Department of Health and Human Services, Office for Civil Rights

HIPAA AUDIT PROTOCOL

Agency Name:
Agency Address:
Date:
Chief Compliance/Privacy Officer:
Phone Number:
E-mail address:

#s	Section	Audit Procedures	Yes	No	NI
		Breach			
1	§164.402	Does a risk assessment process exists to determine significant harm in a breach?			
2	§164.404	Does a process exists for notifying individuals within the required time period?			
3	§164.404	Is there a process that exists for notifying an individual or an individual's next of kin of a breach?			
4	§164.404	Is there a standard template or form letter for breach notification?			
5	§164.406	Does a process exists for notifying media outlets for breaches of more than 500 individuals' PHI and compare it to established performance criteria?			
6	§164.408	Has there been any breaches of unsecured PHI and was the Secretary notified?			
7	§164.410	Have there have been any breaches of unsecured PHI for a business associate and verify that the covered entity was notified?			
8	§164.412	How are notifications delayed in case of law enforcement requests?			
9	§164.414	Does a risk assessment process exists to determine significant harm in a breach? Does a process exists to ensure that all notifications were made as required or that the impermissible use or disclosure did not constitute a breach?			
		Privacy			
10	§164.502	Are requirements with respect to PHI of a deceased person met?			
11	§164.502	Are requirements with respect to personal representatives met?			
12	§164.502	Are uses and disclosures consistent with notice?			
13	§164.502	Does a process exists to permit disclosures of PHI by whistleblowers and the conditions under which whistleblowers may disclose PHI?			
14	§164.502	Does a process exists to permit certain disclosures of PHI by workforce members who are victims of a crime and the conditions under which they may disclose PHI?			
15	§164.502	Does a process exists to ensure the entity complies with confidential communication requirements?			
16	§164.504	Does a business associate contract permit the use and disclosure of PHI for the proper management and administration of the business associate?			
17	§164.504	Do the plan documents restrict the use and disclosure of PHI by the plan sponsor?			
18	§164.504	Does the entity have multiple functions and if so, is the use and disclosure of PHI only for the purpose related to the appropriate function being performed?			
19	§164.506	Does a process exists for the use or disclosure of PHI for treatment, payment, or health care operations provided and is such use or disclosure consistent with other applicable requirements?			
20	§164.506	Has your entity determined that obtaining the individual's consent is necessary?			
21	§164.508	Does a process exists to determine when authorization is required?			
22	§164.508	Do formal or informal policies and procedures exist for obtaining a valid authorization?			
23	§164.508	Does your entity use or disclose PHI for the purpose of research, provide research and/or psychotherapy services, or use compound authorizations? Specify whether PHI being disclosed pursuant to an authorization is a psychotherapy note?			
24	§164.508	When can the entity condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits?			
25	§164.510	Does a process exists for disclosing only information relevant to the person's involvement with the individual's health care?			
26	§164.510	Does your entity maintain a directory of individuals in its facility?			
27	§164.510	Does a process exists to use or disclose PHI for the facility directory due to an emergency treatment?			
28	§164.510	What is the process for disclosing PHI to family members, relatives, close personal friends or other persons identified by the individual?			
29	§164.510	How does your entity disclose PHI to persons involved in the individual's care when the individual is present, and can it disclose PHI with the individual present?			
30	§164.510	Does a process exists for disclosing PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts?			
31	§164.510	Are there objections by individuals to restrict or prohibit some or all of the uses or disclosures that are obtained and maintained?			
32	§164.512	Does a process exists to determine if the disclosure of PHI in the course or any judicial or administrative proceeding is appropriate?			
33	§164.512	Do procedures exist to use PHI for research?			
34	§164.512	Does a process exist to determine what documentation of approval or waiver is needed to permit a use or disclosure?			

35	§164.512	Are your requirements to use or disclose PHI required by law, met?			
36	§164.512	Is there a process in place specifying public health activities for which the entity may disclose PHI?			
37	§164.512	Specify whether disclosure about victims of abuse, neglect, or domestic violence are permitted? Is a process in place to inform the individual that a disclosure has been or will be made?			
38	§164.512	Is PHI disclosed to the appropriate health oversight agency?			
39	§164.512	Are your conditions for disclosure of PHI to a law enforcement official appropriate?			
40	§164.512	Specify whether the response to a law enforcement official's request is limited to information for identification and location purposes?			
41	§164.512	Specify whether conditions in which your entity may disclose PHI in response to a law enforcement official's request are met prior to disclosure.			
42	§164.512	Is a process in place to determine when it is permitted to disclose PHI about an individual who has died to a law enforcement official?			
43	§164.512	Is a process in place to determine what information about a medical emergency is necessary to disclose to alert law enforcement?			
44	§164.512	Is the process for disclosing PHI to a coroner or medical examiner appropriate?			
45	§164.512	Is the process for disclosing PHI to organ procurement organizations or other entities engaged in the procurement is appropriate?			
46	§164.512	Is a process in place to determine which government functions your entity is permitted to disclose PHI?			
47	§164.512	Is a process in place to determine why PHI is disclosed to authorized federal officials?			
48	§164.512	Is a process in place to determine for what protective services your entity is permitted to disclose PHI?			
49	§164.512	Is a process in place to determine the purpose for disclosing PHI to the Department of State (DOS)?			
50	§164.512	Is a process in place to determine if the disclosure of PHI to a correctional institution or law enforcement official is necessary?			
51	§164.512	Is a process in place to determine the need to disclose PHI for the purpose of workers' compensation?			
52	§164.514	Is access to PHI restricted?			
53	§164.514	Are policies and procedures in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of disclosure?			
54	§164.514	Specify whether the disclosure of PHI to a business associate or institutionally related foundation, is limited to demographic information relating to an individual; and the dates when health care was provided to an individual.			
55	§164.514	Are there procedures in place restricting the health plan's uses and/or disclosures of PHI for underwriting purposes, or for any other purpose except as may be required by law?			
56	§164.514	Are formal or informal policies and procedures are in place to verify the identity of individuals who request PHI?			
57	§164.514	Are data use agreements in place between the covered entity and its limited data set recipients?			
58	§164.514	Are policies and procedures in place to terminate data use agreements if the agreement is violated?			
59	§164.514	Specify whether a process to re-identify PHI exists. (Optional)			
60	§164.514	A covered entity may de-identify PHI; however they are not required to. If a covered entity does de-identify PHI, does a process to de-identify PHI exists?			
61	§164.520	Are individuals notified of the potential uses and disclosures of PHI by the covered entity?			
62	§164.520	Specific requirements for health plans: Inquire of management as to how the covered entity the notice to any person upon request.			
63	§164.520	Specific requirements for certain covered health care providers: Inquire of management as to how the covered entity the notice to any person upon request.			
64	§164.520	Specific requirements for electronic notice: If the covered entity provides electronic notice, obtain and review the policies and procedures regarding the provision of the NOPP by email and the process by which an individual can withdraw their request for receipt of electronic notice.			
65	§164.520	Covered entities that participate in organized health care arrangements: Inquire of management as to whether a joint notice of privacy practices meets the minimum requirements set forth by the HIPAA Privacy Standards.			
66	§164.520	Confirm that documentation of privacy practices must be maintained in electronic or written form and retained for a period of six years.			
67	§164.522	Are individuals permitted to request alternative means or alternative locations to receive communications of PHI?			
68	§164.522	Is there a process in place to terminate restrictions of the use and/or disclosure of PHI?			
69	§164.522	Specify whether documentation of restrictions is maintained in electronic or written form and retained for a period of six years.			
70	§164.522	Is there a process in place to permit an individual to request that the entity restrict uses or disclosures of PHI?			
71	§164.524	Specify how an individual can access PHI.			
72	§164.524	Is there a process to facilitate review of denial of access to PHI?			
73	§164.524	Are unreviewable denied requests for access properly documented?			
74	§164.524	Are policies and procedures in place to have the denial of access reviewed?			
75	§164.524	Does a process of document retention for amendments to PHI exist?			
76	§164.526	Does a policy exist regarding an individual's right to amend their PHI in a designated record set?			
77	§164.526	Are grounds for denying requests for amendment are documented?			
78	§164.526	Specify whether requirements the entity must comply with are documented if a request for amendment is accepted.			
79	§164.526	Are the requirements the entity must comply with documented if a request for amendment is denied?			
80	§164.528	Do policies and procedures exist for an accounting of disclosures of PHI?			
81	§164.528	Does the content of the accounting of disclosures meet the minimum requirements set forth in the HIPAA Privacy Standards?			
82	§164.528	Do policies and procedures exist to provide the individual with the requested accounting of PHI?			

83	§164.528	How are the accounting of disclosures documented and retained?			
84	§164.530	Is training provided to the agency's work force on HIPAA Privacy Standards?			
85	§164.530	Do formal or informal policies and procedures exist for receiving and processing complaints over the agency's privacy practices?			
86	§164.530	Do sanctions exist against members of the covered agency's workforce who fail to comply with the privacy policies and procedures?			
87	§164.530	Are policies and procedures with respect to PHI, in place that are designed to comply with the standards, implementation specifications and other requirements of the HIPAA Privacy Standards?			
88	§164.530	Are administrative, technical and physical safeguards in place to protect all PHI?			
89	§164.530	Does the agency mitigate any harmful effect that is known to the agency of a use or disclosure of PHI by the agency or its business associates, in violation of its policies and procedures?			
90	§164.530	Do policies and procedures exist preventing intimidating or retaliatory actions against any individual for the exercise by the individual of any right established, or for participation in any process provided, for filing complaints against the agency?			
91		Does the agency have training documentation for employees over Privacy Practices and agency training policy(s)?			
92		Does the agency clearly identify to employees who the Chief Compliance Officer/Privacy Officer is?			
		Security			
93	§164.308	Do formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI?			
94	§164.308	Do formal or informal policy and procedures exist covering the specific features of the HIPAA Security Rule information systems §164.306(a) and (b)?			
95	§164.308	Do formal or informal policy and procedures exist to review information system activities; such as audit logs, access reports, and security incident tracking reports?			
96	§164.308	Are current security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)?			
97	§164.308	Specify whether the organization has assigned responsibility for the HIPAA security to a Security Official to oversee the development, implementation, monitoring, and communication of security policies and procedures.			
98	§164.308	Are the roles and responsibilities of the assigned individual or organization properly documented in a job description and communicated to the entire organization?			
99	§164.308	Specify whether the level of authorization and/or supervision of workforce members has been established.			
100	§164.308	Is a formal document in place identifying levels of access to information systems that houses ePHI?			
101	§164.308	Do staff members have the necessary knowledge, skills, and abilities to fulfill particular roles?			
102	§164.308	Do procedures exist for granting access to ePHI?			
103	§164.308	Are there separate procedures for terminating access to ePHI when the employment of a workforce member ends, i.e., voluntary termination (retirement, promotion, transfer, change of employment) vs. involuntary termination (termination for cause, reduction in force, involuntary transfer)? Inquire of management as to whether a standard set of procedures are in place to recover access control devices and deactivate computer access upon termination of employment.			
104	§164.308	Are policies and procedures in place to grant access to ePHI?			
105	§164.308	Do policies and standards exist to authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process?			
106	§164.308	Are policy and procedures for access consistent with the HIPAA Security Rule?			
107	§164.308	Specify whether formal or informal policies and procedures exist relating to the security measures for access controls.			
108	§164.308	Do security awareness and training programs address the specific required HIPAA policies?			
109	§164.308	Do security awareness and training programs outline the scope of the program?			
110	§164.308	Do formal or informal policy and procedures exist to inform employees of the importance of protecting against malicious software and exploitation of vulnerabilities?			
111	§164.308	Do training materials incorporate relevant current IT security topics?			
112	§164.308	Do employees receive all required training?			
113	§164.308	Are security policies and procedures updated periodically?			
114	§164.308	Is training conducted whenever there are changes in the technology and practices?			
115	§164.308	Are there formal or informal policies and/or procedures in place for identifying, responding to, reporting, and mitigating security incidents?			
116	§164.308	Do policy or procedures exist regarding identifying, documenting, and retaining a record of security incidents?			
117	§164.308	Does a formal contingency plan with defined objectives exists? Inquire of management as to the process in place for identifying critical applications, data, operations, and manual and automated processes involving ePHI.			
118	§164.308	Do disaster recovery and data backup plans exist to restore any lost data?			
119	§164.308	Do policy and procedures exist to enable the continuation of critical business processes that protect the security of ePHI while operating in emergency mode?			
120	§164.308	Do policy and procedures exist for periodic testing and revision of contingency plans?			
121	§164.308	How are preventive measures identified and deemed practical and feasible in the organization's given environment?			
122	§164.308	Do procedures exist for recovering documents from emergency or disastrous events?			
123	§164.308	Does a procedure exist to create and maintain exact copies of ePHI?			
124	§164.308	Are evaluations conducted by internal staff or external consultants. For evaluations conducted by external consultants, determine if an agreement or contract exists and if it includes verification of consultants' credentials and experience. For evaluations conducted by internal staff, determine if the documentation covers elements from the specified performance criteria.			

125	§164.308	Do policy and procedures exist to ensure an evaluation considers all elements of the HIPAA Security Rule.			
126	§164.308	Do policy and procedures exist to ensure all necessary information needed to conduct an evaluation is obtained and documented in advance.			
127	§164.308	Do formal or informal policy and procedures exist to document the evaluation of findings, remediation options and recommendations, and remediation decisions.			
128	§164.308	Do formal or informal security policies and procedures specify that evaluations will be repeated when environmental and operational changes are made that affect the security of ePHI?			
129	§164.308	Does a process exists to ensure contracts or agreements include security requirements to address confidentiality, integrity, and availability of ePHI?			
130	§164.308	Does a process exists to identify federal, state, or local government business associates?			
131	§164.310	Do formal or informal policies and procedures exist regarding access to and use of facilities and equipment that house ePHI?			
132	§164.310	Do formal or informal policies and procedures exist to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft.?			
133	§164.310	Do procedures exist for controlling access by staff, contractors, visitors, and probationary employees?			
134	§164.310	Do formal or informal documentation exists that allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency?			
135	§164.310	Do policies and procedures exist to document repairs and modifications to the physical components of a facility that are related to security?			
136	§164.310	Does a process exists for identifying workstations by type and location?			
137	§164.310	Do formal or informal policies and procedures exist related to the proper use and performance of workstations?			
138	§164.310	Do formal or informal policies and procedures exist to prevent or preclude unauthorized access to an unattended workstation, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed?			
139	§164.310	How are workstations physically restricted to limit access to only authorized personnel?			
140	§164.310	What physical security measures are in place to prevent unauthorized access to restricted information?			
141	§164.310	How is the disposal of hardware, software, and ePHI data managed?			
142	§164.310	How is the location and movement of media and hardware containing ePHI tracked?			
143	§164.310	What are the procedures established over the backup and restoration of ePHI data?			
144	§164.310	What are the processes established to remove ePHI before reusing electronic media and who is responsible for overseeing those processes?			
145	§164.312	Is there an encryption mechanism in place to protect ePHI?			
146	§164.312	How are the workloads and operations analyzed to determine the access needs of all users within the entity?			
147	§164.312	How are technical access control capabilities defined?			
148	§164.312	How are users assigned unique user IDs?			
149	§164.312	Is there an access control policy in place?			
150	§164.312	What access control procedures are in place?			
151	§164.312	How are generic and system IDs implemented?			
152	§164.312	Who has access to add, modify, or delete user access?			
153	§164.312	Are user access to systems and applications reviewed on a periodic basis?			
154	§164.312	Is an emergency access procedure in place for obtaining necessary ePHI during an emergency?			
155	§164.312	whether and how access to initiate the emergency access process is limited to appropriate personnel.			
156	§164.312	Does an automatic logoff occur after a predetermined time of inactivity?			
157	§164.312	How is user access removed upon termination or change of position on a timely basis?			
158	§164.312	Have audit controls been implemented over information systems that contain or use ePHI?			
159	§164.312	Have systems and applications been evaluated to determine whether upgrades are necessary to implement audit capabilities?			
160	§164.312	Does a formal or informal audit policy is in place to communicate the details of the entity's audits and reviews to the work force?			
161	§164.312	Are procedures in place on the systems and applications to be audited and how they will be audited?			
162	§164.312	Have all users who should have access to ePHI, been identified?			
163	§164.312	Are access control procedures in place?			
164	§164.312	Are electronic mechanisms in place to authenticate ePHI?			
165	§164.312	What are the authentication methods that have been identified for the entity's systems and applications?			
166	§164.312	Have authentication methods been evaluated for the entity's systems and applications to assess strengths and weaknesses and the cost to benefit ratio of different types of authentication in order to establish an appropriate level of authentication?			
167	§164.312	Is there a formal authentication policy in place for the entity's systems and applications?			
168	§164.312	How is the authentication system periodically tested and upgraded when upgrades are available?			
169	§164.312	Inquire of management as to the formal ePHI data transmission policy in place for the entity.			