## HIPAA

### Administrative Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.308(a)(1)(i)** Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | | | |
| **164.308(a)(1)(i)** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **164.308(a)(1)(ii)(A)** Risk Analysis (R): 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 covered entity. | | | |
| **164.308(a)(1)(ii)(A)** Verify that an annual risk assessment process is documented that identifies assets, threats, vulnerabilities, and results in a formal risk assessment. | **Describe how** it was verified that an annual risk-assessment process is documented that: | |  |
| * Identifies critical assets, threats and vulnerabilities. |  |
| * Results in formal, documented analysis of risk. |  |
| **164.308(a)(1)(ii)(B)** Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | | | |
| **164.308(a)(1)(ii)(B)** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | * **Identify** the risk assessment result documentation reviewed to verify that: * The risk assessment process is performed at least annually. * The risk assessment is performed upon significant changes to the environment. * The documented risk assessment process was followed. |  |  |
| **164.308(a)(1)(ii)(C)** Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | | | |
| **164.308(a)(1)(ii)(C)** Inquire with Human Resource department management and verify that employees are sanctioned when they violate security policies. | **Identify** the Human Resources personnel interviewed who confirm that employees are sanctioned when they violate security policies. |  |  |
| **164.308(a)(1)(ii)(D)** Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | | | |
| **164.308(a)(1)(ii)(D).a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | * **Identify** the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| Describe the manual or log tools used for daily review of logs. |  |
| **164.308(a)(1)(ii)(D).b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | * **Identify** the personnel interviewed who confirm that the following are reviewed at least daily: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | |
| All security events. |  |
| Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. |  |
| Logs of all critical system components. |  |
| Logs of all servers and system components that perform security functions. |  |
| **164.308(a)(2)** Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | | | |
| **164.308(a)(2)** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | * Provide the name of the assessor who attests that responsibilities were verified to be formally assigned for: * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  |  |
| **164.308(a)(3)(i)** Workforce Security: 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, 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. | | | |
| **164.308(a)(3)(i)** Examine written policy for access control, and verify that the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | * **Identify** the written policy for access control that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows: * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **164.308(a)(3)(ii)(A)** Authorization and/or Supervision (A): 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. | | | |
| **164.308(a)(3)(ii)(A)** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | * **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **164.308(a)(3)(ii)(B)** Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | | | |
| **164.308(a)(3)(ii)(B)** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | * **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| * **Identify** the responsible management personnel interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  |
| * For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are based on an individual’s job classification and function. |  |
| **164.308(a)(3)(ii)(C)** Termination Procedure (A): 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. | | | |
| **164.308(a)(3)(ii)(C).a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** the sample of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **164.308(a)(3)(ii)(C).b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  |  |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  |
| **164.308(a)(4)(i)** Information Access Management: 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. | | | |
| **164.308(a)(4)(i)** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | * **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **164.308(a)(4)(ii)(A)** Isolating Healthcare Clearinghouse Functions (R): If a healthcare 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. | | | |
| **164.308(a)(4)(ii)(A)** | **Identify** whether the organization is a healthcare clearinghouse that is part of a larger organization. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 164.308(a)(4)(ii)(A) as “Not Applicable”*  *If “yes,” complete the following:* | | |
| **Identify** the policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. |  |  |
| **164.308(a)(4)(ii)(C)** Access Establishment and Modification (A): 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. | | | |
| **164.308(a)(4)(ii)(C)** Confirm that access control systems are in place on all system components. | **Identify** vendor documentation examined. |  |  |
| **Describe how** system settings were examined with the vendor documentation to verify that access control systems are in place on all system components. |  |  |
| **164.308(a)(5)(i)** Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management). | | | |
| **164.308(a)(5)(i)** Review the security awareness training documentation to verify it provides awareness to all personnel about the importance of protecting customer information. | **Identify** the documented security awareness training documentation reviewed to verify it includes at least the following topics:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| **164.308(a)(5)(ii)(A)** Security Reminders (A): Periodic security updates. | | | |
| **164.308(a)(5)(ii)(A)** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **164.308(a)(5)(ii)(B)** Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software. | | | |
| **164.308(a)(5)(ii)(B).a** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  |  |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  |
| **164.308(a)(5)(ii)(B).b** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | * **Identify** the vendor documentation reviewed to verify that anti-virus programs: * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| Detect all known types of malicious software, |  |
| Remove all known types of malicious software, and |  |
| Protect against all known types of malicious software. |  |
| **164.308(a)(5)(ii)(B).c** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are Configured to perform automatic updates. |  |  |
| **164.308(a)(5)(ii)(C)** Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies. | | | |
| **164.308(a)(5)(ii)(C).a** Verify access to all audit trails is logged. | For all items in the sample, **describe how** configuration settings were observed to verify access to all audit trails is logged. |  |  |
| **164.308(a)(5)(ii)(C).b** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** the documented security policies and procedures examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  |  |
| **164.308(a)(5)(ii)(C).c** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  |  |
| **Identify** the personnel interviewed who confirm that follow-up to exceptions and anomalies is performed. |  |
| **164.308(a)(5)(ii)(D)** Password Management (A): Procedures for creating, changing, and safeguarding passwords. | | | |
| **164.308(a)(5)(ii)(D).a** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | **Identify** the documented password procedures examined to verify the procedures define that:   * First-time passwords must be set to a unique value for each user. * First-time passwords must be changed after the first use. * Reset passwords must be set to a unique value for each user. * Reset passwords must be changed after the first use. |  |  |
| **Describe how** security personnel were observed to: | |
| * Set first-time passwords to a unique value for each new user. |  |
| * Set first-time passwords to be changed after first use. |  |
| * Set reset passwords to a unique value for each existing user. |  |
| * Set reset passwords to be changed after first use. |  |
| **164.308(a)(5)(ii)(D).b** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify t**he document examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |  |
| **Describe** the non-face-to-face methods used for requesting password resets. |  |
| **Describe how** security personnel were observed to verify that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |
| **164.308(a)(6)(i)** Security Incident Procedures: Implement policies and procedures to address security incidents. | | | |
| **164.308(a)(6)(i)** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach. | **Identify** the documented incident response plan and related procedures examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts:   24/7 incident monitoring  24/7 incident response   * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  |  |
| **164.308(a)(6)(ii)** Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | | | |
| **164.308(a)(6)(ii).a** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |  |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |
| **164.308(a)(6)(ii).b** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify** the documented policy reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify** the sample of responsible personnel interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **164.308(a)(7)(i)** Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | | | |
| **164.308(a)(7)(i)** Examine the contingency plan and related procedures to verify entity is prepared to respond immediately to an emergency. | **Identify** the documented contingency plan and related procedures examined to verify the entity is prepared to respond immediately to an emergency. |  |  |
| **164.308(a)(7)(ii)(A)** Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | | | |
| **164.308(a)(7)(ii)(A)** Examine the data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. | **Identify** the documented data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. |  |  |
| **164.308(a)(7)(ii)(B)** Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. | | | |
| **164.308(a)(7)(ii)(B)** Examine the disaster recovery plan and related procedures to verify entity is able to restore any loss of data. | **Identify** the documented disaster recovery plan and related procedures to verify entity is able to restore any loss of data. |  |  |
| **164.308(a)(7)(ii)(C)** Emergency Mode Operation Plan (R): 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. | | | |
| **164.308(a)(7)(ii)(C)** Examine the emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **Identify** the documented emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. |  |  |
| **164.308(a)(7)(ii)(D)** Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. | | | |
| **164.308(a)(7)(ii)(D)** Examine the contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. | **Identify** the documented contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. |  |  |
| **164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. | | | |
| **164.308(a)(7)(ii)(E)** Examine the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. | **Identify** the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. |  |  |
| **164.308(a)(8)** Evaluation: 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. | | | |
| **164.308(a)(8)** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Identify** the document reviewed to verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  |  |
| **Describe how** the information security policy was verified to be: | |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **164.308(b)(1)** Business Associate Contracts and Other Arrangements: 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 Sec. 164.314(a), that the business associate will appropriately safeguard the information. | | | |
| **164.308(b)(1)** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented. |  |  |
| **164.308(b)(4)** Written Contract or Other Arrangement (R): 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). | | | |
| **164.308(b)(4)** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of customer data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s network, applications or systems. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer data, or manages the customer's network, applications or systems on behalf of a customer. |  |  |

### Physical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.310(a)(1)** Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | | | |
| **164.310(a)(1)** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. | **Identify and briefly describe** all of the storage areas containing protected health information: | |  |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **164.310(a)(2)(i)** Contingency Operations (A): 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. | | | |
| **164.310(a)(2)(i)** Examine the disaster recovery plan and/or emergency mode operation plan and related 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. | **Identify** the documented disaster recovery plan and/or emergency mode operation plan and related 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. |  |  |
| **164.310(a)(2)(ii)** Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | | | |
| **164.310(a)(2)(ii)** Examine the facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. | **Identify** the documented facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. |  |  |
| **164.310(a)(2)(iii)** Access Control and Validation Procedures (A): 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. | | | |
| **164.310(a)(2)(iii).a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** the documented processes reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **164.310(a)(2)(iii).b** Observe processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and   It is easy to distinguish between onsite personnel and visitors. | **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | |  |
| * Visitors are clearly identified, and |  |
| * It is easy to distinguish between onsite personnel and visitors. |  |
| **164.310(a)(2)(iv)** Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | | | |
| **164.310(a)(2)(iv)** Review documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | **Identify** the documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |  |  |
| **164.310(b)** Workstation Use: 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. | | | |
| **164.310(b)** Review documented 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. | **Identify** the documented 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. |  |  |
| **164.310(c)** Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users. | | | |
| **164.310(c)** Verify that all workstations that access electronic protected health information are located in areas restricted authorized users. | **Describe how** it was observed that all workstations that access electronic protected health information are located in areas restricted authorized users. |  |  |
| **164.310(d)(1)** Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | | | |
| **164.310(d)(1)** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** the documented policy to control distribution of media that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  |
| **Describe how** media distribution is controlled, including distribution to individuals. |  |
| **164.310(d)(2)(i)** Disposal (R): 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. | | | |
| **164.310(d)(2)(i)** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media. | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  |  |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify** the industry-accepted standards used. |  |
| **164.310(d)(2)(ii)** Media Reuse (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | | | |
| **164.310(d)(2)(ii)** Verify that cardholder data on electronic media is removed before the media are made available for reuse. | **Identify** the procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. |  |  |
| **164.310(d)(2)(iii)** Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | | | |
| **164.310(d)(2)(iii)** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** responsible personnel interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| *For each item in the sample above,* **describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |
| **164.310(d)(2)(iv)** Data Backup and Storage (A): Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment. | | | |
| **164.310(d)(2)(iv)** Verify that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. | **Identify** responsible personnel interviewed who confirm that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. |  |  |

### Technical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.312(a)(1)** Access Control: 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). | | | |
| **164.312(a)(1)** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings were examined to verify that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  |  |
| **164.312(a)(2)(i)** Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. | | | |
| **164.312(a)(2)(i)** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** the responsible administrative personnel interviewed for this testing procedure. |  |  |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or cardholder data. |  |
| **164.312(a)(2)(ii)** Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | | | |
| **164.312(a)(2)(ii)** Review documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. | **Identify** the documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. |  |  |
| **164.312(a)(2)(iii)** Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | | | |
| **164.312(a)(2)(iii)** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** the sample of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  |
| **164.312(a)(2)(iv)** Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | | | |
| **164.312(a)(2)(iv)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** the documentation about the system used to protect the electronic protected health information examined. |  |  |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the electronic protected health information. |  |
| **164.312(b)** Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | | | |
| **164.312(b)** Implement audit trails to link all access to system components to each individual user. | Identify the system administrator(s) interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  |  |
| **Describe how** audit trails were observed to verify the following: | |
| * Audit trails are enabled and active for system components. |  |
| * Access to system components is linked to individual users. |  |
| **164.312(c)(1)** Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | | | |
| **164.312(c)(1)** Implement controls to protect electronic protected health information from improper alteration or destruction. | Identify the system administrator(s) interviewed who confirm that controls have been implemented which protect electronic protected health information from improper alteration or destruction. |  |  |
| **164.312(c)(2)** Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | | | |
| **164.312(c)(2)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(d)** Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | | | |
| **164.312(d)** Review procedures and confirm they define processes for verifying that a person or entity seeking access to electronic protected health information is the one claimed. | **Identify** the written procedures for user identification management examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or electronic protected health information data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **164.312(e)(1)** Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | | | |
| **164.312(e)(1).a** Identify all locations where electronic protected health information is transmitted or received over open, public networks. Examine system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where electronic protected health information is transmitted or received over open, public networks. |  |  |
| **164.312(e)(1).b** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all electronic protected health information is encrypted with strong cryptography during transit. | **Describe** the sample of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all electronic protected health information is encrypted with strong cryptography during transit. |  |
| **164.312(e)(2)(i)** Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | | | |
| **164.312(e)(2)(i)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(e)(2)(ii)** Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | | | |
| **164.312(e)(2)(ii)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** the documentation about the system used to protect the electronic protected health information examined. |  |  |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the electronic protected health information. |  |