**TRS**

**Information Security Risk Assessment**

***HIPAA Compliance – Supplemental Assessment***

|  |  |
| --- | --- |
| **Contractor Name:** |  |
|  |  |  |  |
| **Completed by:** |  |
|  |  |  |  |
| **Email Address:** |  |
|  |  |  |  |
| **Phone Number:** |  |
|  |  |  |  |

**Completed by TRS**

|  |  |
| --- | --- |
| **Reviewed by:** |  |
|  |  |  |  |
| **Accepted:** |  | **Rejected:** |  |  |

 **Comments:**

**Section A - Administrative Safeguards**

**A1.0 - Security management process - 164.308(a)(1)(i)**

**Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.**

**A1.1 - Risk analysis - 164.308(a)(1)(ii)(A)**

**Required Implementation Specification: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the business associate.**

1. Is there a documented analysis of current safeguards and their effectiveness relative to the identified risks to the confidentiality, integrity and availability of ePHI held by the business associate?
2. Does the analysis cover all processes involving ePHI, including creation, receipt, maintenance, and transmission?
3. Does the analysis include documentation of the information system configuration, including connections to other systems?
4. Does the analysis include identification of all hardware and software that maintains or transmits ePHI, including removable media and remote access devices?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A1.2 - Risk management - 164.308(a)(1)(ii)(B)**

**Required Implementation Specification: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).**

1. Has the business associate protected (to a reasonable and appropriate level) the security, integrity, and availability of the ePHI against all reasonably anticipated threats or hazards?
2. Do current safeguards protect against reasonably anticipated uses or disclosures of ePHI that are not permitted by the Privacy Rule?
3. Has the business associate assured workforce compliance with all policies and procedures involving ePHI?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A1.3 - Sanction policy - 164.308(a)(1)(ii)(C)**

**Required Implementation Specification: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the business associate.**

1. Is there a formal process in place to address misuse, abuse, and fraudulent activity with regard to ePHI?
2. Does the process include sanctions appropriate to the magnitude, harm, and possible types of inappropriate disclosures?
3. Does the process include procedures for notifying managers and employees of suspect activity (i.e., failing to comply with security policies and procedures)?
4. Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of ePHI?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A1.4 - Information system activity review - 164.308(a)(1)(ii)(D)**

**Required Implementation Specification: Implement procedures to review records of information system activity, such as audit logs, access reports, and security incident tracking reports.**

1. Are information system activity records (e.g., audit/security logs, access reports, security incident tracking reports) reviewed and analyzed in a regular and consistent manner?
2. If yes, how often does the review and analysis of information system activity records take place (e.g., daily, weekly, monthly, randomly, event-driven)?
3. Are information system activity records (e.g., audit/security logs, access reports, security incident tracking reports) adequately protected from unauthorized disclosure, modification, or deletion?
4. Briefly describe the methods used to protect the information system activity records:
5. Are procedures in place to assess the effectiveness of the review process and revise the process when necessary?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A2.0 - Assigned security responsibility - 164.308(a)(2)**

**Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the business associate.**

1. Has someone been assigned to have final responsibility for security for the business associate? This individual should be able to assess effective security and serve as the point of contact for security policy, implementation, and monitoring.
2. If yes, identify the individual:
3. Does this individual's job description accurately reflect assigned security duties and responsibilities?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A3.0 - Workforce security - 164.308(a)(3)(i)**

**Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section [164.308(a) (4) - Information Access Management], 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.**

**A3.1 - Authorization and/or supervision - 164.308(a)(3)(ii)(A)**

**Addressable Implementation Specification: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have procedures been implemented to authorize and/or supervise workforce members who work with ePHI or in locations where it might be accessed?

[ ] Yes [ ] No

**A3.2 - Workforce clearance procedures - 164.308(a)(3)(ii)(B)**

**Addressable Implementation Specification: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Do procedures exist for obtaining appropriate authorization from management to grant or terminate access to ePHI for workforce members?
2. Are there written job descriptions that correlate with appropriate levels of access?
3. Have staff members been provided copies of their job descriptions, informed of access granted to them, and notified of the conditions under which this access can be used?
4. Does the personnel hiring process include checking the qualifications of candidates for specific positions against the job description and determining that the candidates are able to perform required job tasks?
5. Have policies or procedures been implemented that address appropriate background screening of persons who will have access to ePHI?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A3.3 - Termination procedures - 164.308(a)(3)(ii)(C)**

**Addressable Implementation Specification: Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are there separate procedures for terminating access to ePHI for voluntary termination (retirement, promotion, change of employment) vs. involuntary termination (termination for cause, reduction in force, involuntary transfer, criminal or disciplinary actions) of employment?
2. Is there a standard checklist for all action items that should be completed when an employee leaves (e.g., return of all access devices, deactivation of logon accounts, and delivery of any needed data solely under the employee's control)?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A4.0 - Information access management - 164.308(a)(4)**

**Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.**

**A4.1 - Isolating health care clearinghouse functions - 164.308(a)(4)(ii)(A)**

**Required Implementation Specification: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.**

1. Does the business associate constitute a health care clearinghouse under the HIPAA security rule and is it part of a larger organization?

[Note: This question is informational. Negative answers are not scored.]

1. Have steps been taken to ensure that ePHI for the clearinghouse is protected from unauthorized access by the larger organization concerning physical security, staff security, network security, and logical security?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A4.2 - Access authorization - 164.308(a)(4)(ii)(B)**

**Addressable Implementation Specification: Implement policies and procedures for granting access to electronic protected health information (e.g., through access to a workstation, transaction, program, process, or other mechanism). Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Does the business associate have policies and procedures for granting access to ePHI?
2. Is the information system capable of setting the access controls specified in the policies and procedures?
3. Select the method(s) of access control used (all that apply):

A) identity-based

B) role-based

C) location-based

D) other:

[ ] Yes [ ] No

[ ] Yes [ ] No

**A4.3 - Access establishment and modification - 164.308(a)(4)(ii)(C)**

**Addressable Implementation Specification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are duties separated such that only the minimum necessary ePHI is made available to each staff member based on job requirements?
2. Does management regularly review the list of access authorizations, including remote access authorizations, to verify that the list is accurate and has not been inappropriately altered?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A5.0 - Security awareness and training - 164.308(a)(5)(i)**

**Standard: Implement a security awareness and training program for all members of its workforce (including management).**

1. Have all employees received adequate training to fulfill their security responsibilities?
2. Does the business associate's security awareness and training program cover all topics relevant to the organization (e.g., portable device security, remote access security, desktop security, email security, etc.)?
3. Are employees appropriately trained on security and risks to ePHI when reusing hardware?
4. Are procedures in place to assess the effectiveness of the security awareness training program and revise the training when necessary?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A5.1 - Security reminders - 164.308(a)(5)(ii)(A)**

**Addressable Implementation Specification: Periodic security updates. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Is security awareness discussed with all new hires?
2. Are procedures in place to keep staff aware of security topics?
3. What methods are used to keep staff aware of security topics (e.g., emails, staff meetings, posters, newsletters):
4. Is security refresher training performed on a periodic basis?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A5.2 - Protection from malicious software - 164.308(a)(5)(ii)(B)**

**Addressable Implementation Specification: Procedures for guarding against, detecting, and reporting malicious software. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have appropriate staff been made aware of the importance of timely application of security-related patches and updates (e.g., Windows hotfixes, antivirus definition updates, antispyware definition updates) to protect against malicious software and exploitation of vulnerabilities?

[ ] Yes [ ] No

**A5.3 - Log-in monitoring - 164.308(a)(5)(ii)(C)**

**Addressable Implementation Specification: Procedures for monitoring login attempts and reporting discrepancies. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have users been formally notified that log­in attempts may be monitored (e.g., warning screen, pop-up, written documentation)?
2. Are procedures in place for reporting login discrepancies to the proper security authority?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A5.4 - Password management - 164.308(a)(5)(ii)(D)**

**Addressable Implementation Specification: Procedures for creating, changing and safeguarding passwords. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have staff been made aware of their roles and responsibilities in selecting passwords of appropriate strength, changing the passwords periodically (if required), and safeguarding their passwords?

[ ] Yes [ ] No

**A6.0 - Security incident procedures - 164.308(a)(6)(i)**

**Standard: Implement policies and procedures to address security incidents.**

**A6.1 - Response and reporting - 164.308(a)(6)(ii)**

**Required Implementation Specification: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes.**

1. Are there procedures in place for reporting and handling security incidents?
2. Does the business associate have or have access to incident response personnel or an incident response team?
3. Has a written incident response plan been developed and provided to the appropriate personnel?
4. Has the business associate developed standard incident report templates to ensure that all necessary information related to the incident is documented and investigated?
5. Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared (e.g., incident response personnel, security manager, information system owner, CIO, ISO, CSO, law enforcement), and is this list reviewed and updated on a regular basis?
6. Do incident response personnel have adequate knowledge of the business associate's hardware and software?
7. Does the business associate keep adequate documentation of security incidents and their outcomes, which may include what weaknesses were exploited and how access to information was gained?
8. Has the business associate determined reasonable and appropriate mitigation options for foreseeable security incidents?
9. Are procedures in place to assess the effectiveness of the incident management procedures and revise the procedures when necessary?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A7.0 - Contingency plan - 164.308(a)(7)(i)**

**Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.**

1. Has a determination been made regarding when the contingency plan needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery, etc.)?
2. Have cross-functional dependencies been identified to determine how the failure in one system may negatively affect another one?
3. Has responsibility for managing, maintaining and updating the contingency plan been assigned?
4. If yes, identify the individual(s):

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A7.1 - Data backup plan - 164.308(a)(7)(ii)(A)**

**Required Implementation Specification: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.**

1. Have procedures for creating and maintaining retrievable exact copies of ePHI been developed, documented, and made available to the appropriate staff?
2. Has responsibility for implementation of the procedures for creating and maintaining retrievable exact copies of ePHI been assigned?
3. If yes, identify the individual(s) or work group:

[ ] Yes [ ] No

[ ] Yes [ ] No

**A7.2 - Disaster recovery plan - 164.308(a)(7)(ii)(B)**

**Required Implementation Specification: Establish (and implement as needed) procedures to restore any loss of data.**

1. Have procedures for data restoration been developed, documented, and made available to the appropriate staff?
2. Is there a formal, written disaster recovery plan?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A7.3 - Emergency mode operations plan - 164.308(a)(7)(ii)(C)**

**Required Implementation Specification: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.**

1. Have procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode (e.g., controlling physical access to backup media or storage devices containing ePHI) been developed, documented, and made available to the appropriate staff?

[ ] Yes [ ] No

**A7.4 - Testing and revision procedures - 164.308(a)(7)(ii)(D)**

**Addressable Implementation Specification: Implement procedures for periodic testing and revision of contingency plans. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have procedures to test and revise the contingency plan been developed, documented, and made available to the appropriate staff?
2. Describe the testing methodology (e.g., full, phased approach, "tabletop" scenarios):
3. Is the contingency plan tested and revised periodically?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A7.5 - Applications and data criticality analysis - 164.308(a)(7)(ii)(E)**

**Addressable Implementation Specification: Assess the relative criticality of specific applications and data in support of other contingency plan components. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have the hardware, software and personnel that are critical to daily operations (including ePHI) been identified and documented?
2. Have the hardware, software and personnel that are critical to daily operations (including ePHI) been analyzed in order to determine their relative criticality in support of components of the contingency plan?

[ ] Yes [ ] No

[ ] Yes [ ] No

**A8.0 - Evaluation - 164.308(a)(8)**

**Standard: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**

1. Does the evaluation process consider all standards and implementation specifications of the HIPAA security rule?
2. Are the appropriate technical, legal, compliance, and business knowledge represented adequately in the personnel conducting the evaluation?
3. Has the evaluation process been formally communicated to participating personnel?
4. Does the evaluation process support development of security recommendations?
5. Is penetration testing part of the evaluation process? [Note: This question is informational. Negative answers are not scored.]
6. Has specifically ­worded written approval for the use of penetration testing been obtained from the information resource owner and any other entities that have approval authority over such testing?
7. Have steps been taken to ensure the security of any evaluation results and written reports and their availability to the appropriate personnel?
8. Do security policies specify that evaluations will be repeated when environmental and operational changes are made that affect the security of ePHI?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A9.0 - Business associate contracts and other arrangements - 164.308(b)(1)**

**Standard: A covered entity, in accordance with 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314(a) that the business associate will appropriately safeguard the information.**

1. Do associations exist in which the covered entity and the business associate are both government entities? If you are unsure of your organization's status as a possible government entity, please contact your legal counsel. [Note: This question is informational. Negative answers are not scored.]
2. Is the business associate a business associate of another covered entity? [Note: This question is informational. Negative answers are not scored.]
3. Is the business associate in full compliance with the satisfactory assurances it provided as a business associate of another covered entity? (If the business associate is in violation, answer no.)

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**A9.1 - Written contract or other arrangement - 164.308(b)(3)**

**Required Implementation Specification: Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of 164.314(a).**

1. Has responsibility been assigned for coordinating and preparing the final agreements or arrangements (e.g., business associate contracts)?
2. If yes, identify the individual(s) or work group:
3. Do the agreements or arrangements specify how information is to be transmitted to and from business associates?
4. Have appropriate security controls been specified for the business associates?
5. Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected?
6. Is there a process in place to evaluate periodically the effectiveness of business associate security controls?
7. For associations in which the covered entity and the business associate are both government entities, are there procedures in place to use a memorandum of understanding or a reliance on law or regulation that require equivalent actions on the part of the business associate?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**Section B - Physical Safeguards**

**B1.0 - Facility access control - 164.310(a)**

**Standard: 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.**

**B1.1 - Contingency operations - 164.310(a)(2)(i)**

**Addressable Implementation Specification: Establish (and implement 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. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have procedures been developed that allow access to the facility in which the information systems are housed in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan?
2. Are the procedures appropriate for all types of foreseeable potential disasters (e.g., fire, flood, earthquake, etc.)?

[ ] Yes [ ] No

[ ] Yes [ ] No

**B1.2 - Facility security plan - 164.310(a)(2)(ii)**

**Addressable Implementation Specification: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Is there a facility/space inventory available (e.g., building name/number, room number, etc.)?
2. Have procedures been developed and implemented for securing the facilities?
3. Briefly describe the procedures for securing the facilities:
4. Has an individual been assigned responsibility for facility security?
5. Identify the individual:

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**B1.3 - Access control and validation - 164.310(a)(2)(iii)**

**Addressable Implementation Specification: Implement 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. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are there policies and procedures in place to control and validate access to facilities by staff (by role or function), contractors, and visitors?
2. Have all points of access to the facility been identified and are they covered by access control policies and procedures?

[ ] Yes [ ] No

[ ] Yes [ ] No

**B1.4 - Maintenance records - 164.310(a)(2)(iv)**

**Addressable Implementation Specification: Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors and locks). Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are repairs and modifications to the physical components of the facility (e.g., hardware, walls, doors, locks, etc.) documented?
2. Are records of repairs and modifications to the physical components of the facility maintained as per applicable records retention policies?
3. Has responsibility for maintaining facility repair and modification records been assigned?
4. Identify the individual(s) or work group:

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**B2.0 - Workstation use - 164.310(b)**

**Standard: Implement 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.**

1. Have policies and procedures related to the proper use of workstations been developed?
2. Have policies and procedures related to mitigation of key operational risks that could result in a breach of security been developed?
3. Have policies and procedures related to mitigation of risks associated with the physical attributes of the surroundings of the workstations been developed?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**B3.0 - Workstation security - 164.310(c)**

**Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**

1. Does the business associate maintain an accurate inventory of all types of computing devices used as workstations (e.g., desktops, laptops, tablet PCs, thin terminals, PDAs) identified and inventoried, including their location or the staff members to whom they have been assigned?
2. If yes, identify the person(s) responsible for this inventory and its maintenance:
3. Have adequate physical safeguards been put in place to restrict access to ePHI to authorized users (e.g., locked doors, screen barriers, cameras, guards), including in areas that may be particularly vulnerable to unauthorized use, theft, or viewing of the data they contain or display?
4. Briefly describe the physical security measures that have been taken to protect workstations:

[ ] Yes [ ] No

[ ] Yes [ ] No

**B4.0 - Device and media controls - 164.310(d)(1)**

**Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information in and out of a facility, and the movement of these items within the facility.**

**B4.1 - Disposal - 164.310(d)(2)(i)**

**Required Implementation Specification: Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.**

1. Does your process, or that of any entity hired, contracted, or assigned, for removing ePHI from equipment during disposal, ensure that ePHI is unrecoverable using common techniques or analysis? (Examples of processes include destruction of media, degaussing, and multi-pass overwrites.)
2. Does your process for final disposition of removable media such as floppy disks, backup tapes and CDs that contain ePHI include destruction of media?

[ ] Yes [ ] No

[ ] Yes [ ] No

**B4.2 - Media re-use - 164.310(d)(2)(ii)**

**Required Implementation Specification: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.**

1. Are procedures in place that ensure the secure removal of ePHI from electronic media (e.g., flash drives or backup tapes) before the media are made available for re-use?

[ ] Yes [ ] No

**B4.3 - Accountability - 164.310(d)(2)(iii)**

**Addressable Implementation Specification: Maintain a record of the movements of hardware and electronic media and any person responsible thereof. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Has one entity (individual, department, team, etc.) been assigned responsibility for coordinating the disposal of data and the re-use of hardware?
2. If yes, identify the entity:
3. Does the business associate have procedures to track the accurate movements of hardware and electronic media within the organization and/or facility?
4. Do procedures exist to track hardware or electronic media (e.g., laptops, PDAs, flash drives, backup tapes) that contain or may be used to access ePHI if said hardware or media is removed from the facility?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**B4.4 - Data backup and storage - 164.310(d)(2)(iv)**

**Addressable Implementation Specification: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Do procedures exist to create a retrievable, exact copy of ePHI prior to relocating equipment?
2. Are backup files maintained off-site to assure data availability in the event data is lost while transporting or moving electronic media containing ePHI?

[ ] Yes [ ] No

[ ] Yes [ ] No

**Section C - Technical Safeguards**

**C1.0 - Access control - 164.312(a)(1)**

**Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).**

1. Are rules being enforced to remove access by staff members who no longer have a need to know because they have changed assignments or have stopped working for the business associate?
2. Does the business associate have documented access control procedures?
3. Have new employees and/or users of systems that utilize ePHI been given proper instructions for protecting data and systems?
4. Are there procedures for new employee/user access to data and systems?
5. Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C1.1 - Unique user identification - 164.312(a)(2)(i)**

**Required Implementation Specification: Assign a unique name and/or number for identifying and tracking user identity.**

1. Are all users of systems that access ePHI assigned a unique name and/or number for recording and tracking user identity?
2. Can system activity be traced to a specific user?
3. Is there sufficient data in system and/or application logs to support audit and other related business functions?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C1.2 - Emergency access procedure - 164.312(a)(2)(ii)**

**Required Implementation Specification: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.**

1. Have procedures been established for obtaining necessary ePHI during an emergency?
2. Have individuals been identified and assigned authorization to activate emergency ePHI access procedures?
3. If yes, identify the individuals:
4. Have the emergency ePHI procedures been tested and found to be adequate?
5. Have criteria for activation of the emergency ePHI access procedures been identified?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C1.3 - Automatic logoff - 164.312(a)(2)(iii)**

**Addressable Implementation Specification: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are automatic logoff features available for the business associate’s operating systems and/or other major applications?
2. Have automatic logoff features been implemented?
3. What period of inactivity (number of minutes) prior to automatic logoff is being used?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C1.4 - Encryption and decryption - 164.312(a)(2)(iv)**

**Addressable Implementation Specification: Implement a mechanism to encrypt and decrypt electronic protected health information.**

1. Is ePHI encrypted during transmission?
2. If yes, what type of encryption is used to protect ePHI during transmission:
3. Is ePHI encrypted when being stored and maintained?
4. If yes, what type of encryption is used to protect ePHI while it is being stored and maintained:

[ ] Yes [ ] No

[ ] Yes [ ] No

**C2.0 - Audit controls - 164.312(b)**

**Standard: Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**

1. Are system activity audits conducted on systems that contain or use ePHI and the results analyzed periodically?
2. If yes, how often are system activity audits conducted and the results analyzed:
3. What auditing and system activity tools are in place:
4. Has an individual been assigned responsibility for the overall audit process and results?
5. If yes, identify the individual:
6. Have mechanisms been implemented to assess the effectiveness of the audit process (metrics) and revise it if necessary?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C3.0 - Integrity - 164.312(c)(1)**

**Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**

1. Have the integrity requirements been documented?
2. Has a written policy been developed and communicated to system users?
3. Are implemented audit, logging, and access control techniques sufficient to address the integrity of the information?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C3.1 - Mechanism to authenticate electronic protected health information - 164.312(c)(2)**

**Addressable Implementation Specification: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Are electronic mechanisms (software or hardware) being used to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?

[ ] Yes [ ] No

**C4.0 - Person or entity authentication - 164.312(d)**

**Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**

1. Has the appropriate level of authentication (single-factor or multi-factor) been determined based on risk assessment?
2. Is the determined level of authentication being used?
3. Have formal authentication policy and procedures been established and communicated?
4. Do the authentication procedures include ongoing system maintenance and updates?
5. Is the authentication process implemented in such a way that it does not compromise the authentication information (e.g., password file encryption and passwords not transmitted in clear text)?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C5.0 - Transmission security - 164.312(e)(1)**

**Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**

**C5.1 - Integrity controls - 164.312(e)(2)(i)**

**Addressable Implementation Specification: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Have measures been implemented that protect the integrity of the ePHI during transmission?
2. If yes, what measures exist to protect ePHI in transmission?
3. Is there assurance that information is not altered during transmission?
4. Is there an auditing process in place to verify that ePHI has been protected against unauthorized access during transmission?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**C5.2 - Encryption - 164.312(e)(2)(ii)**

**Addressable Implementation Specification: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. Refer to the appendix regarding 164.306(d)(3)(ii)(B) compliance.**

1. Is encryption reasonable and appropriate for ePHI in transmission or needed to protect the information in transmission?

[Note: This question is informational. Negative answers are not scored.]

1. Is encryption utilized in order to protect ePHI during transmission?
2. Does the business associate have the appropriate staff to maintain a process for encrypting ePHI during transmission?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**Section D - Organizational Requirements**

**D1.0 - Business associate contracts - 164.314(a)(2)(i)**

**Required Implementation Specification: The contract between a covered entity and a business associate must provide that the business associate will: (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by covered entity, if the business associate determines that the business associate has violated a material term of the contract.**

1. Do the written agreements between the covered entity and the business associates address the applicable functions related to creating, receiving, maintaining, and transmitting ePHI that the business associates are to perform on behalf of the covered entity?
2. Do the written agreements address the issue of ePHI access by subcontractors and other agents of the business associates?
3. Is there a procedure in place for reporting of incidents by business associates?
4. Have key business associate staff that would be the point(s) of contact in the event of a security incident been identified?
5. For each business associate contract, have standards and thresholds for termination of the contract been included in the contract (unless the covered entity or its business associate have statutory obligations that require the removal of such language)?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**D1.1 - Other arrangements - 164.314(a)(2)(ii)**

**Required Implementation Specification: (A) When a covered entity and its business associate are both governmental entities, the business associate is in compliance with paragraph (a)(1) of this section, if— (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or Department of Health and Human Services § 164.316 (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. (B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph § 164.504 (e)(2)(iii) if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.**

1. For associations in which the covered entity and the business associate are both government entities, do the arrangements provide protections for ePHI equivalent to those provided by the covered entity's business associate contracts?
2. For associations in which the covered entity and the business associate are both government entities, if termination of the memorandum of understanding is not possible due to the nature of the relationship between the covered entity and the business associate, are other mechanisms for enforcement available, reasonable, and appropriate?
3. Has the business associate made a good faith attempt to obtain satisfactory assurances that the security standards required by this section are being met?
4. Are attempts to obtain satisfactory assurances and the reasons assurances cannot be obtained, if applicable, documented?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**D2.0 - Requirements for group health plans - 164.314(b)(1)**

**Standard: Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.**

**D2.1 - The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to - 164.314(b)(2)**

**Required Implementation Specification: (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.**

1. Is the covered entity a health care plan as defined in 45 CFR Sec. 160.103 that does not fall under the exception described in 45 CFR Sec. 164.314(b)(1)?

[Note: This question is informational. Negative answers are not scored.]

1. Do the plan documents require the plan sponsor to safeguard ePHI reasonably and appropriately?
2. Do plan documents address the obligation to keep ePHI secure with respect to the plan sponsor's employees, classes of employees, or other persons who will be given access to ePHI?
3. Do the plan documents of the group health plan address the issue of subcontractors and other agents of the plan sponsor implementing reasonable and appropriate security measures?
4. Do the plan documents require the plan sponsor to report to the group health plan any security incident of which it becomes aware?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**Section E - Policies, Procedures and Documentation**

**E1.0 - Policies and procedures - 164.316(a)**

**Standard: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, if the changes are documented and are implemented in accordance with this subpart.**

1. Are reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule in place?
2. Do procedures exist for periodically re-evaluating the policies and procedures, updating them as necessary?
3. As policies and procedures are changed, are new versions made available and are workforce members appropriately informed?

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**E2.0 - Documentation - 164.316(b)(1)**

**Standard: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.**

1. Are all required policies and procedures documented?
2. Is HIPAA security documentation updated in response to periodic evaluations, following security incidents, after the acquisition of new technology, and/or after the development/implementation of new procedures?
3. Has an individual been assigned responsibility for maintaining the HIPAA Security Rule documentation?
4. If yes, identify the individual(s):

[ ] Yes [ ] No

[ ] Yes [ ] No

[ ] Yes [ ] No

**E2.1 - Time limit - 164.316(b)(2)(i)**

**Required Implementation Specification: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.**

1. Have documentation retention requirements under HIPAA been aligned with the business associate's other data retention policies?

[ ] Yes [ ] No

**E2.2 - Availability - 164.316(b)(2)(ii)**

**Required Implementation Specification: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.**

1. Is the location of documentation known to all staff that need to access it?
2. Is availability of the documentation made known as part of education, training, and awareness activities?

[ ] Yes [ ] No

[ ] Yes [ ] No

**E2.3 - Updates - 164.316(b)(2)(iii)**

**Required Implementation Specification: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.**

1. Is there a version control procedure that allows verification of the timeliness of policies and procedures, if reasonable and appropriate?
2. Is there a process for soliciting input into updates of policies and procedures from staff, if reasonable and appropriate?

[ ] Yes [ ] No

[ ] Yes [ ] No

**Appendix**

In order to be compliant with 164.306(d)(3)(ii)(B), if a covered entity does not implement an Addressable specification, the following process must be followed: assess whether the implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic protected health information; document why it would not be reasonable and appropriate to implement the implementation specification; and implement an equivalent alterative measure if reasonable and appropriate.