HIPAA Data Security Monitoring Tool

Provider Name:

Team Member:

Contract Number:

Post-Site QA Check (LastName/Date):

Date of Completion:

Date of Tool Revision:7/1/23

Requirements	Authority	JCAHO	CARF	COA	Source	Fully Met?
Applicability of HIPAA: These questions are not rated for compliance!						
Has the provider signed the Business Associate Agreement or is it in the contract? AND Does the provider safeguard, use, or disclose protected health information that is created, received, maintained, or transmitted by the provider or its subcontractors incidental to the contract?	Contract and Attachment (business associate agreement 2.1.2)					
If the provider has not signed the BA agreement, then does the provider transmit any health information related to the contract in electronic format? AND Does the provider define itself as required to comply with HIPAA in its policies and procedures, or does the contract otherwise say the provider must follow HIPAA?	HIPAA 164.104					
If the answer to either of the applicability questions is Yes, please answer remaining questions. Otherwise, STOP! HIPAA data security requirements are not clearly applicable.						
Associate Agreements						
Are there any business associates or subcontractors of the provider that create, receive, maintain, or transmit electronic PHI on the provider's behalf? (e.g., storage facility, parent organization, subcontractors).	Applicability question - not rated for compliance					
If yes, does the provider have copies of assurances or agreements on file stating that other parties with whom it shares client information will appropriately safeguard the information? Note 1: this does not apply to many types of information sharing including information shared for treatment purposes. Note 2: see subcontract tool for analysis of specific required elements of the agreements.	45 CFR 164.308(b)					
Other Administrative Requirements						
Does the provider have appropriate sanctions to take against members of the workforce who fail to comply with HIPAA data security policies, procedures, requirements?	45 CFR 164.308(a)(1)(ii)(C)					
Does the provider have an identified security official who is responsible for development and implementation of data security policies and procedures required by HIPAA?	45 CFR 164.308(a)(2)		1.C.12.b.			

HIPAA Data Security Monitoring Tool

Provider Name:

Contract Number:

Post-Site QA Check (LastName/Date):

Date of Tool Revision:7/1/23

Team Member:

Date of Completion:

Requirements	Authority	JCAHO	CARF	COA	Source	Fully Met?
Security Standards Providers are Permitted Flexibility of Approach under 45 CFR 164.306(b). Organizations may use any security measures that reasonably and appropriately implement the standards. **Required** Standards must be implemented. See 45 CFR 164.306(d)(2). **Addressable** Standards must be implemented if reasonable and appropriate. Or, provider must document why it is not reasonable and appropriate to implement, and must implement an equivalent alternative if reasonable and appropriate.						
Risk Analysis - Required. Did the provider conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the provider?	45 CFR 164.308(a)(1)(ii)(A)			RPM 2.01.h.		
Risk Management - Required. Did the provider implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?	45 CFR 164.308(a)(1)(ii)(B)					
Information System Activity Review - Required. Did the provider implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports?	45 CFR 164.308(a)(1)(ii)(D)					
Authorization and/or Supervision - Addressable. Did the provider implement procedures for the authorization and/or supervision of workforce members working with electronic PHI or in areas where electronic PHI could be accessed?	45 CFR 164.308(a)(3)(ii)(A)		1.C.12.c.	RPM 6.01.a.		
Workforce Clearance Procedure - Addressable. Did the provider implement procedures to determine that the access of a workforce member to electronic PHI is appropriate?	45 CFR 164.308(a)(3)(ii)(B)		1.C.12.c.	RPM 6.01.a.		
Termination Procedure - Addressable. Did the provider implement procedures for terminating access to electronic PHI when employment of a workforce member ends, or when responsibilities change as specified in the Workforce Clearance Procedure (see above)?	45 CFR 164.308(a)(3)(ii)(C)					
If the provider is a hybrid organization with distinct and separate healthcare information function, has the provider implemented policies and procedures that protect the PHI from unauthorized access by the larger organization? Required. See 45 CFR 164.105 for definitions.	45 CFR 164.308(a)(4)(ii)(A)					

HIPAA Data Security Monitoring Tool

Provider Name:

Team Member:

Contract Number:

Post-Site QA Check (LastName/Date):

Date of Completion:

Date of Tool Revision:7/1/23

Requirements	Authority	JCAHO	CARF	COA	Source	Fully Met?
Health Care Clearinghouse Access Policies - Addressable. **If the provider is a hybrid organization with distinct and separate healthcare information function,** has the provider implemented policies and procedures for granting access to PHI, and for establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process?	45 CFR 164.308(a)(4)(ii)(B) and (C)					
Security Awareness - Addressable. Has the provider implemented periodic security updates; procedures for guarding against, detecting, and reporting malicious software; procedures for monitoring log-in attempts and reporting discrepancies; and procedures for creating, changing, and safeguarding passwords?	45 CFR 164.308(a)(5)(ii)					
Security Incidents Response and Reporting - Required. Has the provider implemented policies and procedures to address security incidents, including identifying and responding to suspected or known security incidents, mitigating harmful effects of incidents, and documenting security incidents and outcomes?	45 CFR 164.308(a)(6)(ii)					
Data Backup Plan - Required. Has the provider implemented policies and procedures to create and maintain retrievable exact copies of electronic PHI?	45 CFR 164.308(a)(7)(ii)(A)	IM.2.30	1.C.12.e.	RPM 6.01.b.		
Disaster Recovery Plan - Required. Has the provider implemented policies and procedures to restore any loss of electronic PHI data?	45 CFR 164.308(a)(7)(ii)(B)	IM.2.30	1.C.8.a.(7)	RPM 6.01		
Emergency Mode Operation Plan - Required. Has the provider implemented policies and procedures to enable continuation of critical business processes for protection and security of electronic PHI while operating in emergency mode?	45 CFR 164.308(a)(7)(ii)(C)	IM.2.30				
Testing and Revision of Plans and Analysis of Applications - Addressable. Has the provider implemented procedures for periodic testing and revision of contingency plans? Has the provider assessed relative criticality of specific applications and data in support of other contingency plan operations?	45 CFR 164.308(a)(7)(ii)(D) and (E)	IM.2.30				
Contingency Operations - Addressable. Has the provider implemented procedures for allowing access to facility in support of data recovery under the disaster recovery and emergency management plan?	45 CFR 164.310(a)(2)(i)					

HIPAA Data Security Monitoring Tool

Provider Name:

Contract Number:

Post-Site QA Check (LastName/Date):

Team Member:

Date of Completion:

Date of Tool Revision:7/1/23

Requirements	Authority	JCAHO	CARF	COA	Source	Fully Met?
Facility Security Plan - Addressable. Has the provider implemented procedures to safeguard facility and equipment from unauthorized access, tampering, and theft?	45 CFR 164.310(a)(2)(ii)		1.C.12.d.			
Facility Access Control and Validation - Addressable. Has the provider implemented procedures for control and validation of access to facilities and/or to software?	45 CFR 164.310(a)(2)(iii)					
Maintenance Records - Addressable. Has the provider implemented procedures for documenting repairs and modifications to physical components of facility related to security?	45 CFR 164.310(a)(2)(iv)					
Workstation Use - Required. Has the provider implemented policies and procedures that specify proper functions to be performed, the manner in which functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI?	45 CFR 164.310(b)					
Workstation Security - Required. Has the provider implemented physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users?	45 CFR 164.310(c)					
Disposal of Media and Devices - Required. Has the provider implemented policies and procedures to address final disposition of electronic PHI and/or the hardware or electronic media on which it is stored?	45 CFR 164.310(d)(2)(i)					
Media Re-use - Required. Has the provider implemented policies and procedures to address removal of electronic PHI from electronic media before the media are made available for reuse?	45 CFR 164.310(d)(2)(ii)					
Accountability for Media - Addressable. Does the provider maintain a record of the movements of hardware and electronic media and any person responsible therefore?	45 CFR 164.310(d)(2)(iii)					
Data Backup and Storage - Addressable. Does the provider create a retrievable, exact copy of electronic PHI, when needed, prior to movement of equipment?	45 CFR 164.310(d)(2)(iv)					
Unique User Identification - Required. Does the provider assign a unique name and/or number for identifying and tracking user identity?	45 CFR 164.312(a)(2)(i)					
Emergency Access Procedure - Required. Has the provider established and implemented as needed procedures for obtaining electronic PHI during an emergency?	45 CFR 164.312(a)(2)(ii)	IM.2.30				

HIPAA Data Security Monitoring Tool

Provider Name:

Contract Number:

Post-Site QA Check (LastName/Date):

Team Member:

Date of Completion:

Date of Tool Revision:7/1/23

Requirements	Authority	JCAHO	CARF	COA	Source	Fully Met?
Automatic Logoff - Addressable. Has the provider implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity?	45 CFR 164.312(a)(2)(iii)					
Encryption and Decryption - Addressable. Has the provider implemented a mechanism to encrypt and decrypt electronic PHI?	45 CFR 164.312(a)(2)(iv)					
Audit Controls - Required. Has the provider implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain and use PHI?	45 CFR 164.312(b)					
Mechanism to Authenticate Protected Health Information - Addressable. Has the provider implemented electronic mechanisms to corroborate that PHI has not been altered or destroyed in an unauthorized manner?	45 CFR 164.312(c)(2)	IM.2.20				
Person or Entity Authentication - Required. Has the provider implemented procedures to verify that a person or entity seeking access to electronic PHI is the one claimed?	45 CFR 164.312(d)					
Integrity Controls - Addressable. Has the provider implemented security measures to ensure electronic PHI is not improperly modified without detection until disposed of?	45 CFR 164.312(e)(2)(i)					
Encryption - Addressable. Has the provider implemented electronic mechanisms to encrypt electronic PHI whenever deemed appropriate?	45 CFR 164.312(e)(2)(ii)					