APPENDIX PR 10-A

# HIPAA Security Standards Matrix

| ADMINISTRATIVE SAFEGUARDS | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.308(a)(1) | Security Management Process | 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 (PHI) held by the covered entity. |
| | | 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), which requires covered entities to ensure the confidentiality, integrity, and availability of ePHI; protect against reasonably anticipated threats to its security or integrity; and protect against reasonably anticipated unlawful uses or disclosures. |
| | | Sanction policy | R | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. |
| | | 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. |
| 45 C.F.R. Section 164.308(a)(2) | Assigned Security Responsibility | Security Official | R | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. |

| ADMINISTRATIVE SAFEGUARDS (Cont.) | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.308(a)(3) | Workforce security | Authorization and/or supervision | A | Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed. |
| | | Workforce clearance procedure | A | Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate. |
| | | Termination procedure | A | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in the workforce clearance procedures. |
| 45 C.F.R. Section 164.308(a)(4) | Information access management | Isolating health care clearinghouse function | R | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization. |
| | | Access authorization | A | Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism. |
| | | 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. |
| 45 C.F.R. Section 164.308(a)(5) | Security awareness and training | Security reminders | A | Periodic security updates. |
| | | Protection from malicious software | A | Procedures for guarding against, detecting, and reporting malicious software. |
| | | Log-in monitoring | A | Procedures for monitoring log-in attempts and reporting discrepancies. |
| | | Password management | A | Procedures for creating, changing, and safeguarding passwords. |

| ADMINISTRATIVE SAFEGUARDS (Cont.) | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.308(a)(6) | Security incident procedures | 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. |
| 45 C.F.R. Section 164.308(a)(7) | Contingency plan | Data back-up plan | R | Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI. |
| | | Disaster recovery plan | R | Establish (and implement as needed) procedures to restore any loss of data. |
| | | 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 PHI while operating in emergency mode. |
| | | Testing and revision procedure | A | Implement procedures for periodic testing and revision of contingency plans. |
| | | Applications and data criticality analysis | A | Assess the relative criticality of specific applications and data in support of other contingency plan components. |
| 45 C.F.R. Section 164.308(a)(8) | Evaluation | Technical and nontechnical evaluation | R | 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 PHI, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet HIPAA requirements. |
| 45 C.F.R. Section 164.308(b)(1) | Business associate contracts and other arrangements | Written contract or other arrangement | R | Document that a covered entity has received satisfactory assurances that a business associate will appropriately safeguard PHI through a written contract or other arrangement with the business associate that meets HIPAA business associate requirements *(see chapter 11 regarding business associate requirements)*. |

| Physical Safeguards | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.310(a)(1) | Facility access controls | 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. |
| | | Facility security plan | A | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. |
| | | 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. |
| | | 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). |
| 45 C.F.R. Section 164.310(b) | Workstation use | Function and attributes | R | 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 PHI. |
| 45 C.F.R. Section 164.310(c) | Workstation security | Restrict access | R | Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users. |

| Physical Safeguards (Cont.) | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.310(d)(1) | Device and media controls | Disposal | R | Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored. |
| | | Media re-use | R | Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. |
| | | Accountability | A | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. |
| | | Data back-up and storage | A | Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment. |

| Technical Safeguards | | | | |
|---|---|---|---|---|
| **Section** | **Standards** | **Implementation Specification R = Required, A = Addressable** | | **Description** |
| 45 C.F.R. Section 164.312(a)(1) | Access control | Unique user identification | R | Assign a unique name and/or number for identifying and tracking user identity. |
| | | Emergency access procedure | R | Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency. |
| | | Automatic log-off | A | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. |
| | | Encryption and decryption | A | Implement a mechanism to encrypt and decrypt electronic PHI. |
| 45 C.F.R. Section 164.312(b) | Audit controls | | R | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. |
| 45 C.F.R. Section 164.312(c) | Integrity | Mechanism to authenticate electronic protected health information | A | Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner. |
| 45 C.F.R. Section 164.312(d) | Person or entity authentication | | R | Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. |
| 45 C.F.R. Section 164.312(e)(1) | Transmission security | Integrity controls | A | Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of. |
| | | Encryption | A | Implement a mechanism to encrypt electronic PHI whenever deemed appropriate. |