

SECURITY RISK ASSESSMENT SUMMARY

Providers Business Name: _____

Providers Business Address: _____

City, State, Zip _____

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 for the Security Risk Assessment

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?

- The Department of Health and Human Services sets forth the HIPAA requirements for privacy, security, enforcement, and breach in 45 CFR Parts 160 and 164 of the Federal Register.
- The preparer is responsible for reviewing the HIPAA requirements and modifying the security risk assessment to meet the current HIPAA requirements.
- 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 determine whether or not it is a 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.
- The Security Risk Assessment is divided into two categories:
 - a. Administrative Safeguards
 - b. Physical Safeguards
- **REF** - The reference refers to the C.F.R. (Code of Federal Regulations) maps to the requirement or safeguard to the specific regulation.
- **SAFEGUARDS** - This field is the requirement of the safeguard being evaluated.
- **STATUS** - This field is to specify the status of the requirement or safeguard (Complete, Not Complete, In Progress, Unknown, or N/A). Check only one box per safeguard. Each requirement provides for comments relating to the Safeguard being assessed. You may add any additional comments to the field or on a separate sheet of paper.
- Last Revision Date – 07/01/2013.

SECURITY RISK ASSESSMENT SUMMARY

REF	Administrative Safeguards	STATUS
§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. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.522	Develop policies for alternative means of communication requests. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.520	Develop and disseminate notice of privacy practice. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.524	Develop policies for access to designated record sets: - Providing access - Denying access COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.526	Develop policies for amendment requests: - Accepting an amendment - Denying an amendment - Actions on notice of an amendment - Documentation COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§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. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.528	Develop policies for accounting of disclosures. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§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. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.530	Implementation of Privacy Rule Administrative requirements, including: - Appoint of a HIPAA privacy officer. - Training of workforce - Sanctions for non-compliance - Develop compliance policies. - Develop anti-retaliation policies. - Policies and Procedures COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§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. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed in accordance with NIST Guidelines? COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(1)(ii)(B)	Has the Risk Management process been completed in accordance with NIST Guidelines? COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.308(a)(1)(ii)(D)	<p>Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(3)(i)	<p>Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information (EPHI).</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(3)(ii)(A)	<p>Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(3)(ii)(B)	<p>Have you implemented procedures to determine that the access of an employee to EPHI is appropriate?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(1)(ii)(C)	<p>Have you implemented procedures for terminating access to EPHI when an employee leaves your organization?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(4)(ii)(A)	<p>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?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(4)(ii)(B)	<p>Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.308(a)(1)(ii)(C)	<p>Have you implemented policies and procedures that are based upon your access authorization policies to establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(5)(ii)(A)	<p>Do you provide periodic information security reminders?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(5)(ii)(B)	<p>Do you have policies and procedures for guarding against, detecting, and reporting malicious software?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(5)(ii)(D)	<p>Do you have procedures for creating, changing, and safeguarding passwords?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(6)(ii)	<p>Do you have procedures to identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(7)(ii)(A)	<p>Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(7)(ii)(B)	<p>Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.308(a)(7)(ii)(C)	<p>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?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(7)(ii)(D)	<p>Have you implemented procedures for periodic testing and revision of contingency plans?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(7)(ii)(E)	<p>Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(8)	<p>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?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(b)(4)	<p>Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances that the BA will appropriately safeguard the information?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.308(a)(1)(ii)(C)	<p>Do you have formal sanctions against employees who fail to comply with security policies and procedures?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

REF	PHYSICAL SAFEGUARDS	STATUS
§164.312(b)	<p>Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(b)	<p>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?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.312(e)(2)(i)	<p>Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.312(a)(2)(iv)	<p>Have you implemented a mechanism to encrypt and decrypt EPHI?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.312(a)(2)(iv)	<p>Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.312(c)(2)	<p>Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.310(c)	<p>Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(a)(2)(iii)	<p>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?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(a)(2)(ii)	<p>Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.312(d)	<p>Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access to EPHI is the one claimed?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§13402	<p>Process for notification to the following in the event of a breach of unsecured PHI:</p> <ul style="list-style-type: none"> - Individuals - Media - Secretary of HHS <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(a)(2)(iv)	<p>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).</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§164.310(d)(2)(i)	<p>Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(d)(2)(ii)	<p>Have you implemented procedures for removal of EPHI electronic media before the media are available for reuse?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(d)(2)(iii)	<p>Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§164.310(d)(2)(iv)	<p>Do you create a retrievable, exact copy of EPHI, when needed, before movement of equipment?</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§13405(c)	<p>Process to allow individual to obtain an accounting of disclosures made by Covered Entity and 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.</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
§13402	<p>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.</p> <p>COMMENTS:</p>	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A

SECURITY RISK ASSESSMENT SUMMARY

§13401	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. COMMENTS:	<input type="checkbox"/> Complete <input type="checkbox"/> Not Complete <input type="checkbox"/> In Progress <input type="checkbox"/> Unknown <input type="checkbox"/> N/A
--------	---	--

Additional Comments:

Safeguard:	Comments:

SECURITY RISK ASSESSMENT SUMMARY

References:

- DHHS 45 CFR Parts 160 and 164
- OCR: §45 CFR 164.318 308 (a)(1)(ii)(a)
- ONC: §45 CFR 170
-
-
-

Updates

Performed By	Date Performed	Software Version	Comments

Last Preparer Contact Information:

Name:

Address:

City, State, Zip Code

Phone:

E-Mail:

Attachments:

- Security Policy (Recommended)
- Plan of Correction (Recommended)