AHCCCS Security Rule Compliance Summary Checklist

Security Management Process - Implement policies and procedures to prevent, detect, contain, and correct security violations.

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.

Workforce Security - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.

Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements .

Security Awareness and Training - Implement a security awareness and training program for all members of its workforce (including management).

Security Incident Procedures - Implement policies and procedures to address security incidents.

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.

Evaluation - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented 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.

Business Associate Contracts - A covered entity 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 that the business associate will appropriately safeguard the information.

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.

Workstation Use - Implement polices 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.

Workstation Security - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

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.

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.

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.

Integrity - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Person or Entity Authentication - Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

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.