#	Policy	Description
1	**INFORMATION PROTECTION PROGRAM POLICY**	To provide a framework for management direction and support for information security in accordance with business requirements and relevant laws and regulations.
2	**ENDPOINT PROTECTION**	To ensure organization complies with security guidelines pursuant to safe usage and storage of ePHI, and to protect the confidentiality and integrity, and to secure the availability of organization ePHI in compliance with the security regulations.
3	**PORTABLE MEDIA SECURITY**	To protect and secure patient personal information that can lead to identity theft or financial abuse, including but not limited to social security number and cardholder data, in compliance with governmental regulations, including the security regulations developed under the Payment Card Industry (PCI) Data Security Standards (DSS) and Red Flag Rules.
4	**MOBILE DEVICE SECURITY POLICY**	To outline a process for an organization to properly and safely protect corporate information that may be accessed and/or stored on individual-liable and corporate-liable devices and to ensure that an organization complies with security guidelines pursuant to safe usage and storage of ePHI that may be on the device.
5	**WIRELESS SECURITY**	This policy defines the essential rules regarding the management and maintenance of switches, routers and firewalls at the organization.
6	**CONFIGURATION MANAGEMENT**	To define a process by which all software and hardware is purchased and installed. Additionally, the policy address various configuration standards.
7	**VULNERABILITY MANAGEMENT**	To establishes the scope, objectives, and procedures of an organization information security risk management process in compliance with an organization's security risk analysis and risk management regulatory requirements.
8	**NETWORK PROTECTION**	To protect the confidentiality, integrity, and availability of an organization ePHI in compliance with security regulations.
9	**TRANSMISSION PROTECTION**	To provide guidance surrounding the encryption of data at rest and during transit. Encryption is the act of obscuring data in such a way that it is indecipherable and unreadable to anyone who does not possess the proper key to unlock the data.

#	Policy	Description
10	**PASSWORD MANAGEMENT**	To outline a process for an organization to possess secure passwords and user IDs for the organization.
11	**ACCESS CONTROL**	To provides a structured process for granting user access to accounts, and adhering to the standards of auditors and regulatory agencies.
12	**AUDIT LOGGING & MONITORING**	To outline a process for an organization to properly and safely protect corporate information that may be accessed and/or stored on personally owned (individual-liable) and organization-owned (corporate-liable) devices and to develop a process for the periodic review of application audit logs to properly assess security threats that possibly exist
13	**EDUCATION, TRAINING AND AWARENESS POLICY**	To outline a policy to properly educate the staff on matters of security and awareness.
14	**THIRD PARTY ASSURANCE**	To provide a policy which vendor's must adhere to, which relates to an organization data, network, computer, and infrastructure security. Vendors are required to adhere to this policy or they will not be granted access.
15	**INCIDENT MANAGEMENT**	To address an adverse event impacting an organization's ability to ensure the confidentiality, integrity, or availability of data and information systems.
16	**BUSINESS CONTINUITY & DISASTER RECOVERY POLICY**	To help meet the organization's goal of protecting the availability, integrity, and confidentiality of ePHI, an organization has developed policies and procedures for responding to an emergency or other unexpected negative event or occurrence that may damage or disrupt any system(s) containing ePHI.
17	**RISK MANAGEMENT**	To establish the scope, objectives, and procedures of the organization information security risk management process in compliance with risk analysis and risk management regulatory requirements.
18	**PHYSICAL & ENVIRONMENTAL SECURITY**	To safeguard the confidentiality, integrity, and availability of PHI, business, and proprietary information within an organization information systems/applications by controlling access to the physical buildings/facilities that house these systems/applications.
19	**DATA PROTECTION & PRIVACY**	To provide guidance around the encryption of data at rest and during transit and to assist in determining the appropriate response to the privacy/security violation and ensuring consistency of application across the organization.