EXHIBIT A

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R) = Required (A) - Addressable	
Security Management Process	164.308(a)(1)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	
		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.	
		Risk Management	(R)
		Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.	
		Sanction Policy	(R)
		Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures	
		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.	
Assigned Security Responsibility	164.308 (a)(2)	Identify the security official responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	(R)
Workforce Security	164.308(a)(3)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (i.e., that they have the proper level of access), and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.	
		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.	
		Workforce Clearance Procedure	(A)
		Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	
		Termination Procedures	(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 under the workforce clearance procedure, above.	
Information Access Management	164.308(a)(4)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with safeguards required under HIPAA.	
		Isolating Health Care Clearing House Function	(R)
		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.	
		Access Authorization	(A)
		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.	
		Access Establishment and Modification	(A)
		Implement policies and procedures that, based upon the entity's	

Standards	Sections	Implementation Specifications (R) = Required (A) - Addressable	
		access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	
Security Awareness and Training	164.308(a)(5)	Implement a security awareness and training program for all members of its workforce (including management).	
		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.	
Security Incident Procedures	164.308(a)(6)	Implement policies and procedures to address security incidents.	
		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.	
Contingency Plan	164.308(a)(7)	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.	
		Data Backup Plan	(R)
		Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	
		Disaster Recovery Plan	(R)
		Establish (and implement as needed) procedures to restore any lost 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 protected health information 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.	
Evaluation	164.308(a)(8)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security 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.	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	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.	
		Written Contract or other Agreement	(R)
		Document the satisfactory assurances described above through a written contract or other arrangement with the business associate that meets the applicable requirements of HIPAA.	

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R) = Required (A) - Addressable	
Facility Access Controls	164.310(a)(1)	Implement policies and procedures to limit physical access to the covered entity's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	
		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).	
Workstation Use	164.310(b)	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.	(R)
Workstation Security	164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	(R)
Device and Media Controls	164.310(d)(1)	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.	
		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.	
		Media Re-Use	(R)
		Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	
		Accountability	(A)
		Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	
		Data Backup and Storage	(A)
		Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R) = Required (A) - Addressable	
Access Control	164.312(a)(1)	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 described above.	
		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 protected health information during an emergency..	
		Automatic Logoff	(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 protected health information.	
Audit Controls	164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	(R)
Integrity	164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	
		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.	
Person or Entity Authentication	164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	(R)
Transmission Security	164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	
		Integrity Controls	(A)
		Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
		Encryption	(A)
		Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	