EXHIBIT A

- HIPAA Security Assessment Template -

Department/Unit: _____ Date: _____

Person(s) Conducting Assessment: _____ Title: _____

1. Administrative Safeguards:

The HIPAA Security Rule defines administrative safeguards as, *"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."*

The purpose of this section is to determine whether the unit/department has established administrative functions required in HIPAA security rules with the corresponding implementation specifications to meet the security standards.

Below are criteria to validate the reviewing department suggested by CMS and NIST publication 800-66:

ADMINISTRATIVE SAFEGUARDS	IMPLEMENTATION SPECIFICATION	SAMPLE QUESTIONS TO ASK	OBSERVATIONS	RECOMMENDATIONS
Security Management Process	Risk Analysis (Required) *The department is required to conduct accurate and thorough assessment of potential risks to ePHI, considering all the relevant losses caused by unauthorized use and disclosure of ePHI if the security measure is absent.*	• Are there any prior risk assessments, audit comments, security requirements, and/or security test results? • What are the current and planned controls? • Is the facility located in a region prone to any natural disasters, such as earthquakes, floods, or fires? • Has responsibility been assigned to check all hardware and software, including hardware and software used		

		for remote access, to determine whether selected security settings are enabled? • Is there an analysis of current safeguards and their effectiveness relative to the identified risks? • Have all processes involving ePHI been considered, including creating, receiving, maintaining, and transmitting it?		
	Risk Management (Required) *The department is required to detect and respond to security incidents, and implement sufficient security measures to reduce risks.*	• Do current safeguards ensure the confidentiality, integrity, and availability of all ePHI? • Do current safeguards protect against reasonably anticipated uses or disclosures of ePHI that are not permitted by the Privacy Rule? • Has the covered entity protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI? • Has the covered entity assured compliance with all policies and procedures by its workforce?		

	Sanction Policy (Required) *Appropriate sanctions must be in place so that the department staff members understand the consequences of failing to comply with security policies and procedures.*	• Is there a formal process in place to address system misuse, abuse, and fraudulent activity? • Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of ePHI? • How will managers and employees be notified regarding suspect activity?		
	Information System Activity Review (Required) *Audit logs and/or access reports process must be enforced to determine if any ePHI is used or disclosed inappropriate manner.*	• Who is responsible for the overall process and results? • How often will reviews take place? • How often will review results be analyzed? • What is the organization's sanction policy for employee violations? • Where will audit information reside (e.g., separate server)?		

Assigned Security Responsibility	*The department must assign security responsibilities to one official. The responsibilities include management and supervision of use*	• Who in the organization—
		  ○ Oversees the development and communication of security policies and procedures?
		  ○ Is responsible for		

	of security measures associated with this standard.	conducting the risk assessment? ○ Handles the results of periodic security evaluations and continuous monitoring? ○ Directs IT security purchasing and investment? ○ Ensures that security concerns have been addressed in system implementation? • Who in the organization is authorized to accept risk from information systems on behalf of the organization?		
Workforce Security	Authorization and/or Supervision (Addressable) *Staff members should be supervised or have clearance when working in locations where ePHI is located.*	• Are there written job descriptions that are correlated with appropriate levels of access? • Have staff members been provided copies of their job descriptions, informed of the access granted to them, as well as the conditions by which this access can be used?		
	Workforce Clearance Procedure	• Is there an implementation strategy that supports the		

	(Addressable) *An established background check or screening process to verify that workforce members get appropriate access to ePHI.*	designated access authorities? • Are applicants' employment and educational references checked, if reasonable and appropriate? • Have background checks been completed, if reasonable and appropriate? • Do procedures exist for obtaining appropriate sign-offs to grant or terminate access to ePHI?		
	Termination Procedures (Addressable) *Termination procedures to remove access privileges when an employee, contractor, or other individual previously entitled to access information no longer has these privileges.*	• Are there separate procedures for voluntary termination (retirement, promotion, transfer, change of employment) vs. involuntary termination (termination for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions), if reasonable and appropriate? • Is there a standard checklist for all action items that should be completed when an employee leaves (return of all access devices, deactivation of logon accounts [including remote access], and delivery of		

		any needed data solely under the employee's control)?		
Information Access Management	Access Authorization (Addressable) *Policies or procedures should be in place for access authorization to system with ePHI.*	• Do the organization's IT systems have the capacity to set access controls? • Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties? • Does the organization grant remote access to ePHI? • What method(s) of access control is (are) used (e.g., identity-based, role-based, location-based, or a combination)?		
	Access Establishment and Modification (Addressable) *Policies or procedures should be in place for accounts establishment and modification for access to systems with ePHI.*	• Are duties separated such that only the minimum necessary ePHI is made available to each staff member based on their job requirements?		
Security Awareness and Training	Security Reminders (Addressable) *The department should*	• Have employees received a copy of, and do they have ready access to, the organization's security		

	implement documented reminders such as security notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, or formal retraining on security policies and procedures.	procedures and policies? • Do employees know whom to contact and how to handle a security incident? • Do employees understand the consequences of noncompliance with the stated security policies? • Do employees who travel know how to handle physical laptop security issues and information security issues? • Has the covered entity researched available training resources? • Is dedicated training staff available for delivery of security training? If not, who will deliver the training?		
	Protection from Malicious Software (Addressable) *The department staff members should be trained regarding their role in protecting against malicious software.*	• Do employees know the importance of timely application of system patches to protect against malicious software and exploitation of vulnerabilities?		

	Log-in Monitoring (Addressable) *The department staff members should be informed on how users log onto systems and how they are supposed to manage their passwords.*	• Are employees aware that log-in attempts may be monitored? • Do employees that monitor log-in attempts know to whom to report discrepancies?		
	Password Management (Addressable) *The department staff members should be trained on how to safeguard the information by establishing guidelines for creating passwords and changing them periodically.*	• Do employees understand their roles and responsibilities in selecting a password of appropriate strength, changing the password periodically (if required), and safeguarding their password?		
Security Incident Procedures	Response and Reporting (Required) *The department must implement a procedure to describe how staff members are to respond to an incident,*	• Has the organization determined that maintaining a staffed security incident hotline would be reasonable and appropriate? • Has the organization determined reasonable and appropriate mitigation options		

	such as preserving evidence, documenting the incident and the outcome, and evaluating and reporting the incidents as an ongoing risk management.	for security incidents? • Has the organization determined that standard incident report templates to ensure that all necessary information related to the incident is documented and investigated are reasonable and appropriate? • Has the organization determined under what conditions information related to a security breach will be disclosed to the media? • Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared? • Has a written incident response plan been developed and provided to the incident response team?		
Contingency Plan	Data Backup Plan (Required) *The department must establish and implement procedures*	• Is there a formal, written contingency plan? • Does it address disaster recovery and data backup? • Do data backup procedures exist? • Are responsibilities assigned to conduct backup activities?		

	for data backup.	• Are data backup procedures documented and available to other staff?		
	Disaster Recovery Plan (Required) *The department must establish and implement procedures for disaster recovery.*	• Have procedures related to recovery from emergency or disastrous events been documented? • Has a coordinator who manages, maintains, and updates the plan been designated? • Has an emergency call list been distributed to all employees? Have recovery procedures been documented? • Has a determination been made regarding when the plan needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery, etc.)?		
	Emergency Mode Operation Plan (Required) *The department must establish and implement procedures for emergency mode operation.*	• Have procedures been developed to continue the critical functions identified in Key Activity? • If so, have those critical functions that also involve the use of ePHI been identified? • Would different staff, facilities, or systems be needed to perform those functions? • Has the security of that ePHI in that alternative mode of operation been assured?		

	Testing and Revision Procedures (Addressable) *The department should implement procedures for periodic testing, documenting, and revision of contingency plans.*	• How is the plan to be tested? • Does testing lend itself to a phased approach? • Is it feasible to actually take down functions/services for the purposes of testing? • Can testing be done during normal business hours or must it take place during off hours? • If full testing is infeasible, has a "tabletop" scenario (e.g., a classroom-like exercise) been considered? • How frequently is the plan to be tested (e.g., annually)? • When should the plan be revised?		

	Application and Data Criticality Analysis (Addressable)
	
	The department should identify their applications that store, maintain, or transmit ePHI to determine how important each is to patient care and business needs.
		• What critical services must be provided within specified timeframes?
		  ○ Patient treatment, for example, may need to be performed without disruption.
		  ○ By contrast, claims processing may be delayed during an emergency with no long-term damage to the organization.
		• Have cross-functional dependencies been identified		

		so as to determine how the failure in one system may negatively impact another one?		
Evaluation	*The department must periodically evaluate technical and non-technical security measures in response to changing environment, technology or operations.*	• How much training will staff need on security-related technical and nontechnical issues? • Have management, operational, and technical issues been considered? • Do the elements of each evaluation procedure (questions, statements, or other components) address individual, measurable security safeguards for ePHI? • Do security policies specify that evaluations will be repeated when environmental and operational changes are made that affect the security of ePHI?		
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement (Required) *The department must obtain a written contract regarding satisfactory assurances of business associates that create, receive, maintain, or transmit ePHI.*	• Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected? • Are there any new organizations or vendors that now provide a service or function on behalf of the organization? • Such services may include the		

		following: ○ Claims processing or billing ○ Data analysis ○ Utilization review ○ Quality assurance ○ Benefit management ○ Practice management ○ Re-pricing ○ Hardware maintenance ○ All other HIPAA-regulated functions • Have outsourced functions involving the use of ePHI been considered, such as the following: ○ Actuarial services ○ Data aggregation ○ Administrative services ○ Accreditation ○ Financial services?		

***** Be sure to ask for documentations for the above administrative safeguards

2. Physical Safeguards:

The HIPAA Security Rule defines physical safeguards as, *"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."*

The purpose of this section is to determine if the department/unit has mechanisms to protect electronic systems, equipment, and data from threats, environmental hazards, and unauthorized intrusion, including restricting access to ePHI and retaining offsite data backups.

PHYSICAL SAFEGUARDS	IMPLEMENTATION SPECIFICATION	SAMPLE QUESTIONS TO ASK	OBSERVATIONS	RECOMMENDATIONS
Facility Access Controls	Contingency Operations (Addressable) *The department should establish procedures regarding contingency operations during an emergency.*	• Who needs access to ePHI in the event of a disaster? • What is the backup plan for access to the facility and/or ePHI? • Who is responsible for the contingency plan for access to ePHI? • Who is responsible for implementing the contingency plan for access to ePHI in each department, unit, etc.? • Will the contingency plan be appropriate in the event of all types of potential disasters (fire, flood, earthquake, etc.)?		
	Facility Security Plan (Addressable) *The department should*	• If reasonable and appropriate, do nonpublic areas have locks and cameras? • Are workstations protected		

	implement controls to ensure only authorized individuals have access to facilities and equipment that contain ePHI.	from public access or viewing? • Are entrances and exits that lead to locations with ePHI secured? • Do policies and procedures already exist regarding access to and use of facilities and equipment? • Are there possible natural or man-made disasters that could happen in our environment? • Do normal physical protections exist (locks on doors, windows, etc., and other means of preventing unauthorized access)?		
	Access Control and Validation Procedures (Addressable) *The department should implement procedures to control and validate individuals' access to facilities.*	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary?		
	Maintenance Records (Addressable) *The department should document repairs and*	• Are records of repairs to hardware, walls, doors, and locks maintained? • Has responsibility for maintaining these records been assigned?		

	modifications to the physical security components of the facilities.			
Workstation Use	*The department must specify the proper functions to be performed by electronic computing devices by implement policies and procedures.*	• What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations? • How are workstations used in day-to-day operations? • What are key operational risks that could result in a breach of security?		
Workstation Security	*The department must protect electronic computing devices from unauthorized users.*	• Is there an inventory of all current workstation locations? • Are any workstations located in public areas? • Are laptops used as workstations? • What safeguards are in place, i.e., locked doors, screen barriers, cameras, guards? • Do any workstations need to be relocated to enhance physical security?		

		• Have employees been trained on security?		
Device and Media Controls	Disposal (Required) *Procedures must be in-place to remove any ePHI from computing devices before their disposal.*	• What data is maintained by the organization, and where? • Is data on removable, reusable media such as tapes and CDs? • Is there a process for destroying data on hard drives and file servers? • What are the options for disposing of data on hardware? What are the costs?		
	Media Re-Use (Required) *Procedures must be in-place to remove any ePHI from computing devices before their re-use.*	• Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? • Is one individual and/or department responsible for coordinating the disposal of data and the reuse of the hardware and software? • Are employees appropriately trained on security and risks to ePHI when reusing software and hardware?		
	Accountability (Addressable) *The department should maintain an inventory and record of the*	• Where is data stored (what type of media)? • What procedures already exist regarding tracking of hardware and software within the company? • If workforce members are		

	movements of hardware and electronic media and any person responsible therefore.	allowed to remove electronic media that contain or may be used to access ePHI, do procedures exist to track the media externally? • Who is responsible for maintaining records of hardware and software?		
	Data Backup and Storage (Addressable) *The department should create an exact copy of ePHI before movement of computing equipment to prevent the loss of data.*	• Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing ePHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?		

3. Technical Safeguards:

The HIPAA Security Rule defines technical safeguards as, *"the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."*

The purpose of this section is to determine if the reviewing department/unit has the processes to protect data and control access to data, which may include using authentication controls to verify that the person signing onto a computer is authorized to access ePHI, and encrypting data at rest and in transmission.

TECHNICAL SAFEGUARDS	IMPLEMENTATION SPECIFICATION	SAMPLE QUESTIONS TO ASK	OBSERVATIONS	RECOMMENDATIONS
Access Control	Unique User Identification (Required) *Each staff members is required to have unique username for identifying and tracking identity.*	• How should the identifier be established (length and content)? • Should the identifier be self-selected or randomly generated? • What are the procedures for new employee/user access to data and systems? • Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users?		
	Emergency Access Procedure (Required) *The department must establish procedures for obtaining necessary ePHI during an*	• When should the emergency access procedure be activated? • Who is authorized to make the decision? • Who has assigned roles in the process? • Will systems automatically		

	emergency.	default to settings and functionalities that will enable the emergency access procedure or will the mode be activated by the system administrator or other authorized individual?		
	Automatic Logoff (Addressable) *All systems that access ePHI should implement logoff feature to prevent unauthorized users from accessing ePHI when it is left unattended for a period of time.*	• Are automatic logoff features available for any of the covered entity's operating systems or other major applications? • If applications have been created or developed in-house, is it reasonable and appropriate to modify them to feature automatic logoff capability? • What period of inactivity prior to automatic logoff is reasonable and appropriate for the covered entity?		
	Encryption and Decryption (Addressable) *The department should employ encryption on ePHI if feasible to protect the data from being accessed and viewed by unauthorized users.*	• What encryption systems are available for the covered entity's ePHI? • Is encryption appropriate for storing and maintaining ePHI ("at rest"), as well as while it is transmitted?		

Audit Controls	*The department must implement mechanisms to record and examine activities in information systems that contain ePHI.*	• What activities will be monitored (e.g., creation, reading, updating, and/or deleting of files or records containing ePHI)? • What should the audit record include (e.g., user ID, event type/date/time)? • Who is responsible for the overall audit process and results? • How often will audits take place? • How often will audit results be analyzed? • What is the organization's sanction policy for employee violations? • Where will audit information reside (i.e., separate server)?		
Integrity	Mechanism to Authenticate electronic protected health information (Addressable) *The department should implement mechanisms to ensure and confirm that ePHI on systems (data at rest) has not been altered or*	• How are users authorized to access the information? • Is there a sound basis established as to why they need the access? • Have they been trained on how to use the information? • Is there an audit trail established for all accesses to the information? • What are likely sources that could jeopardize information integrity?		

	destroyed in unauthorized manner.	• What can be done to protect the integrity of the information when it is residing in a system (at rest)?		
Person or Entity Authentication	*The department must implement access authentication mechanism to verify a user authority, such as using password or PIN.*	• What authentication methods are available? • Have formal authentication policy and procedures been established and communicated? • Has necessary testing been completed to ensure that the authentication system is working as prescribed?		
Transmission Security	Integrity Control (Addressable) *The department should implement mechanisms to ensure that ePHI on transmission has not been modified improperly, such as hash function.*	• What measures exist to protect ePHI in transmission? • What measures are planned to protect ePHI in transmission? • Is there assurance that information is not altered during transmission?		
	Encryption (Addressable) *The department should apply appropriate encryption security measures for ePHI during transmission.*	• Is encryption reasonable and appropriate for ePHI in transmission? • Is encryption needed to effectively protect the information? • Is encryption feasible and cost-effective in this environment? • What encryption algorithms		

		and mechanisms are available? • Does the covered entity have the appropriate staff to maintain a process for encrypting ePHI during transmission?		