HIPAA/HITECH PRIVACY & SECURITY CHECKLIST
SELF ASSESSMENT INSTRUCTIONS

Thank you for taking the time to fill out the privacy & security checklist. Once completed, this checklist will help us get a better understanding of where we can better assist you. Below you will find some acronyms that are shown throughout the checklist as well as some brief instructions for completing the assessment.

Acronyms

NIST	National Institute of Standards and Technology
FIPS	Federal Information Process Standards
PHI	Protected Health Information
EPHI	Electronic Protected Health Information
BA	Business Associate
CE	Covered Entity
EHR	Electronic Health Record
HHS	Health and Human Services
IS	Information System

Instructions

HIPAA SECURITY RULE - ADMINISTRATIVE SAFEGUARDS (R) = REQUIRED, (A) = ADDRESSABLE		
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed in accordance with NIST Guidelines? (R)	

1 - The HIPAA Security Rule specifies a list of required or addressable safeguards. If an (R) is shown after the safeguard then implementation of that safeguard is required. If an (A) is shown then the safeguard must be assessed to whether or not it is reasonable and appropriate safeguard in your environment. If not implemented, then it's required to document the reason why and also implement an equivalent alternative safeguard if reasonable and appropriate.
2 – The reference refers to the C.F.R. (Code of Federal Regulations) that maps to the requirement or safeguard to the specific regulation.
3 – This field is the requirement or safeguard that is being evaluated. If shown in bold, then specifying a status for that particular is not necessary since it's an overview of the following rows to be evaluated.
4 – For any of the highlighted fields, a status is not required since that row is just an overview of the following rows to be evaluated.
5 – This field is to specify the status of the requirement or safeguard. Please specify the following: N/A, Complete, In Progress, Not Complete, or Unknown. Please feel free to add any additional comments to the field or on a separate sheet of paper.

HIPAA/HITECH PRIVACY & SECURITY CHECKLIST
SELF ASSESSMENT

HIPAA/HITECH REFERENCE	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	STATUS N/A, COMPLETE, IN PROGRESS, NOT COMPLETE, UNKNOWN
	HIPAA PRIVACY RULE	
§164.502 §164.514	Develop "minimum necessary" policies for: - Uses - Routine disclosures - Non-routine disclosures - Limit request to minimum necessary - Ability to rely on request for minimum necessary	
§164.504	Develop polices for business associate (BA) relationships and amend business associate contracts or agreements: - Obtain satisfactory assurances in contract - Document sanctions for non-compliance	
§164.502 §164.504 §164.506 §164.508 §164.510 §164.512	Limit disclosures to those that are authorized by the client, or that are required or allowed by the privacy regulations and state law.	
§164.520	Develop and disseminate notice of privacy practice	
§164.522	Develop policies for alternative means of communication request.	
§164.524	Develop policies for access to designated record set: - Providing access - Denying access	
§164.526	Develop policies for amendment requests: - Accepting an amendment - Denying an amendment - Actions on notice of an amendment - Documentation	
§164.528	Develop policies for accounting of disclosures.	
§164.530	Implementation of Privacy Rule Administrative requirements, including: - Appoint a HIPAA privacy officer. - Training of workforce - Sanctions for non-compliance - Develop complaint policies.	

	- Develop anti-retaliation policies. - Policies and Procedures	
HIPAA SECURITY RULE - ADMINISTRATIVE SAFEGUARDS (R) = REQUIRED, (A) = ADDRESSABLE		
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed in accordance with NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the Risk Management process been completed in accordance with NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)	
164.308(a)(2)	Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. (R)	
164.308(a)(3)(i)	**Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).**	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine that the Access of an employee to EPHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves you organization? (A)	
164.308(a)(4)(i)	**Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.**	
164.308(a)(4)(ii)(A)	If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization? (A)	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? (A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process? (A)	
164.308(a)(5)(i)	**Security Awareness and Training: Implement a security**	

	awareness and training program for all members of its workforce (including management).	
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring login attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes? (R)	
164.308(a)(7)(i)	**Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.**	
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically? (R)	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	Have you established a plan for periodic technical and non technical evaluation of the standards under this rule in response to environmental or operational changes affecting the security of EPHI? (R)	
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered Entity (CE), in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only of the CE obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.**	
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances that the BA will appropriately safeguard the information? (R)	

HIPAA SECURITY RULE - PHYSICAL SAFEGUARDS (R) = REQUIRED, (A) = ADDRESSABLE		
164.310(a)(1)	**Facility Access Controls: Implement 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.**	
164.310(a)(2)(i)	Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency? (A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? (A)	
164.310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks)? (A)	
164.310(b)	Have you implemented 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 EPHI? (R)	
164.310(c)	Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)	
164.310(d)(1)	**Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.**	
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (R)	
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of EPHI, when needed, before movement of equipment? (A)	
HIPAA SECURITY RULE - TECHNICAL SAFEGUARDS (R) = REQUIRED, (A) = ADDRESSABLE		
164.312(a)(1)	**Access Controls: Implement technical policies and procedures for electronic information systems that maintain**	

	EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during and emergency? (R)	
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI? (A)	
164.312(b)	Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)	
164.312(c)(1)	**Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.**	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed? (R)	
164.312(e)(1)	**Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.**	
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	
HITECH ACT		
§13401	**Application of security provisions and penalties to Business Associates of Covered Entities; Annual guidance on security provisions.**	
	Are Business Associate Agreements updated appropriately? - The HITECH Act changes applicable to covered entities also apply to business associates for both privacy and security and needs to be incorporated into the BA agreements.	
§13402	**Notification in the case of breach**	
	Process for notification to the following in the event of a breach of unsecured PHI: - Individuals - Media	

	- Secretary of HHS	
	Use of encryption in accordance with HHS guidance. For example, the use of FIPS 140-2 whole disk encryption as specified in NIST 800-111.	
§13405	**Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format.**	
	Process for Handling Individual's Request to Restrict Disclosure	
	Limit disclosure or use of PHI to minimum necessary to accomplish purpose by, to the extent possible, limiting use/disclosure to "limited data set"	
§13405(c)	**Accounting of certain protected health information disclosures required if CE uses electronic health record.**	
	If Covered Entities use electronic health record, Covered Entities must include disclosures made through an EHR for payment/treatment/health care operation on the accounting and the individual can get an accounting of payment/treatment/health care operation disclosures made during past 3 years.	
	Process to allow individual to obtain an accounting of disclosures made by Covered Entity & Business Associates or an accounting of disclosures by Covered Entity and a list of Business Associates with contact information. Business Associates must give individuals an accounting of PHI disclosures.	

References:

1. IHS - HIPAA Security Checklist, from
http://hipaa.ihs.gov
2. KaMMCO - Checklist for Covered Entities, from
http://www.kammco.com
3. Alabama Medicaid Agency – Checklist for HIPAA Privacy, from
http://www.medicaid.state.al.us
4. Patricia I. Carter (2010)
HIPAA Compliance Handbook 2010 Edition