Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
Administrative Safeguards						
164.308(a)(1)(i)	***Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.***	Implement real-time monitoring of systems for security / viral activities Implement a reporting / notification mechanism for security incidents.				
164.308(a)(1)(ii)(A)	**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	1) Implement a full review of relevant information systems, data devices, data storage and procedures being used with the Information Technology group and the end user community where HIPAA related data is being captured, stored or used. 2) Obtain physical maps of offices and locations where HIPAA information might be stored. 3) Schedule regular Annual Reviews to coincide with				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
		the original analysis.				
164.308(a)(1)(ii)(B)	**Risk Management (R):** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	Implement and monitor physical and logical access to HIPAA data and transmission information.	1)			
164.308(a)(1)(ii)(C)	**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.	Implement an Annual Review process.				
164.308(a)(2)	**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.	Identify two (2) roles within to assist with enforcing and updating HIPAA guidelines. The two roles are: 1) HIPAA Security Officer 2) HIPAA Privacy Officer				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.308(a)(3)(i)	**Workforce Security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, 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 electronic protected health information.	Identify all staff who receive or use HIPAA regulated data. Create systems and procedures to ensure access to only those staff.				
164.308(a)(3)(ii)(A)	**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.	Create, implement and maintain a process for rights authorization to HIPAA identified data stores.				
164.308(a)(3)(ii)(B)	**Workforce Clearance Procedure (A):** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Identify checkpoint with hiring manager and / or supervising manager for any new staff to identify HIPAA need.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.308(a)(3)(ii)(C)	**Termination Procedure (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 as specified in paragraph (a)(3)(ii)(B) of this section.	Update all termination procedures to ensure timely and appropriate account deactivation.				
164.308(a)(4)(i)	***Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.***	Create, implement and review all security groups, access control lists and other mechanisms to protect the confidentiality of the data and prohibit access by unnecessary staff. 1) Establish access controls for staff 2) Identify who should have access to the data 3) Evaluate the access measures				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.308(a)(4)(ii)(A)	**Isolating Health Care Clearinghouse 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.	Not Applicable ; Not a Healthcare Clearing House as defined by 45 CFR 160.103.				
164.308(a)(4)(ii)(B)	**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.	Create, implement and maintain a process for rights authorization to HIPAA identified data stores.				
164.308(a)(4)(ii)(C)	**Access Establishment and Modification (A):** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program,	Create, implement and review all security groups, access control lists and other mechanisms to protect the confidentiality of the data and prohibit access by unnecessary staff. 1) Establish access controls for staff				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
	or process.	2) Identify who should have access to the data 3) Evaluate the access measures				
164.308(a)(5)(i)	***Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).***	Include HIPAA module in the on-boarding process and security awareness training. Also provide HIPAA training to all necessary IT staff.				
164.308(a)(5)(ii)(A)	**Security Reminders (A):** Implement periodic security updates.	Staff will sign off on Security Awareness Training.				
164.308(a)(5)(ii)(B)	**Protection from Malicious Software (A):** Implement Procedures for guarding against, detecting, and reporting malicious software.	Require the installation and maintenance of a 3rd party product to conduct Anti-Virus / Anti-Malware services.				
164.308(a)(5)(ii)(C)	**Login Monitoring (A):** Implement procedures for monitoring login attempts and reporting discrepancies.	Standard procedure for Network Administrators to check logs for logins / login attempts.				
164.308(a)(5)(ii)(D)	**Password Management (A):** Implement procedures for creating, changing,	Implement strong passwords and periodic changes.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
	and safeguarding passwords.					
164.308(a)(6)(i)	***Security Incident Procedures: Implement policies and procedures to address security incidents.***	Create / implement a security response system.				
164.308(a)(6)(ii)	**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.	Security Incident reporting system to be implemented and monitored.				
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, and natural disaster) that damages systems that contain electronic protected health***	Create, implement and update a Disaster Recovery Plan.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
	information.					
164.308(a)(7)(ii)(A)	**Data Backup Plan (R):** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Implement a data rotation and backup plan to support the protection of the data.				
164.308(a)(7)(ii)(B)	**Disaster Recovery Plan (R):** Establish (and implement as needed) procedures to restore any loss of data.	Implement DRP.				
164.308(a)(7)(ii)(C)	**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.	Create a policy to handle emergency operations in the event of a disaster.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.308(a)(7)(ii)(D)	**Testing and Revision Procedure (A):** Implement procedures for periodic testing and revision of contingency plans.	Determine the appropriate level of testing for DRP. Update plans as needed.				
164.308(a)(7)(ii)(E)	**Applications and Data Criticality Analysis (A):** Assess the relative criticality of specific applications and data in support of other contingency plan components.	Conduct a review of systems and identify systems that are critical for contingency plans.				
164.308(a)(8)	***Evaluation: Perform a periodic technical and non technical evaluation, based initially upon the standards implemented under this 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.***	Perform an Annual Review of HIPAA Policies and Guidelines.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.308(b)(1)	***Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.***	Obtain Business Associate Agreements with relevant 3rd parties.				
164.308(b)(4)	**Written Contract or Other Arrangement (R):** Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a).	Obtain Business Associate Agreements with relevant 3rd parties.				
Physical Safeguards						

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.310(a)(1)	***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.***	Utilize existing facility safety systems to ensure physical access to information is regulated.				
164.310(a)(2)(i)	**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.	Determine the location and process to be used in the case of an emergency to maintain operations.				
164.310(a)(2)(ii)	**Facility Security Plan (A):** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Create a baseline of security for each physical location.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.310(a)(2)(iii)	**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.	Link staff role and physical space access.				
164.310(a)(2)(iv)	**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).	Ensure that any changes to the physical surroundings within our HIPAA regulated areas are noted and checked.				
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 electronic protected health information.***	Track all systems in use . Identify those systems that are a part of the HIPAA related practices. Create and publish system standards for all equipment used. Publish these standards internally and with our external vendor(s). Create a base image file to be used on all computers. This base image is controlled by IT				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
		and all systems get the base image burned on the machine.				
164.310(c)	***Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.***	All access to VK physical space to be restricted. Computer locks are offered and recommended for all systems.				
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 electronic protected health information into and out of a facility, and the movement of these items within the facility.***	Assign and track all systems to an individual employee. Require and provide encrypted / secure flash drives for HIPAA regulated data movement within the firm. Require all HIPAA regulated data to be transmitted via encrypted email.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.310(d)(2)(i)	**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.	Create, implement and monitor disposal practice for HIPAA regulated data stores and systems.				
164.310(d)(2)(ii)	**Media Re-Use (R):** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	Create, implement and monitor the reuse practice for HIPAA regulated data stores.				
164.310(d)(2)(iii)	**Accountability (A):** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Maintain logs and asset tracking.				
164.310(d)(2)(iv)	**Data Backup and Storage (A):** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Covered under DRP and Backup Procedures.				
Technical Safeguards						

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.312(a)(1)	***Access Controls: 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 specified in Sec. 164.308(a)(4).***	Confirm and maintain security / policy groups to enforce data access controls. Design and implement greater access controls on physical devices and storage groups.				
164.312(a)(2)(i)	**Unique User Identification (R):** Assign a unique name and/or number for identifying and tracking user identity.	Create, implement and maintain a method using unique IDs and passwords to determine identity and confirm access.				
164.312(a)(2)(ii)	**Emergency Access Procedure (R):** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	See DRP above.				
164.312(a)(2)(iii)	**Automatic Logoff (A):** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Create a mechanism to logoff users with inactivity.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
164.312(a)(2)(iv)	**Encryption and Decryption (A):** Implement a mechanism to encrypt and decrypt electronic protected health information.	All HIPAA regulated data will be handled on encrypted media or transmissions.				
164.312(b)	***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***	Enhance system security to protect HIPAA regulated data. Implement procedures for supervision and monitoring of staff access to HIPAA regulated data.				
164.312(c)(1)	***Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.***	Implement a standard and secure process to "wipe" all media and computers that may be exposed to HIPAA regulated data.				
164.312(c)(2)	**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.	Implement a standard and secure process to "wipe" all media and computers that may be exposed to HIPAA regulated data. Continue to examine and determine an implementation plan for a document management system.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
		Ensure that appropriate backup procedures are in place to maintain proper versioning and updates of HIPAA regulated data files.				
164.312(d)	***Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.***	Institute internal security controls for access to HIPAA regulated Data. Implement secure transmission mechanism for HIPAA regulated data.				
164.312(e)(1)	***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.***	Supply staff with email encryption for use with HIPAA regulated data.				
164.312(e)(2)(i)	**Integrity Controls (A):** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until	Secure the transmission of HIPAA data via encryption.				

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Compliance Response	Compliance Documentation	Frequency Of Test	Method Used for Test	Exceptions / Remediation
	disposed of.					
164.312(e)(2)(ii)	**Encryption (A):** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	All HIPAA regulated staff / data is supplied with encrypted / protected flash drives, encrypted email and encrypted hard drives.				