EXHIBIT A

SECURITY RULE REQUIREMENTS

The following chart summarizes HIPAA Security Rule standards and specifications that should be implemented by covered entities and business associates through the establishment of organizational policies and safeguards. The administrative, technical and physical safeguards described below are applicable to covered entities and business associates alike. The chart shows the regulatory citations and references the applicable security standard (in bold) along with the “Addressable” and “Required” implementation specifications that must be met in order to satisfy the applicable standard. The regulatory references are to 45 CFR § 164.300 *et seq.*, but please keep in mind that the Security Rule is subject to amendment so the only way to ensure compliance is to review the Security Rule and the applicable legal requirements.

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
Administrative Safeguards		
164.308(a)(1)(i)	**Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
164.308(a)(1)(ii)(A)	Risk Analysis: Have you conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (“e-PHI”) held by your organization, using the National Institute of Standards and Technology[i] (NIST) Guidelines? (R)	
164.308(a)(1)(ii)(B)	Have you completed the risk management process by implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, consistent with NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have a formal sanctions policy and do you impose sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports? (R)	
164.308(a)(2)	**Assign 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 covered entity or business associate.**	

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
164.308(a)(3)(i)	**Workforce security: Implement policies and procedures to ensure that all members of workforce have appropriate access to e-PHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to e-PHI.**	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of workforce members who work with e-PHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine whether the access of an employee to e-PHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to e-PHI when an employee leaves your organization or as required by other determinations under HIPAA? (A)	
164.308(a)(4)(i)	**Information access management: Implement policies and procedures for authorizing access to e-PHI that are consistent with the applicable requirements of subpart E of this part.**	
164.308(a)(4)(ii)(A)	If you are a clearinghouse that is part of a larger organization, has the clearinghouse implemented policies and procedures that protect the e-PHI of the clearinghouse from unauthorized access by the larger organization? (A)	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to e-PHI, for example, through access to a workstation, transaction, program, process, or other mechanism? (A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user’s right of access to a workstation, transaction, program, or process? (A)	
164.308(a)(5)(i)	**Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management).**	
164.308(a)(5)(ii)(A)	Do you provide periodic information security updates? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring log-in attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	**Security incident procedures: Implement policies and procedures to address security incidents.**	

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
164.308(a)(6)(ii)	Do you identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the organization; and document security incidents and their outcomes? (R)	
164.308(a)(7)(i)	**Contingency plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems that contain e-PHI.**	
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of e-PHI? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of e-PHI? (R)	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of the security of your e-PHI while operating in emergency mode? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	Have you established a plan for 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 e-PHI, that establish the extent to which your security policies and procedures meet the requirements of this subpart? (R)	
164.308(b)(1)	**Business associate contracts and other arrangements: A covered entity may permit a business associate to create, receive, maintain, or transmit e-PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Section 164.314(a) that the business associate will appropriately safeguard the information.**	
164.308(b)(2)	**A business associate may permit a subcontractor to create, receive, maintain, or transmit e-PHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with Section 164.314(a), that the subcontractor will appropriately safeguard the information.**	

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
164.308(b)(3)	Have you established written contract or other arrangement that documents satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section that meets the applicable requirements of Section 164.314(a)? (R)	
Physical Safeguards		
164.310(a)(1)	**Facility access controls: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.**	
164.310(a)(2)(i)	Have you established (and implemented 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? (A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? (A)	
164. 310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks)? (A)	
164.310(b)	**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 e-PHI.**	
164.310(c)	**Workstation security: Implement physical safeguards for all workstations that access e-PHI, to restrict access to authorized users.**	
164.310(d)(1)	**Device and media controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain e-PHI into and out of a facility, and the movement of these items within the facility.**	

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of e-PHI, and/or the hardware or electronic media on which it is stored? (R)	
164.310(d)(2)(ii)	Have you implemented procedures for removal of e-PHI from electronic media before the media are available for re-use? (R)	
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and any person responsible such movements? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of e-PHI, when needed, before moving equipment? (A)	
Technical Safeguards		
164.312(a)(1)	**Access controls: Implement technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights as specified in Section 164.308(a)(4).**	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining necessary e-PHI during an emergency? (R)	
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt e-PHI? (A)	
164.312(b)	Have you implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI? (R)	
164.312(c)(1)	**Integrity: Implement policies and procedures to protect e-PHI from improper alteration or destruction.**	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	Have you implemented person or entity authentication procedures to verify a person or entity seeking access to e-PHI is the one claimed? (R)	

HIPAA Security Rule Reference	**Safeguard and whether it is Required (R) or Addressable (A)**	**Status: Complete / Comments**
164.312(e)(1)	**Transmission security: Implement technical security measures to guard against unauthorized access to e-PHI being transmitted over an electronic communications network.**	
164.312(e)(2)(i)	Have you implemented security measures to ensure electronically transmitted e-PHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt e-PHI whenever deemed appropriate? (A)	

[i] This document contains references to the National Institute of Standards and Technology, a federal agency that publishes freely available material, including Special Publications and guidelines regarding risk assessments and risk management. Although only federal agencies are required to follow NIST standards and the HHS Office for Civil Rights has not explicitly endorsed the NIST standard, its guidelines represent the industry standard for good business practices concerning standards for carrying out the organizational risk assessment and risk management processes.