| IDN §162 | Description | Passed/Failed |
|---|---|---|
| §162 401 | NPI Issued:<br>Ensure the confidentiality, integrity, and availability of all electronic protected health information. | |
| §162 410 (a) | NPI Provided (National Provider Identifier) | |
| §162 504 | HPID Issued (#######) | |
| §162 605 | EIN Issued (##-#######) | |
| §162 930 | Compliant HCC<br>Receive a standard transaction on behalf of the covered entity and translate it into a nonstandard transaction.<br>Receive a nonstandard transaction from the covered entity and translate it into a standard transaction for transmission on behalf of the covered entity. | |
| §162* | Dedicated Privacy Official | |

| IDN §164 | Description | Passed/Failed |
|---|---|---|
| §164 306 (a) | Reasonable Security Precautions<br>Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates,receives, maintains, or transmits. | |
| §164 306 (b) | Flexibility of approach<br>Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation | |
| §164 308.1 (a) | Risk analysis in the last 12 mo.<br>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 or business associate. | |
| §164 308.1 (b) | Compliant risk managemet<br>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). | |
| §164 308.1 (c) | Sanction Policy<br>Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. | |
| §164 308.1 (d) | ISMS deployed + sys. review<br>Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | |
| §164 308.3 | Workforce security<br>Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information | |
| §164 308.3 (a) a | Workforce authorization<br>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. | |
| §164 308.3 (b) a | Workforce clearence<br>Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | |
| §164 308.4 | Compliant access management<br>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. | |
| §164 308.4 (a) | HCC Isolation<br>If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | |
| §164 308.4 (b) | Endpoint access authorization<br>Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | |
| §164 308.5 | Security awareness/training<br>Implement a security awareness and training program for all members of its workforce (including management). | |
| §164 308.5 (a) a | Recurring security reminders<br>Periodic security updates. | |

| IDN §164 | Description | Passed/Failed |
|---|---|---|
| §164 308.5 (b) a | Reasonable malware protection<br>Procedures for guarding against, detecting, and reporting malicious software. | |
| §164 308.5 (c) | Endpoint access monitoring<br>Procedures for monitoring log-in attempts and reporting discrepancies. | |
| §164 308.5 (d) a | Password management system<br>Procedures for creating, changing, and safeguarding passwords. | |
| §164 308.6 | Threat detection + reporting<br>Implement policies and procedures to address security incidents. | |
| §164 308.7 | Contingency plan established<br>Establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information. | |
| §164 308.7 (a) | Data backup plan<br>Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | |
| §164 308.7 (b) | Disaster recovery plan<br>Establish procedures to restore any loss of data. | |
| §164 308.7 (c) | Emergency operation plan<br>Establish procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | |
| §164 308.7 (d) a | Recurring emergency testing<br>Implement procedures for periodic testing and revision of contingency plans. | |
| §164 308.7 (e) a | Data criticality assessment<br>Assess the relative criticality of specific applications and data in support of other contingency plan components. | |
| §164 308.8 | Periodic security auditing proc.<br>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 a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. | |
| §164 310 (a1) | Physical access controls<br>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 (ai) a | Physical contingency operations<br>Establish 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 (aii) a | Facility security plans<br>Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | |

| IDN §164 | Description | Passed/Failed |
|---|---|---|
| §164 310 (aiii) a | Role based fcility access control<br>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 (aiv) a | Written maintenance records<br>Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security | |
| §164 310 (b) | Designated workstation usage<br>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 (c) | Physical workstation safeguards<br>Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | |
| §164 310 (d) | Device and media control<br>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 (di) | Media disposal procedures<br>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 (dii) | Media reuse procedures<br>Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | |
| §164 310 (diii) a | Physical media chain of custody<br>Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | |
| §164 310 (div) a | Media backup system<br>Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | |
| §164 312 (a) | Access control for ePHI<br>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 (ai) | Unique user idenfitication<br>Assign a unique name and/or number for identifying and tracking user identity. | |
| §164 312 (aii) | Emergency access procedure<br>Establish procedures for obtaining necessary electronic protected health information during an emergency. | |
| §164 312 (aiii) | Automatic logoff<br>Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | |
| §164 312 (aiv) | Encryption of ePHI<br>Implement a mechanism to encrypt and decrypt electronic protected health information. | |

| IDN §164 | Description | Passed/Failed |
|---|---|---|
| §164 312 (b) | Information monitoring system<br>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 (c) | Data integrity assurance<br>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | |
| §164 312 (d) | User authentication<br>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | |
| §164 312 (e) | Transmission security<br>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 (ei) a | Transmission Integrity controls<br>Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | |
| §164 312 (eii) a | Transmission encryption<br>Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | |
| §164 314 | Business associate contracts<br>The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable. | |
| §164 316 | Sufficient compliance policies<br>Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). | |
| §164 * | Physical PHI Secured | |

| IDN §162 & §164 | Description | Passed/Failed |
|---|---|---|
| S1 | Externally accessible ePHI | |
| S2 | Externally accessible endpoints | |
| S3 | Internally insecured endpoints | |
| S4 | end-to-end PCI encryption | |
| S5 | Internal vulnerability scan | |
| S6 | Secure wifi networks | |
| S7 | Isolated public WAN | |
| S8 | Secured LAN Access | |
| S9 | Private data in unintended areas | |

| IDN §164 | Description | Passed/Failed |
|---|---|---|
| ps1 | Physicaly secure PHI | |
| ps2 | All endpoints secured | |
| ps3 | Client facing ePHI display | |
| ps4 | Entryways secured | |
| ps5 | Compliant CCTV (If applicable) | |
| ps6 | Patient accessible EP logging | |