69. A sample of communications for fundraising purposes to determine if it contains a clear and conspicuous opportunity to opt-out of further fundraising communications or reference to a mechanism for opting out (P52)
70. Documentation that the P&P are conveyed to the workforce (P52)
71. P&P related to a health plan addressing limitations on use and disclosure of PHI for underwriting and other purposes (P53)
72. P&P if health insurance or health benefits are not placed with the health plan limiting further use or disclosure for such purpose or as may be required by law (P53)
73. P&P in (§ 164.502(a)(5)(i)) regarding underwriting and GINA subject to the prohibition (102)
74. P&P regarding verification of the ID of persons requesting PHI (P54)
75. Sample documentation of how the CE has verified several requestors, could include copy or notation of official credentials, a completed verification checklist, a copy of the request on official letterhead, etc. (P54)
76. Obtain a copy of NPP to validate required elements. Provide all copies of NPP (translated, etc) (P55)
77. Question from July 2016 audit: Upload a copy of all notices posted on website and within the facility, as well as the notice distributed to individuals, in place as of the end of the previous calendar year.
78. P&P for Provisions of Notice - Health Plans regarding the provision and posting of the NPP (P55)
79. For a sample of individuals, obtain and review documentation of when and how notices were provided (P55)
80. NPP as part of a standard mailing sent to new health plan members provide a NPP provided to the selected individuals (P55)
81. Question from July 2016 audit: P&P in place regarding the NPP (Notice of Privacy Practices) (P57) (P58) (P60)
82. Sample acknowledgement of receipt of NPP and documenting showing a good faith effort was made when an acknowledgement could not be obtained (P57)
83. A sample population of individuals who were new documentation to determine if initial date of service corresponds with date NPP was received, if they do not match was the first encounter an emergency or other explanation (P57)
84. Documentation related to provision of NPP to patients who present as an emergency (P57)
85. Observe the web site to determine if the NPP is prominently displayed and available. An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices (P58)
86. Documentation of the agreement with the individual to receive the notice via e-mail or other electronic form; If the CE has experienced failures when trying to provide the NPP by e-mail documentation of its attempts to provide a paper copy of the notice via alternative means (e.g., mail) (P58)
87. Question from July 2016 audit: Upload the URL for the entity web site and the URL for the posting of the entity notice (NPP), if any. (P58)

88. Question from July 2016 audit: If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically (P58)
89. Question from July 2016 audit: Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form (P58)
90. P&P for joint notice by separate covered entities. For CEs that participate in an OHCA use a joint NPP (P59)
91. Applicable documentation criteria for NPP are established and communicated to the workforce (copies of all applicable notices and sample of acknowledgements) (P60)
92. P&P permitting an individual to request a restriction on the use of PHI for TPO; and for terminating restrictions; documenting and maintaining documentation on restriction requests (P61) (P62) (P63)
93. Sample of documentation of each request and subsequent agreement to determine if restrictions are given effect (P61)
94. All requests since 9/23/13 for restrictions to a health plan for an item or service that has been paid out of pocket (P61)
95. Documentation to see if such restrictions were given effect (P61)
96. Sample documented terminated restriction (P62)
97. Has the CE agreed to any restrictions in the past 6 years? (P63)
98. P&P permit individuals to request alternative means or locations to receive communications of PHI (P64)
99. Sample requests for alternative means or locations to receive communications of PHI and the covered entity response (P64)
100. Question from July 2016 audit: Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year. (P65)
101. Question from July 2016 audit: Upload all documentation related to the last five access requests for which the entity extended the time for response to the request (P65)
102. Question from July 2016 audit: Upload any standard template or form letter required by or used by the CE to document access requests (P65)
103. Question from July 2016 audit: Upload the notice of privacy practices (NPP) (P65)
104. Question from July 2016 audit: Upload policies and procedures for individuals to request and access to protected health information (PHI) (P65)
105. P&P for individuals to request and obtain access to PHI and; to denial of access ensuring timely, written denials with all required elements; dictating when denials of requests for access are unreviewable; reviewable grounds for denial of access; request for and fulfillment of instances of denial of access; if a person or office is specified to process requests for access (P65)(P66) (P67) (P68) (P69)(P70)
106. NPP for correct reference to access rights (P65)
107. Access requests that were granted and documentation of fulfillment if any, and access requests that were denied to determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided (P65)
108. A standard form for individual's requesting access to their PHI (P65)
109. Sample of denied access requests (P66)

110. Documentation of the current DRS (Designated Record Sets) subject to access requests along with documentation for last 6 years (P70)
111. Name or office for each of the last 6 years that process access requests (P70)
112. P&P allowing an individual the right to amend protected health information in a designated health record set and; circumstances which the entity has grounds for denial of amendment; denial of amendment request (P71) (P72) (P74)
113. Sample of requests by individuals to amend their PHI in a DRS (P73)
114. Sample of requests related to denials of amendments (P74)
115. P&P in place to document and respond to an AOD request, including limiting grounds for denial; to provide individual with timeliness and fees for AOD (P75)(P76) (P77)
116. Sample of request for AOD and the entity fulfillment of those requests (P76)
117. Documentation of who is responsible for development and implementation of P&P (P79)
118. Documentation of what person or office is designated to receive complaints; how complaints are received, processed and documented (P79) (P82)
119. Documentation of development & implementation of P&P and complaints are maintain in electronic or written form for 6 years (P79)
120. P&P related to training its workforce as necessary and timely (P80)
121. From the population of new hires within specified audit period a sample of the documentation of training on the HIPAA privacy rule that was provided and completed (P80)
122. Documentation that workforce members have been trained on material changes to P&P (15
123. P&P to determine if appropriate administrative, technical & physical safeguards are in place (P81)
124. Documentation of specific safeguards from all 3 categories to reasonably protect PHI. Such documentation may include, but is not limited to; P&P, photographic or documentary documentation of physical and technical safeguards and statements from privacy and security officials (P81)
125. Sample of documentation of complaints (P83)
126. P&P to determine if the entity has applied sanctions (P84)
127. Documentation of applicable sanctions to a sample of workforce members to determine if appropriate sanctions were applied (P84)
128. Documentation related to a CE mitigating any harmful effect known to the CE of a use or disclosure by CE or BA in violation of P&P (P85)
129. Documentation that a process is in place to ensure mitigation actions are taken pursuant to the P&P (P85)
130. From a population of non-compliance within the audit period whether mitigation plans were developed and applied pursuant to the P&P (P85)
131. Documentation that P&P are conveyed to workforce (P85)
132. P&P in place in relation to anti-intimidation and anti-retaliatory standards (P86)
133. Documentation that P&P related to anti-intimidation and anti-retaliatory standards are conveyed to the workforce (P86)

134. P&P and patient health plan/member info to ensure that a waiver of their right to complain is not required as a condition of treatment, payment or enrollment in a health plan or eligibility for benefits (P87)
135. P&P with respect to PHI designed to comply with the requirements of the HIPAA Privacy Rule including evidence that P&P are reasonably designed to ensure compliance for size and types of activities performed, that the entity changes promptly these P&P as necessary to comply with changes in the law, that any corresponding changes are made to the NPP as applicable (170)
136. Copies of P&P from the previous calendar year and January 1, 2012 and the corresponding NPP in effect for those dates illustrating that material changes e.g. for health plans limits on genetic info for underwriting, for providers that a request for restriction must be accepted in certain situations are incorporated into the P&P (P88)
137. Documentation of maintenance all required P&P written communications and documentation in written or electronic form (P89)

Security Audit Request Documents

1. Question from July 2016 audit: P&P regarding the entity's risk analysis process (S2)
2. Question from July 2016 audit: Documentation demonstrating that P&P related to security risk analysis were in place and in force six (6) years prior to the date of receipt of notification (S2)
3. Question from July 2016 audit: Documentation of risk analysis results from the previous calendar year and that such documentation is available to the persons responsible for this implementation and that such documentation is periodically reviewed and, if needed, updated (S2)
4. Question from July 2016 audit: Upload documentation of the current risk analysis and the most recently conducted prior risk analysis (S2)
5. Question from July 2016 audit: Upload documentation of current risk analysis results (S2)
6. Obtain risk analysis P&P; Upload policies and procedures regarding the entity's risk analysis process (S2)(S4)
7. P&P related to security variations and evaluation of compliance with PC for countermeasures or safeguards implemented - Question from July 2016 audit: Documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment (S3)
8. Question from July 2016 audit: Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment (S3)(S5)
9. Documentation demonstrating these P&P have been implemented and that the processes match the P&P (S3)
10. Question from July 2016 audit: Documentation demonstrating that policies and procedures related to reducing risk as result of a security risk analysis and mitigation/remediation of its results are in place and in force six (6) years prior to the date of receipt of notification (S3)
11. Question from July 2016 audit: Documentation demonstrating the efforts used to manage risk during the previous calendar year (S3)
12. Question from July 2016 audit: P&P related to the risk management process (S3)(S5)
13. Question from July 2016 audit: Documentation demonstrating that current and ongoing risks reviewed and updated (S3)
14. Question from July 2016 audit: Documentation from the previous calendar year demonstrating that documentation related to reducing risk as result of a security risk analysis and mitigation / remediation of its results is available to the persons responsible for security risk analysis and the risk reduction processes and that such documentation is periodically reviewed and, if needed, updated (S3)
15. P&P addressing purpose & scope, workforce member responsibility, management involvement and how frequently the analysis is reviewed and updated (S4)
16. Written risk analysis documents or other records that document an accurate assessment was conducted that contains: a. Defined scope of all systems that create, transmit, maintain or transmit

ePHI, b. Details of identified threats, c. Assessment of current security measures, d. Impact & likelihood analysis, e. Risk rating (S4)

17. If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any (S4)
18. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why (S4)
19. Sanctions P&P (S6)
20. Documentation demonstrating sanctions applied to workforce members (S6)
21. P&P related to records of info systems activities (S7)
22. Documentation of reviews of info system activity such as audit logs, access reports, security incident tracking (S7)
23. Documentation demonstrating capabilities of the info system logs (S7)
24. Documentation of the security official's responsibilities (e.g. job description) (S8)
25. P&P ensuring all workforce members have access to ePHI required to perform their job (S9)
26. Documentation of access granted to workforce members and correlation to their job duties (S9)
27. Documentation demonstrating management reviews access levels for systems with ePHI that access is appropriate (S9)
28. P&P related to authorization/supervision of workforce members (S10)
29. Documentation of how requests for access to ePHI are processed (S10)
30. Identification of who has the authorization and/or supervisory permission to approve. Access to information systems and/or locations where ePHI may be accessed (S10)
31. Documentation demonstrating how access requests to locations where ePHI might be accessed are processed (S10)
32. Documentation of workforce members who were authorized access to ePHI or locations where ePHI might be accessed and organizational charts/lines of authority (S10)
33. If an alternative measure (addressable) has been implemented produce documentation of why the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented (S10)
(S11)(S12)(S15)(S16)(S18)(S19)(S20)(S21)(S28)(S29)(S34)(S35)(S36)(S37)(S43)(S44)(S48)(S49)(S52)(S55)(S56)
34. Documentation related to workforce clearance procedures and whether they work to determine whether access is appropriate (S11)
35. Documentation demonstrating use of workforce clearance in granting appropriate access to ePHI (S11)
36. Documentation demonstrating approval or verification of access to ePHI (e.g., approved access request forms, electronic approval workflow, etc.) (S11)
37. Documentation that access was terminated (S12)
38. Documentation demonstrating changes in access levels for workforce members with ePHI access (S12)
39. Documentation of the job duties of workforce members before and after ePHI access level was changed (S12)

40. P&P to determine that access is reasonably and appropriately restricted to those that need access. (S13)
41. P&P for minimum necessary (S13)
42. Access controls that support Minimum Necessary (S13)
43. P&P related to protecting ePHI held by clearinghouse from unauthorized access by the larger organization (S14)
44. P&P regarding workforce member access to ePHI (S15)
45. Procedures to create enable, modify, disable, and remove information system accounts (S15)
46. Documentation associated with granting access to ePHI (S15)
47. P&P and evaluate content relative to PC for authorizing access, documenting, reviewing and modifying user access to workstation, transaction, program or process (S16)
48. Documentation regarding individuals whose access to info systems has been reviewed based on access authorization P&P (S16)
49. Documentation of individuals whose access has been modified based on access P&P (S16)
50. P&P for security awareness & training program (S17)
51. Documentation demonstrating implementation of security & awareness program including related training materials (S17)
52. Documentation demonstrating that security awareness programs are provided to the entire organization and BA if appropriate (S17)
53. Documentation of how periodic security reminders are conducted (S18)
54. Documentation demonstrating that periodic security updates are conducted (S18)
55. Procedures against, detecting and reporting malicious software are incorporated into security training (S19)
56. Documentation of the workforce members who should be trained on procedures to guard against, detect and report malicious software (S19)
57. Procedures (or other vehicle) for monitoring login and reporting discrepancies and related training materials (S20)
58. Documentation demonstrating procedures in place to monitor login attempts and report discrepancies (S20)
59. Documentation of workforce members role types and who should be trained about monitoring and reporting login attempts (S20)
60. Password management procedures and training for creating, changing and safeguarding passwords (S21)
61. Documentation demonstrating procedures for creating, changing and safeguarding passwords are in place (S21)
62. Documentation of workforce members and role types who should be trained on password management (S21)
63. Documentation of the workforce members who were trained on password management (S21)
64. P&P related to security incidents(S22)
65. Documentation demonstrating security incident P&P are implemented (S22)
66. Documentation of responding to, reporting, and mitigating security incidents (S23)
67. P&P related to formal contingency plan (S24)

68. Documentation demonstrating that a contingency plan is implemented (S24)
69. P&P related to data back-up plans (S25)
70. Documentation demonstrating how data is backed up (S25)
71. Documentation demonstrating data backup and restoration tests (S25)
72. Documentation related to a disaster recovery plan (S26)
73. Procedures for restoring lost data (S26)
74. Documentation of data restore tests and test results (S26)
75. Procedures related to an emergency mode operation plan (S27)
76. Documentation demonstrating business continuity while in emergency mode (S27)
77. P&P related to periodic testing and revision of contingency plans (S28)
78. Documentation demonstrating the revision of contingency plans (S28)
79. Documentation of contingency plan tests and related results (S28)
80. Documentation of critical ePHI applications and their assigned criticality levels (S29)
81. Documentation of the procedures regarding how ePHI applications (data applications that store, maintain or transmit ePHI) are identified (S29)
82. Documentation of P&P related to technical and nontechnical evaluation (S30)
83. Documentation demonstrating periodic technical and non-technical evaluations (S30)
84. Documentation of procedures for technology change control/management and documentation of major technology changes which affected the security of ePHI (S30)
85. Documentation of plans related to risk management or mitigation efforts in response to evaluations conducted due to a major technology change which affected the security of ePHI (S30)
86. Documentation identifying all business associates (S30)
87. BAA and/or contracts (S30)
88. This inquiry is for BAs only]: Determine whether the BA contract identifies if it utilizes any subcontractors and review the BAA (S30)
89. Documentation of all BAs (S32)
90. Written agreements or other arrangements (i.e., a MOU if the CE and BA are government agencies) (S32)
91. This inquiry is for BAs only: Written contract or other arrangement identifies if there are any subs, if so review the written contract or other arrangement (S32)
92. P&P regarding facility access control (S33)
93. Documentation of workforce members with authorized physical access to electronic information systems and the facility or facilities in which they are housed (S33)
94. Documentation of procedures for granting individuals access to entity facility or facilities where electronic information systems are housed (S33)
95. Documentation of visitor physical access to electronic information systems and the facility or facilities where it is housed (S33)
96. Contingency operations procedures (S34)
97. Documentation demonstrating contingency operation procedures currently implemented (S34)
98. Documentation demonstrating that contingency operation procedures are tested (S34)
99. P&P related to the facility security plan (S35)

100. Documentation demonstrating that facility security plan procedures are implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft (S35)
101. Procedures related to access control and validation documentation demonstrating the control of visitor's physical access to facilities (S36)
102. Documentation demonstrating control of access to software program for modification and revision (S36)
103. Documentation demonstrating facility and software access control and validation procedures are implemented (S36)
104. P&P related to maintaining maintenance records (S37)
105. Documentation demonstrating records of repairs and mods to physical security components (S37)
106. P&P related to workstation use (S38)
107. Procedures related to the proper use and performance of workstations (S38)
108. Inventory of the locations and types of workstations (S38)
109. Documentation demonstrating workstation classification (S38)
110. Documentation demonstrating workstation use policies and procedures implemented (S38)
111. P&P related to workstation security (S39)
112. Documentation demonstrating workstation security P&P being implemented (S39)
113. P&P related to device and media controls (S40)
114. Documentation demonstrating the movement of hardware and electronic media containing ePHI into, out of and within the facility (S40)
115. Documentation demonstrating the type of security controls implemented for the facility in, out, and within movements of workforce members' assigned hardware and electronic media that contain ePHI (S40)
116. P&P related to disposal of any electronic media that stores ePHI (S41)
117. Documentation demonstrating how the disposal of hardware, software, and ePHI data is completed, managed, and documented (S41)
118. Documentation demonstrating how the sanitization of electronic media is completed, managed, and documented (S41)
119. Procedures related to media re-usage (S42)
120. Documentation demonstrating media re-use procedures being implemented and how ePHI has been removed from electronic media (S42)
121. P&P related to device and media accountability (S43)
122. Documentation demonstrating a record of movements of hardware and electronic media and person responsible therefore (S43)
123. P&P related to data backup and storage procedures (S44)
124. Documentation demonstrating how ePHI data is backed up for equipment being moved to another location (S44)
125. Documentation demonstrating how ePHI data backups for moved equipment are stored (S44)
126. Documentation demonstrating the restoration of ePHI data backups for moved equipment (S44)

127. P&P related to access control (S45)
128. Demonstrating the implementation of access controls for electronic information systems that maintain ePHI (S45)
129. Documentation demonstrating a list of new workforce members from the electronic information system who was granted access to ePHI (S45)
130. Documentation demonstrating the access levels granted to new workforce members (S45)
131. Documentation of a list of users with privileged access (S45)
132. List of default, generic/shared, and service accounts from the electronic information systems with access to ePHI (S45)
133. Documentation demonstrating the access levels granted to default, generic/shared, and service accounts (S45)
134. Documentation demonstrating that periodic reviews of procedures related to access controls have been conducted (S45)
135. Documentation demonstrating a list of terminations and job transfers (S45)
136. Documentation demonstrating the removal or modification of user access levels (S45)
137. P&P regarding the assignment of unique user IDs (S46)
138. Documentation demonstrating the assignment, creation, and use of unique user IDs (S46)
139. Procedures in place to provide necessary access to ePHI during an emergency (S47)
140. Documentation demonstrating a list of workforce members with authority to initiate the emergency access procedures (S47)
141. Documentation demonstrating technical systems limiting emergency access initiation (S47)
142. P&P regarding automatic logoff (S48)
143. Documentation (e.g., screenshots, system settings, etc.) demonstrating the implementation of automatic logoff (S48)
144. P&P regarding the encryption and decryption of ePHI (S49)
145. Documentation demonstrating ePHI being encrypted and decrypted (S49)
146. Documentation relative to audit controls (S50)
147. Documentation demonstrating the implementation of hardware, software and/or procedural mechanisms to record and examine activity (S50)
148. P&Ps regarding the implementation of integrity controls to protect ePHI (S51)
149. Documentation demonstrating processes in place to protect ePHI from improper alteration or destruction (S51)
150. P&P for authenticating ePHI (electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner) (S52)
151. Documentation demonstrating that electronic mechanisms are implemented to authenticate ePHI (Mechanisms to determine that appropriately corroborate that ePHI has not been altered or destroyed in an unauthorized manner) (S52)
152. P&P regarding person or entity authentication (able to verify that a person or entity seeking access to ePHI is the one claimed) (S53)
153. Documentation demonstrating the implementation of authentication procedures for persons or entities seeking access to ePHI (S53)
154. P&P related to transmission security controls (S54)

155. Identify the various methods, devices, and networks used to electronically transmit ePHI (S54)
156. Identify the technical security controls implemented to guard against unauthorized access to ePHI transmitted over electronic communication networks (S54)
157. Documentation demonstrating the implementation of technical security measures to protect electronic transmissions of ePHI (S54)
158. P&P related to transmission security measures (S55)
159. Documentation demonstrating the implementation of security measures to protect electronic transmissions of ePHI (S55)
160. P&P regarding the encryption of electronically transmitted ePHI (does the entity have encryption mechanism to encrypt ePHI whenever deemed?) (S56)
161. Documentation demonstrating the encrypted mechanism is implemented to encrypt ePHI (S56)
162. Documentation demonstrating that electronically transmitted ePHI is encrypted (S56)
163. P&P in place regarding its contractual arrangements with contractors or other entities to which it discloses ePHI for use on its behalf (S57)
164. The entity's standard business associate contract template(s) (S57)
165. Documentation demonstrating the entity's approval process when deviations affecting the implementation of safeguards (by the BA?) to protect ePHI are considered (S57)
166. Obtain BA contracts (S58)(S59)(S60)
167. Documentation demonstrating that the entity's business associates have reported security incidents of which it was aware, including breaches of unsecured PHI (S60)
168. P&P in place regarding other arrangements to have in place (e.g., a MOU if the CE and BA are government agencies) (S61)
169. Documentation of the entity's other arrangements with BAs (S61)
170. BA contracts entered into with subcontractors (S62)
171. P&P in place to ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan (S63)
172. Review plan documents (S63)
173. Review plan documentation (language that requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan) (S64)
174. Health plan documentation (ensure adequate separation between the group health plan and the plan sponsor) (S65)
175. Health plan documentation (incorporate provisions that requires the sponsors to ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures) (S66)
176. Health plan documentation (language that requires plan sponsors to report to the group health plan any security incident of which it becomes aware) (S67)
177. Documentation of the policies and procedures regarding the implementation of compliant P&P (S68)
178. P&P regarding the maintenance of P&P (S69)

179. Documentation demonstrating that P&P are being maintained (S69)
180. Written documentation demonstrating the entity's action, activity or assessment that is required by the Security Rule (S69)
181. Documentation of P&P for compliance with retention requirements (S70)
182. Documentation demonstrating that P&P are being maintained for six (6) years from the date of its creation or the date when it last was in effect (S70)
183. Documentation demonstrating that an action, activity, or assessment is being maintained for six (6) years from the date of its creation or the date when it last was in effect (S70)
184. Documentation of P&P regarding the availability of documentation (S71)
185. Documentation demonstrating that Security Rule P&P are made available to the workforce members responsible for implementing the pertaining procedures (S71)
186. P&P regarding documentation reviews and updates to security P&P (S72)
187. Documents demonstrating that P&P are reviewed and updated on a periodic basis (S72)