

ISAAC Section	Section Title	Sub-section	Subsection Title	CFR Reference	Specification Type	Q. Num	Question	Answer Type
A	Administrative Safeguards	A1.0	Security management process	164.308(a)(1)(i)	Standard	---	---	---
A	Administrative Safeguards	A1.1	Risk analysis	164.308(a)(1)(ii)(A)	Required Implementation Specification	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 covered entity?	Yes/No
A	Administrative Safeguards	A1.1	Risk analysis	164.308(a)(1)(ii)(A)	Required Implementation Specification	2	Does the analysis cover all processes involving EPHI, including creation, receipt, maintenance and transmission?	Yes/No
A	Administrative Safeguards	A1.1	Risk analysis	164.308(a)(1)(ii)(A)	Required Implementation Specification	3	Does the analysis include documentation of the information system configuration, including connections to other systems?	Yes/No
A	Administrative Safeguards	A1.1	Risk analysis	164.308(a)(1)(ii)(A)	Required Implementation Specification	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
A	Administrative Safeguards	A1.2	Risk management	164.308(a)(1)(ii)(B)	Required Implementation Specification	1	Has the covered entity protected (to a reasonable and appropriate level) the security, integrity and availability of the EPHI against all reasonably anticipated threats or hazards?	Yes/No
A	Administrative Safeguards	A1.2	Risk management	164.308(a)(1)(ii)(B)	Required Implementation Specification	2	Do current safeguards protect against reasonably anticipated uses or disclosures of EPHI that are not permitted by the Privacy Rule (http://www.access.gpo.gov/nara/cfr/waisidx_06/45cfr164_06.html)?	Yes/No
A	Administrative Safeguards	A1.2	Risk management	164.308(a)(1)(ii)(B)	Required Implementation Specification	3	Has the covered entity assured workforce compliance with all policies and procedures involving EPHI?	Yes/No
A	Administrative Safeguards	A1.3	Sanction policy	164.308(a)(1)(ii)(C)	Required Implementation Specification	1	Is there a formal process in place to address misuse, abuse, and fraudulent activity with regard to EPHI?	Yes/No
A	Administrative Safeguards	A1.3	Sanction policy	164.308(a)(1)(ii)(C)	Required Implementation Specification	2	Does the process include sanctions appropriate to the magnitude, harm, and possible types of inappropriate disclosures?	Yes/No
A	Administrative Safeguards	A1.3	Sanction policy	164.308(a)(1)(ii)(C)	Required Implementation Specification	3	Does the process include procedures for notifying managers and employees of suspect activity (i.e., failing to comply with security policies and procedures)?	Yes/No
A	Administrative Safeguards	A1.3	Sanction policy	164.308(a)(1)(ii)(C)	Required Implementation Specification	4	Have employees been made aware of policies concerning sanctions for inappropriate access, use and disclosure of EPHI?	Yes/No
A	Administrative Safeguards	A1.4	Information system activity review	164.308(a)(1)(ii)(D)	Required Implementation Specification	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?	Yes/No
A	Administrative Safeguards	A1.4	Information system activity review	164.308(a)(1)(ii)(D)	Required Implementation Specification	1.1	How often does the review and analysis of information system activity records take place (e.g., daily, weekly, monthly, randomly, event-driven)?	Free Text Answer
A	Administrative Safeguards	A1.4	Information system activity review	164.308(a)(1)(ii)(D)	Required Implementation Specification	2	Are information system activity records (e.g., audit/security logs, access reports, security incident tracking reports) adequately protected from unauthorized disclosure, modification or deletion?	Yes/No
A	Administrative Safeguards	A1.4	Information system activity review	164.308(a)(1)(ii)(D)	Required Implementation Specification	2.1	Briefly describe the methods used to protect the information system activity records.	Free Text Answer
A	Administrative Safeguards	A1.4	Information system activity review	164.308(a)(1)(ii)(D)	Required Implementation Specification	3	Are procedures in place to assess the effectiveness of the review process and revise the process when necessary?	Yes/No
A	Administrative Safeguards	A2.0	Assigned security responsibility	164.308(a)(2)	Standard	1	Has someone been assigned to have final responsibility for security for the covered entity? This individual should be able to assess effective security and serve as the point of contact for security policy, implementation and monitoring.	Yes/No
A	Administrative Safeguards	A2.0	Assigned security responsibility	164.308(a)(2)	Standard	1.1	Identify the individual:	Free Text Answer
A	Administrative Safeguards	A2.0	Assigned security responsibility	164.308(a)(2)	Standard	2	Does this individual's job description accurately reflect assigned security duties and responsibilities?	Yes/No
A	Administrative Safeguards	A3.0	Workforce security	164.308(a)(3)(i)	Standard	---	---	---
A	Administrative Safeguards	A3.1	Authorization and/or supervision	164.308(a)(3)(ii)(A)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A3.2	Workforce clearance procedures	164.308(a)(3)(ii)(B)	Addressable Implementation Specification	1	Do procedures exist for obtaining appropriate authorization from management to grant or terminate access to EPHI for workforce members?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.2	Workforce clearance procedures	164.308(a)(3)(ii)(B)	Addressable Implementation Specification	2	Are there written job descriptions that correlate with appropriate levels of access?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.2	Workforce clearance procedures	164.308(a)(3)(ii)(B)	Addressable Implementation Specification	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?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.2	Workforce clearance procedures	164.308(a)(3)(ii)(B)	Addressable Implementation Specification	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?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.2	Workforce clearance procedures	164.308(a)(3)(ii)(B)	Addressable Implementation Specification	5	Have policies or procedures been implemented that address appropriate background screening of persons who will have access to EPHI?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.3	Termination procedures	164.308(a)(3)(ii)(C)	Addressable Implementation Specification	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?	Yes/No/No but Compliant
A	Administrative Safeguards	A3.3	Termination procedures	164.308(a)(3)(ii)(C)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A4.0	Information access management	164.308(a)(4)	Standard	---	---	---

A	Administrative Safeguards	A4.1	Isolating health care clearinghouse functions	164.308(a)(4)(ii)(A)	Required Implementation Specification	1	Does the covered entity 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.]	Yes/No
A	Administrative Safeguards	A4.1	Isolating health care clearinghouse functions	164.308(a)(4)(ii)(A)	Required Implementation Specification	2	Have steps been taken to ensure that EPHI for the clearinghouse is protected from unauthorized access by the larger organization with regards to physical security, staff security, network security and logical security?	Yes/No
A	Administrative Safeguards	A4.2	Access authorization	164.308(a)(4)(ii)(B)	Addressable Implementation Specification	1	Does the covered entity have policies and procedures for granting access to EPHI?	Yes/No/No but Compliant
A	Administrative Safeguards	A4.2	Access authorization	164.308(a)(4)(ii)(B)	Addressable Implementation Specification	2	Is the information system capable of setting the access controls specified in the policies and procedures?	Yes/No/No but Compliant
A	Administrative Safeguards	A4.2	Access authorization	164.308(a)(4)(ii)(B)	Addressable Implementation Specification	3	Select the method(s) of access control used (check all that apply): A) identity-based B) role-based C) location-based D) other	Multiple Choice
A	Administrative Safeguards	A4.3	Access establishment and modification	164.308(a)(4)(ii)(C)	Addressable Implementation Specification	1	Are duties separated such that only the minimum necessary EPHI is made available to each staff member based on job requirements?	Yes/No/No but Compliant
A	Administrative Safeguards	A4.3	Access establishment and modification	164.308(a)(4)(ii)(C)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A5.0	Security awareness and training	164.308(a)(5)(i)	Standard	1	Have all employees received adequate training to fulfill their security responsibilities?	Yes/No
A	Administrative Safeguards	A5.0	Security awareness and training	164.308(a)(5)(i)	Standard	2	Does the covered entity'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)?	Yes/No
A	Administrative Safeguards	A5.0	Security awareness and training	164.308(a)(5)(i)	Standard	3	Are employees appropriately trained on security and risks to EPHI when reusing hardware?	Yes/No
A	Administrative Safeguards	A5.0	Security awareness and training	164.308(a)(5)(i)	Standard	4	Are procedures in place to assess the effectiveness of the security awareness training program and revise the training when necessary?	Yes/No
A	Administrative Safeguards	A5.1	Security reminders	164.308(a)(5)(ii)(A)	Addressable Implementation Specification	1	Is security awareness discussed with all new hires?	Yes/No/No but Compliant
A	Administrative Safeguards	A5.1	Security reminders	164.308(a)(5)(ii)(A)	Addressable Implementation Specification	2	Are procedures in place to keep staff aware of security topics?	Yes/No/No but Compliant
A	Administrative Safeguards	A5.1	Security reminders	164.308(a)(5)(ii)(A)	Addressable Implementation Specification	2.1	What methods are used to keep staff aware of security topics (e.g., emails, staff meetings, posters, newsletters)?	Free Text Answer
A	Administrative Safeguards	A5.1	Security reminders	164.308(a)(5)(ii)(A)	Addressable Implementation Specification	3	Is security refresher training performed on a periodic basis?	Yes/No/No but Compliant
A	Administrative Safeguards	A5.2	Protection from malicious software	164.308(a)(5)(ii)(B)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A5.3	Log-in monitoring	164.308(a)(5)(ii)(C)	Addressable Implementation Specification	1	Have users been formally notified that log-in attempts may be monitored (e.g., warning screen, pop-up, written documentation)?	Yes/No/No but Compliant
A	Administrative Safeguards	A5.3	Log-in monitoring	164.308(a)(5)(ii)(C)	Addressable Implementation Specification	2	Are procedures in place for reporting login discrepancies to the proper security authority?	Yes/No/No but Compliant
A	Administrative Safeguards	A5.4	Password management	164.308(a)(5)(ii)(D)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A6.0	Security incident procedures	164.308(a)(6)(i)	Standard	---	---	---
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	1	Are there procedures in place for reporting and handling security incidents?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	2	Does the covered entity have or have access to incident response personnel or an incident response team?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	3	Has a written incident response plan been developed and provided to the appropriate personnel?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	4	Has the covered entity developed standard incident report templates, used to ensure that all necessary information related to the incident is documented and investigated?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	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?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	6	Do incident response personnel have adequate knowledge of the covered entity's hardware and software?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	7	Does the covered entity keep adequate documentation of security incidents and their outcomes, which may include what weaknesses were exploited and how access to information was gained?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	8	Has the covered entity determined reasonable and appropriate mitigation options for foreseeable security incidents?	Yes/No
A	Administrative Safeguards	A6.1	Response and reporting	164.308(a)(6)(ii)	Required Implementation Specification	9	Are procedures in place to assess the effectiveness of the incident management procedures and revise the procedures when necessary?	Yes/No
A	Administrative Safeguards	A7.0	Contingency	164.308(a)(7)(i)	Standard	1	Has a determination been made regarding when the contingency plan	Yes/No

	Safeguards		plan				needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery, etc.)?	
A	Administrative Safeguards	A7.0	Contingency plan	164.308(a)(7)(i)	Standard	2	Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one?	Yes/No
A	Administrative Safeguards	A7.0	Contingency plan	164.308(a)(7)(i)	Standard	3	Has responsibility for managing, maintaining and updating the contingency plan been assigned?	Yes/No
A	Administrative Safeguards	A7.0	Contingency plan	164.308(a)(7)(i)	Standard	3.1	Identify the individual(s):	Free Text Answer
A	Administrative Safeguards	A7.1	Data backup plan	164.308(a)(7)(ii)(A)	Required Implementation Specification	1	Have procedures for creating and maintaining retrievable exact copies of EPHI been developed, documented, and made available to the appropriate staff?	Yes/No
A	Administrative Safeguards	A7.1	Data backup plan	164.308(a)(7)(ii)(A)	Required Implementation Specification	2	Has responsibility for implementation of the procedures for creating and maintaining retrievable exact copies of EPHI been assigned?	Yes/No
A	Administrative Safeguards	A7.1	Data backup plan	164.308(a)(7)(ii)(A)	Required Implementation Specification	2.1	Identify the individual(s) or work group:	Free Text Answer
A	Administrative Safeguards	A7.2	Disaster recovery plan	164.308(a)(7)(ii)(B)	Required Implementation Specification	1	Have procedures for data restoration been developed, documented, and made available to the appropriate staff?	Yes/No
A	Administrative Safeguards	A7.2	Disaster recovery plan	164.308(a)(7)(ii)(B)	Required Implementation Specification	2	Is there a formal, written disaster recovery plan?	Yes/No
A	Administrative Safeguards	A7.3	Emergency mode operations plan	164.308(a)(7)(ii)(C)	Required Implementation Specification	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
A	Administrative Safeguards	A7.4	Testing and revision procedures	164.308(a)(7)(ii)(D)	Addressable Implementation Specification	1	Have procedures to test and revise the contingency plan been developed, documented and made available to the appropriate staff?	Yes/No/No but Compliant
A	Administrative Safeguards	A7.4	Testing and revision procedures	164.308(a)(7)(ii)(D)	Addressable Implementation Specification	1.1	Describe the testing methodology (e.g., full, phased approach, "tabletop" scenarios):	Free Text Answer
A	Administrative Safeguards	A7.4	Testing and revision procedures	164.308(a)(7)(ii)(D)	Addressable Implementation Specification	2	Is the contingency plan tested and revised periodically?	Yes/No/No but Compliant
A	Administrative Safeguards	A7.5	Applications and data criticality analysis	164.308(a)(7)(ii)(E)	Addressable Implementation Specification	1	Have the hardware, software and personnel that are critical to daily operations (including EPHI) been identified and documented?	Yes/No/No but Compliant
A	Administrative Safeguards	A7.5	Applications and data criticality analysis	164.308(a)(7)(ii)(E)	Addressable Implementation Specification	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/No but Compliant
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	1	Does the evaluation process consider all standards and implementation specifications of the HIPAA security rule?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	2	Are the appropriate technical, legal, compliance and business knowledge represented adequately in the personnel conducting the evaluation?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	3	Has the evaluation process been formally communicated to participating personnel?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	4	Does the evaluation process support development of security recommendations?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	5	Is penetration testing part of the evaluation process? [Note: This question is informational. Negative answers are not scored.]	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	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?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	7	Have steps been taken to ensure the security of any evaluation results and written reports and their availability to the appropriate personnel?	Yes/No
A	Administrative Safeguards	A8.0	Evaluation	164.308(a)(8)	Standard	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
A	Administrative Safeguards	A9.0	Business associate contracts and other arrangements	164.308(b)(1)	Standard	1	Does the covered entity have any relationships with business associates that do not fall under the exclusions listed in 164.308(b)(2)? [Note: This question is informational. Negative answers are not scored.]	Yes/No
A	Administrative Safeguards	A9.0	Business associate contracts and other arrangements	164.308(b)(1)	Standard	2	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.]	Yes/No
A	Administrative Safeguards	A9.0	Business associate contracts and other arrangements	164.308(b)(1)	Standard	3	Is the covered entity a business associate of another covered entity? [Note: This question is informational. Negative answers are not scored.]	Yes/No
A	Administrative Safeguards	A9.0	Business associate contracts and other arrangements	164.308(b)(1)	Standard	4	Is the covered entity in full compliance with the satisfactory assurances it provided as a business associate of another covered entity? (If the covered entity is in violation, answer No.)	Yes/No
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	1	Has responsibility been assigned for coordinating and preparing the final agreements or arrangements (e.g., business associate contracts)?	Yes/No
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	1.1	Identify the individual(s) or work group:	Free Text Answer
A	Administrative Safeguards	A9.1	Written contract or	164.308(b)(4)	Required Implementation	2	Do the agreements or arrangements specify how information is to be transmitted to and from business associates?	Yes/No

			other arrangement		Specification			
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	3	Have appropriate security controls been specified for the business associates?	Yes/No
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	4	Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected?	Yes/No
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	5	Is there a process in place to periodically evaluate the effectiveness of business associate security controls?	Yes/No
A	Administrative Safeguards	A9.1	Written contract or other arrangement	164.308(b)(4)	Required Implementation Specification	6	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
B	Physical Safeguards	B1.0	Facility access control	164.310(a)	Standard	---	---	---
B	Physical Safeguards	B1.1	Contingency operations	164.310(a)(2)(i)	Addressable Implementation Specification	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?	Yes/No/No but Compliant
B	Physical Safeguards	B1.1	Contingency operations	164.310(a)(2)(i)	Addressable Implementation Specification	2	Are the procedures appropriate for all types of foreseeable potential disasters (e.g., fire, flood, earthquake)?	Yes/No/No but Compliant
B	Physical Safeguards	B1.2	Facility security plan	164.310(a)(2)(ii)	Addressable Implementation Specification	1	Is there a facility/space inventory available (e.g., building name/number, room number, etc.)?	Yes/No/No but Compliant
B	Physical Safeguards	B1.2	Facility security plan	164.310(a)(2)(ii)	Addressable Implementation Specification	2	Have procedures been developed and implemented for securing the facilities?	Yes/No/No but Compliant
B	Physical Safeguards	B1.2	Facility security plan	164.310(a)(2)(ii)	Addressable Implementation Specification	2.1	Briefly describe the procedures for securing the facilities:	Free Text Answer
B	Physical Safeguards	B1.2	Facility security plan	164.310(a)(2)(ii)	Addressable Implementation Specification	3	Has an individual been assigned responsibility for facility security?	Yes/No/No but Compliant
B	Physical Safeguards	B1.2	Facility security plan	164.310(a)(2)(ii)	Addressable Implementation Specification	3.1	Identify the individual:	Free Text Answer
B	Physical Safeguards	B1.3	Access control and validation	164.310(a)(2)(iii)	Addressable Implementation Specification	1	Are there policies and procedures in place to control and validate access to facilities by staff (by role or function), contractors, and visitors?	Yes/No/No but Compliant
B	Physical Safeguards	B1.3	Access control and validation	164.310(a)(2)(iii)	Addressable Implementation Specification	2	Have all points of access to the facility been identified and are they covered by access control policies and procedures?	Yes/No/No but Compliant
B	Physical Safeguards	B1.4	Maintenance records	164.310(a)(2)(iv)	Addressable Implementation Specification	1	Are repairs and modifications to the physical components of the facility (e.g., hardware, walls, doors, locks) documented?	Yes/No/No but Compliant
B	Physical Safeguards	B1.4	Maintenance records	164.310(a)(2)(iv)	Addressable Implementation Specification	2	Are records of repairs and modifications to the physical components of the facility maintained as per applicable records retention policies?	Yes/No/No but Compliant
B	Physical Safeguards	B1.4	Maintenance records	164.310(a)(2)(iv)	Addressable Implementation Specification	3	Has responsibility for maintaining facility repair and modification records been assigned?	Yes/No/No but Compliant
B	Physical Safeguards	B1.4	Maintenance records	164.310(a)(2)(iv)	Addressable Implementation Specification	3.1	Identify the individual(s) or work group:	Free Text Answer
B	Physical Safeguards	B2.0	Workstation use	164.310(b)	Standard	1	Have policies and procedures related to the proper use of workstations been developed?	Yes/No
B	Physical Safeguards	B2.0	Workstation use	164.310(b)	Standard	2	Have policies and procedures related to mitigation of key operational risks that could result in a breach of security been developed?	Yes/No
B	Physical Safeguards	B2.0	Workstation use	164.310(b)	Standard	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
B	Physical Safeguards	B3.0	Workstation security	164.310(c)	Standard	1	Does the covered entity 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?	Yes/No
B	Physical Safeguards	B3.0	Workstation security	164.310(c)	Standard	1.1	Identify the person(s) responsible for this inventory and its maintenance:	Free Text Answer
B	Physical Safeguards	B3.0	Workstation security	164.310(c)	Standard	2	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?	Yes/No
B	Physical Safeguards	B3.0	Workstation security	164.310(c)	Standard	2.1	Briefly describe the physical security measures that have been taken to protect workstations:	Free Text Answer
B	Physical Safeguards	B4.0	Device and media controls	164.310(d)(1)	Standard	---	---	---
B	Physical Safeguards	B4.1	Disposal	164.310(d)(2)(i)	Required Implementation Specification	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.)	Yes/No
B	Physical Safeguards	B4.1	Disposal	164.310(d)(2)(i)	Required Implementation Specification	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
B	Physical Safeguards	B4.2	Media re-use	164.310(d)(2)(ii)	Required Implementation Specification	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
B	Physical Safeguards	B4.3	Accountability	164.310(d)(2)(iii)	Addressable	1	Has one entity (individual, department, team, etc.) been assigned	Yes/No/No

	Safeguards				Implementation Specification		responsibility for coordinating the disposal of data and the re-use of hardware?	but Compliant
B	Physical Safeguards	B4.3	Accountability	164.310(d)(2)(iii)	Addressable Implementation Specification	1.1	Identify the entity:	Free Text Answer
B	Physical Safeguards	B4.3	Accountability	164.310(d)(2)(iii)	Addressable Implementation Specification	2	Does the covered entity have procedures to accurately track the movement of hardware and electronic media within the organization and/or facility?	Yes/No/No but Compliant
B	Physical Safeguards	B4.3	Accountability	164.310(d)(2)(iii)	Addressable Implementation Specification	3	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/No but Compliant
B	Physical Safeguards	B4.4	Data backup and storage	164.310(d)(2)(iv)	Addressable Implementation Specification	1	Do procedures exist to create a retrievable, exact copy of EPHI prior to relocating equipment?	Yes/No/No but Compliant
B	Physical Safeguards	B4.4	Data backup and storage	164.310(d)(2)(iv)	Addressable Implementation Specification	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/No but Compliant
C	Technical Safeguards	C1.0	Access control	164.312(a)(1)	Standard	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 covered entity?	Yes/No
C	Technical Safeguards	C1.0	Access control	164.312(a)(1)	Standard	2	Does the covered entity have documented access control procedures?	Yes/No
C	Technical Safeguards	C1.0	Access control	164.312(a)(1)	Standard	3	Have new employees and/or users of systems that utilize EPHI been given proper instructions for protecting data and systems?	Yes/No
C	Technical Safeguards	C1.0	Access control	164.312(a)(1)	Standard	4	Are there procedures for new employee/user access to data and systems?	Yes/No
C	Technical Safeguards	C1.0	Access control	164.312(a)(1)	Standard	5	Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users?	Yes/No
C	Technical Safeguards	C1.1	Unique user identification	164.312(a)(2)(i)	Required Implementation Specification	1	Are all users of systems that access EPHI assigned a unique name and/or number for recording and tracking user identity?	Yes/No
C	Technical Safeguards	C1.1	Unique user identification	164.312(a)(2)(i)	Required Implementation Specification	2	Can system activity be traced to a specific user?	Yes/No
C	Technical Safeguards	C1.1	Unique user identification	164.312(a)(2)(i)	Required Implementation Specification	3	Is there sufficient data in system and/or application logs to support audit and other related business functions?	Yes/No
C	Technical Safeguards	C1.2	Emergency access procedure	164.312(a)(2)(ii)	Required Implementation Specification	1	Have procedures been established for obtaining necessary EPHI during an emergency?	Yes/No
C	Technical Safeguards	C1.2	Emergency access procedure	164.312(a)(2)(ii)	Required Implementation Specification	2	Have individuals been identified and assigned authorization to activate emergency EPHI access procedures?	Yes/No
C	Technical Safeguards	C1.2	Emergency access procedure	164.312(a)(2)(ii)	Required Implementation Specification	2.1	Identify the individuals:	Free Text Answer
C	Technical Safeguards	C1.2	Emergency access procedure	164.312(a)(2)(ii)	Required Implementation Specification	3	Have the emergency EPHI procedures been tested and found to be adequate?	Yes/No
C	Technical Safeguards	C1.2	Emergency access procedure	164.312(a)(2)(ii)	Required Implementation Specification	4	Have criteria for activation of the emergency EPHI access procedures been identified?	Yes/No
C	Technical Safeguards	C1.3	Automatic logoff	164.312(a)(2)(iii)	Addressable Implementation Specification	1	Are automatic logoff features available for the covered entity's operating systems and/or other major applications?	Yes/No/No but Compliant
C	Technical Safeguards	C1.3	Automatic logoff	164.312(a)(2)(iii)	Addressable Implementation Specification	2	Have automatic logoff features been implemented?	Yes/No/No but Compliant
C	Technical Safeguards	C1.3	Automatic logoff	164.312(a)(2)(iii)	Addressable Implementation Specification	2.1	What period of inactivity (number of minutes) prior to automatic logoff is being used?	Free Text Answer
C	Technical Safeguards	C1.4	Encryption and decryption	164.312(a)(2)(iv)	Addressable Implementation Specification	1	Is EPHI encrypted during transmission?	Yes/No/No but Compliant
C	Technical Safeguards	C1.4	Encryption and decryption	164.312(a)(2)(iv)	Addressable Implementation Specification	1.1	What type of encryption is used to protect EPHI during transmission?	Free Text Answer
C	Technical Safeguards	C1.4	Encryption and decryption	164.312(a)(2)(iv)	Addressable Implementation Specification	2	Is EPHI encrypted when being stored and maintained?	Yes/No/No but Compliant
C	Technical Safeguards	C1.4	Encryption and decryption	164.312(a)(2)(iv)	Addressable Implementation Specification	2.1	What type of encryption is used to protect EPHI while it is being stored and maintained?	Free Text Answer
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	1	Are system activity audits conducted on systems that contain or use EPHI and the results analyzed periodically?	Yes/No
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	1.1	How often are system activity audits conducted and the results analyzed?	Free Text Answer
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	1.2	What auditing and system activity tools are in place?	Free Text Answer
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	2	Has an individual been assigned responsibility for the overall audit process and results?	Yes/No
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	2.1	Identify the individual:	Free Text Answer
C	Technical Safeguards	C2.0	Audit controls	164.312(b)	Standard	3	Have mechanisms been implemented to assess the effectiveness of the audit process (metrics) and revise it if necessary?	Yes/No
C	Technical Safeguards	C3.0	Integrity	164.312(c)(1)	Standard	1	Have the integrity requirements been documented?	Yes/No
C	Technical Safeguards	C3.0	Integrity	164.312(c)(1)	Standard	2	Has a written policy been developed and communicated to system users?	Yes/No
C	Technical Safeguards	C3.0	Integrity	164.312(c)(1)	Standard	3	Are implemented audit, logging, and access control techniques sufficient to address the integrity of the information?	Yes/No
C	Technical Safeguards	C3.1	Mechanism to authenticate electronic protected	164.312(c)(2)	Addressable Implementation Specification	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/No but Compliant

			health information					
C	Technical Safeguards	C4.0	Person or entity authentication	164.312(d)	Standard	1	Has the appropriate level of authentication (single-factor or multi-factor) been determined based on risk assessment?	Yes/No
C	Technical Safeguards	C4.0	Person or entity authentication	164.312(d)	Standard	2	Is the determined level of authentication being used?	Yes/No
C	Technical Safeguards	C4.0	Person or entity authentication	164.312(d)	Standard	3	Have formal authentication policy and procedures been established and communicated?	Yes/No
C	Technical Safeguards	C4.0	Person or entity authentication	164.312(d)	Standard	4	Do the authentication procedures include ongoing system maintenance and updates?	Yes/No
C	Technical Safeguards	C4.0	Person or entity authentication	164.312(d)	Standard	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
C	Technical Safeguards	C5.0	Transmission security	164.312(e)(1)	Standard	---	---	---
C	Technical Safeguards	C5.1	Integrity controls	164.312(e)(2)(i)	Addressable Implementation Specification	1	Have measures been implemented that protect the integrity of the EPHI during transmission?	Yes/No/No but Compliant
C	Technical Safeguards	C5.1	Integrity controls	164.312(e)(2)(i)	Addressable Implementation Specification	1.1	What measures exist to protect EPHI in transmission?	Free Text Answer
C	Technical Safeguards	C5.1	Integrity controls	164.312(e)(2)(i)	Addressable Implementation Specification	2	Is there assurance that information is not altered during transmission?	Yes/No/No but Compliant
C	Technical Safeguards	C5.1	Integrity controls	164.312(e)(2)(i)	Addressable Implementation Specification	3	Is there an auditing process in place to verify that EPHI has been protected against unauthorized access during transmission?	Yes/No/No but Compliant
C	Technical Safeguards	C5.2	Encryption	164.312(e)(2)(ii)	Addressable Implementation Specification	1	Is encryption reasonable and appropriate for EPHI in transmission or needed to effectively protect the information in transmission? [Note: This question is informational. Negative answers are not scored.]	Yes/No
C	Technical Safeguards	C5.2	Encryption	164.312(e)(2)(ii)	Addressable Implementation Specification	2	Is encryption utilized in order to protect EPHI during transmission?	Yes/No/No but Compliant
C	Technical Safeguards	C5.2	Encryption	164.312(e)(2)(ii)	Addressable Implementation Specification	3	Does the covered entity have the appropriate staff to adequately maintain a process for encrypting EPHI during transmission?	Yes/No/No but Compliant
D	Organizational Requirements	D1.0	Business associate contracts	164.314(a)(2)(i)	Required Implementation Specification	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?	Yes/No
D	Organizational Requirements	D1.0	Business associate contracts	164.314(a)(2)(i)	Required Implementation Specification	2	Do the written agreements address the issue of EPHI access by subcontractors and other agents of the business associates?	Yes/No
D	Organizational Requirements	D1.0	Business associate contracts	164.314(a)(2)(i)	Required Implementation Specification	3	Is there a procedure in place for reporting of incidents by business associates?	Yes/No
D	Organizational Requirements	D1.0	Business associate contracts	164.314(a)(2)(i)	Required Implementation Specification	4	Have key business associate staff that would be the point(s) of contact in the event of a security incident been identified?	Yes/No
D	Organizational Requirements	D1.0	Business associate contracts	164.314(a)(2)(i)	Required Implementation Specification	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 which require the removal of such language)?	Yes/No
D	Organizational Requirements	D1.1	Other arrangements	164.314(a)(2)(ii)	Required Implementation Specification	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?	Yes/No
D	Organizational Requirements	D1.1	Other arrangements	164.314(a)(2)(ii)	Required Implementation Specification	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?	Yes/No
D	Organizational Requirements	D1.1	Other arrangements	164.314(a)(2)(ii)	Required Implementation Specification	3	Has the covered entity made a good faith attempt to obtain satisfactory assurances that the security standards required by this section are being met?	Yes/No
D	Organizational Requirements	D1.1	Other arrangements	164.314(a)(2)(ii)	Required Implementation Specification	4	Are attempts to obtain satisfactory assurances and the reasons assurances cannot be obtained, if applicable, documented?	Yes/No
D	Organizational Requirements	D2.0	Requirements for group health plans	164.314(b)(1)	Standard	---	---	---
D	Organizational Requirements	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	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.]	Yes/No
D	Organizational Requirements	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	2	Do the plan documents require the plan sponsor to reasonably and appropriately safeguard EPHI?	Yes/No

D	Organizational Requirements	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	3	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?	Yes/No
D	Organizational Requirements	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	4	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?	Yes/No
D	Organizational Requirements	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	5	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
E	Policies, Procedures and Documentation	E1.0	Policies and procedures	164.316(a)	Standard	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?	Yes/No
E	Policies, Procedures and Documentation	E1.0	Policies and procedures	164.316(a)	Standard	2	Do procedures exist for periodically re-evaluating the policies and procedures, updating them as necessary?	Yes/No
E	Policies, Procedures and Documentation	E1.0	Policies and procedures	164.316(a)	Standard	3	As policies and procedures are changed, are new versions made available and are workforce members appropriately informed?	Yes/No
E	Policies, Procedures and Documentation	E2.0	Documentation	164.316(b)(1)	Standard	1	Are all required policies and procedures documented?	Yes/No
E	Policies, Procedures and Documentation	E2.0	Documentation	164.316(b)(1)	Standard	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?	Yes/No
E	Policies, Procedures and Documentation	E2.0	Documentation	164.316(b)(1)	Standard	3	Has an individual been assigned responsibility for maintaining the HIPAA Security Rule documentation?	Yes/No
E	Policies, Procedures and Documentation	E2.0	Documentation	164.316(b)(1)	Standard	3.1	Identify the individual(s):	Free Text Answer
E	Policies, Procedures and Documentation	E2.1	Time limit	164.316(b)(2)(i)	Required Implementation Specification	1	Have documentation retention requirements under HIPAA been aligned with the covered entity's other data retention policies?	Yes/No
E	Policies, Procedures and Documentation	E2.2	Availability	164.316(b)(2)(ii)	Required Implementation Specification	1	Is the location of documentation known to all staff that need to access it?	Yes/No
E	Policies, Procedures and Documentation	E2.2	Availability	164.316(b)(2)(ii)	Required Implementation Specification	2	Is availability of the documentation made known as part of education, training and awareness activities?	Yes/No
E	Policies, Procedures and Documentation	E2.3	Updates	164.316(b)(2)(iii)	Required Implementation Specification	1	Is there a version control procedure that allows verification of the timeliness of policies and procedures, if reasonable and appropriate?	Yes/No
E	Policies, Procedures and Documentation	E2.3	Updates	164.316(b)(2)(iii)	Required Implementation Specification	2	Is there a process for soliciting input into updates of policies and procedures from staff, if reasonable and appropriate?	Yes/No