SALT LAKE COUNTY
HIPAA SECURITY CHECKLIST

The HIPAA Security Checklist documents agency status regarding compliance with the HIPAA Security Rule Standards. Please complete the following information:

Agency name: _____
Agency address: _____
Contact info (employee name/phone/email): _____
_____

Part 1

Required Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Security mgmt process	Administrative	Risk analysis				
Security mgmt process	Administrative	Risk management				
Security mgmt process	Administrative	Sanction policy				
Security mgmt process	Administrative	Info system activity review				
Assigned Security Responsibility	Administrative					
Information Access mngmt	Administrative	Isolating Health care clearinghouse function				*This function is for health care clearinghouses only; do not fill out.

Required Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Security incident procedures	Administrative	Response and reporting				
Contingency Plan	Administrative	Data backup plan				
Contingency Plan	Administrative	Disaster recovery plan				
Contingency Plan	Administrative	Emergency mode operation plan				
Evaluation	Administrative					
Business Assoc. contracts	Administrative	Written contract or other arrangements				
Workstation use	Physical					
Workstations security	Physical					
Device and media controls	Physical	Disposal				

Required Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Device and media controls	Physical	Media re-use				
Access control	Technical	Unique user id (				
Access control		Emergency access procedure				
Audit controls	Technical					
Person or entity authentication	Technical					

Part 2

Addressable Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Workforce security	Administrative	Authorization/ Supervision				
Workforce security	Administrative	Workforce clearance				

Addressable Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Workforce security	Administrative	Termination procedures				
Information access management	Administrative	Access authorization				
Information access management	Administrative	Access establishment and modification				
Security awareness & training	Administrative	Security reminders				
Security awareness & training	Administrative	Protection from malicious software				
Security awareness & training	Administrative	Login monitoring				
Security awareness & training	Administrative	Password management				
Contingency plan	Administrative	Testing and revision procedure				

Addressable Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Contingency plan	Administrative	Applications and data criticality analysis				
Facility access controls	Physical	Contingency operations				
Facility access controls	Physical	Facility security plan				
Facility access controls	Physical	Access control and validation procedures				
Facility access controls	Physical	Maintenance records				
Device and media controls	Physical	Accountability				
Device and media controls	Physical	Data backup and storage				
Access control	Technical	Automatic logoff				

Addressable Standards	Safeguard Type	Function	Date Reviewed	Reviewed By-Name	Date completed	Comments
Access control	Technical	Encryption and decryption				
Integrity	Technical	Mechanism to authenticate electronic PHI				
Transmission security	Technical	Integrity controls				
Transmission security	Technical	Encryption				

Definitions: The terms below are taken from 45 CFR 164.304 (those in italics) and the Analysis by the American Health Information Management Association (those underlined). The AHIMA publication is located at http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_017594.html where more detailed information on security standards is available. The term ePHI, which is used in the definitions, means electronic protected health information.

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part.)

Access Authorization: requires that the covered entity address implementing policies and procedures for granting access to ePHI, for example, through access to a workstation (definition above), transaction, program, process, or other mechanism.

Access Control: technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

Access Control and Validation: 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.

Access Establishment and Modification: requires that the covered entity implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's (a designated member of the workforce or other authorized individual) right of access to a workstation, transaction, program, or process.

Accountability: maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Applications and Data Criticality Analysis: assess the relative criticality of specific applications and data in support of other contingency plan components.

Assigned Security Responsibility: identify the security official who is responsible for the development and implementation of the policies and procedures required by the" Security Rule for the entity.

Audit Controls: hardware, software, and/or procedural mechanisms that record and examine activity in the information systems that contain or use ePHI.

Authentication means the corroboration that a person is the one claimed.

Authorization and/or supervision: procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed

Automatic Logoff: electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Contingency Operations: procedures that allow facility access in support or restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

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 ePHI.

Data Backup and Storage: must create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Data Backup Plan: establish and implement procedures to create and maintain retrievable exact copies of ePHI.

Device and Media Controls: policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

Disaster Recovery Plan: establish (and implement as needed) procedures to restore any loss of data.

Disposal: address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

Emergency Access Procedure: procedures for obtaining necessary ePHI during an emergency.

Emergency Mode Operation Plan: procedures to enable continuation of critical business processes for protection of the security of ePHI while operating the emergency mode.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

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 ePHI.

Facility means the physical premises and the interior and exterior of a building(s).

Facility Access Controls: 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

Facility Security Plan: policies and procedures to safeguard the facility and the equipment within from "unauthorized physical access, tampering, and theft.

Information Access Management: policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the Privacy Rule.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Information system activity review: procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Integrity controls: security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Log-In Monitoring: procedures for monitoring log-in attempts and reporting discrepancies. Again, this is a clear situation where the requirement's scalability dictates different solutions by different size and technology dependent organizations.

Maintenance Records: 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.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Media Re-Use: implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

Password means confidential authentication information composed of a string of characters.

Password Management: procedures for creating, changing, and safeguarding passwords.

Person or Entity Authentication: procedures to verify that a person or entity seeking access to ePHI is the one [person] claimed.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protection From Malicious Software: requires you to have procedures for guarding against, detecting, and reporting malicious software

Risk analysis: conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePH (electronic PHI) that it holds.

Risk management: implement security measure sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with security standards.

Sanction policy: apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security Awareness and Training: implement a security awareness and training program for all members of its workforce (including management.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Management Process: policies and procedures to prevent, detect, contain and correct security violations. There are four implementation specifications - all required, covering risk analysis, risk management, sanction policy, and information system activity review.

Security Reminders: Periodic security updates.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Termination procedures: procedures for terminating access to ePHI when the employment of a workforce member ends or as required by the procedures you implement for the "workforce clearance procedure."

Testing and Revision Procedures: implement some sort of procedures for periodic testing and revision of contingency plans.

Transmission Security: security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Unique User Identification: a unique name and/or number for identifying and tracking user identity.

User means a person or entity with authorized access.

Workforce clearance procedure: implement procedures to determine that the access of a workforce member to ePHI is appropriate

Workforce Security: requires the covered entity to "implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided" by the standard for information access management (just below), "and to prevent those workforce members who do not have access under" that standard "from obtaining access to ePHI.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

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 ePHI.

Workstation Security: implement physical safeguard for all workstations that access ePHI, to restrict access to authorized users.

Written Contract or Other Arrangement: must document the satisfactory assurances required by this standard through a written contract or other arrangement (probably a memorandum of agreement) with the business associate.