HIPAA Security Risk Assessment

Purpose:

This self-assessment risk analysis questionnaire is intended to help evaluate the organization's current procedures and identify the organization's gaps in HIPAA Security Rule compliance and provide suggested policies and procedures to mitigate the gaps. The questionnaire focuses on the requirements put forth in the administrative, physical and technical safeguards and specifications of the HIPAA Security Rule.

Instructions:

Please answer each of the questions. Providing accurate answers may require some research and interaction with other departments, but it will help produce a high quality assessment. In the questions that follow, check the box that most accurately represents the organization's current situation. Once all of the questions have been answered, you will have the necessary list of required policies and procedures as well as suggestions for mitigating and documenting HIPAA Security Rule compliance. You may print this document or save it to review later and track your progress towards compliance.

> **Yes** – You currently have security measures in place that address the standard
> **No** – The organization does not currently have security measures in place
> **N/A** – The security measure does not apply to the organization's situation, or can be met through an alternative measure. This must be thoroughly documented.

HIPAA Security Risk Analysis (1 of 2)

	HIPAA Security Risk Analysis Questionnaire	Yes	No	N/A
Administrative Safeguards				
1	Has the organization designated a Security Officer, to be responsible for the development and implementation of the policies and procedures?	o	o	
2	Has the organization developed a job description for the Security Officer?	o	o	
3	Does the organization have a policy and procedure to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the organization?	o	o	
4	Has the organization implemented procedures to review information system activity such as audit logs and access reports on a regular basis?	o	o	o
5	Does the organization have policy and procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed? For example, contractors, who must work in areas where PHI resides, would either be authorized for such "exposure" or supervised by someone who is authorized.	o	o	o
6	Does the organization have policies and procedures to determine that the access of a workforce member to electronic PHI is appropriate?	o	o	o
7	Does the organization have policies and procedures for terminating access to electronic PHI when the employment of a workforce member ends or when the clearance procedures determine that a change in a worker's access privileges is appropriate? It includes such steps as changing combinations or turning in keys, tokens or cards; deactivation of user identification and passwords, and/or removal from access lists; and any other appropriate steps to terminate or alter a user's access to PHI.	o	o	o
8	Has the organization developed policies and procedures to protect its electronic PHI from unauthorized access by persons from the non-covered entity?	o	o	
9	Does the organization have security awareness and training programs for all members of the workforce who access ePHI?	o	o	o
10	Does the organization have policies and procedures for guarding against, detecting and reporting malicious software such as viruses and worms?	o	o	o
11	Does the organization have policies and procedures for monitoring system and application login attempts and reporting discrepancies?	o	o	o
12	Does the organization have policies and procedures in place to identify and respond to suspected or known security incidents; and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes?	o	o	
13	Does the organization have policies and procedures to create and maintain retrievable exact copies of electronic PHI and, if necessary, to restore any loss of data?	o	o	
14	Does the organization have policies and procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode?	o	o	
15	Does the organization have policies and procedures for periodic testing and revision of contingency plans?	o	o	o
16	Has the organization performed a technical and non-technical evaluation that establishes the extent to which the organization's security policies and procedures meet the requirement of the Security Rule?	o	o	
17	Does the organization have written assurances from its vendors, who create, receive, transmit or maintain ePHI on the organization's behalf, and the vendors' subcontractors to implement administrative physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information (PHI) that it creates, receives, maintains, or transmits on behalf of the organization?	o	o	

HIPAA Security Risk Analysis (2 of 2)

HIPAA Security Risk Analysis Questionnaire		Yes	No	N/A
Physical Safeguards				
1	Does the organization have 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 properly authorized access is allowed?	o	o	o
2	Does the organization have policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?	o	o	o
3	Does the organization have policies and procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control and control of access to software programs?	o	o	o
4	Does the organization have policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security?	o	o	o
5	Does the organization have 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 electronic protected health information (PHI)?	o	o	
6	Does the organization have physical safeguards for all workstations that access electronic PHI, in order to restrict access to authorized users?	o	o	
7	Does the organization have policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored once the workstation has been reassigned or taken out of service?	o	o	
8	Does the organization maintain a record of the movements of hardware and electronic media and any person responsible for them?	o	o	
9	Does the organization have a policy and procedure to create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment?	o	o	o

HIPAA Security Risk Analysis Questionnaire		Yes	No	N/A
Technical Safeguards				
1	Do all users have unique usernames and/or numbers for identifying and tracking user identity for each application that creates, maintains, receives or transmits electronic PHI?	o	o	
2	Does the organization have policies and procedures for obtaining necessary electronic PHI during an emergency?	o	o	
3	Are electronic sessions on workstations terminated after a predetermined time of inactivity?	o	o	o
4	Do you have a mechanism to encrypt and decrypt electronic PHI that is being maintained on your servers and workstation? (Note that this applies to electronic PHI that is at rest and NOT being transmitted)	o	o	o
5	Does the organization have hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI?	o	o	
6	Does the organization have policies, procedures, and mechanisms to protect electronic PHI from improper alteration or destruction? (Often operating systems have integrity already built in that you may not be aware of, such as error-correcting memory and magnetic disc storage, which are ubiquitous in hardware and operating systems today. Most software already employs such integrity standards, and if the organization utilizes such software exclusively to alter or delete electronic PHI, it would meet this standard.)	o	o	o
7	Has the organization implemented policies and procedures to verify that a person or entity seeking access to electronic PHI is the one claimed?	o	o	
8	Does the organization have security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of?	o	o	o
9	Does the organization have a mechanism to encrypt electronic PHI whenever deemed appropriate?	o	o	o