

Policy/Procedure	Description
Information Security Policies	
Information Security Strategy	The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.
<i>Security Management Process</i>	The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk Analysis	The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.
Risk Management	The purpose is implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.
Sanction Policy	The purpose is to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the organization.
Information System Activity Review	The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
<i>Assigned Security Responsibility</i>	The purpose of this policy is to identify the security official who is responsible for the development and implementation of policies and procedures required by the HIPAA Security Rule 164.308(a)(2).
<i>Workforce Security</i>	The purpose is to implement policies and procedures to ensure that all members of the workforce have appropriate access to sensitive information and to prevent those workforce members who do not have access from obtaining access to sensitive information.
Authorization and/or Supervision	The purpose is to implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it might be accessed.
Workforce Clearance Procedure	The purpose is to implement procedures to determine

	that the access of a workforce member to sensitive information is appropriate.
Termination Procedures	The purpose is to implement procedures for quickly, securely and appropriately terminating access to sensitive information when the employment of a workforce member ends.
<i>Information Access Management</i>	The purpose is to implement policies and procedures for authorizing access to sensitive information.
Access Authorization	The purpose is to implement policies and procedures for granting access to sensitive information, for example, authorization required to access a workstation, transaction, program, process, or other mechanism.
Access Establishment and Modification	The purpose is to 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, or process.
<i>Security Awareness and Training</i>	The purpose is to implement a security awareness and training program for all members of its workforce, including management.
Security Reminders	The purpose is to implement periodic security updates to all members of the workforce.
Protection from Malicious Software	The purpose is to implement procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring	The purpose is to develop procedures for monitoring log-in attempts and reporting discrepancies.
Password Management	The purpose is to implement procedures for creating, changing and safeguarding passwords.
<i>Security Incident Procedures</i>	The purpose is to address security incidents.
Response and Reporting	The purpose is to 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.
<i>Contingency Plan</i>	The purpose is to 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 sensitive information.
Data Backup Plan	The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information.
Disaster Recovery Plan	The purpose is to establish and implement as needed procedures to restore any loss of data.
Emergency Mode Operation Plan	The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode.
Testing and Revision Procedures	The purpose is to implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis	The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.
<i>Evaluation</i>	The purpose is to perform a technical and non-technical evaluation and subsequently, in response to environmental or operational changes affecting the security of sensitive information that establishes the extent to which the organization's security policies and procedures meet the requirements of impacted regulations.
<i>Business Associate Contracts and Other Arrangements</i>	The purpose is to obtain satisfactory assurances with impacted regulations that the business associate will appropriately safeguard all sensitive information.
<i>Facility Access Controls</i>	The purpose is to implement policies and procedures to limit physical access to the organization's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Contingency Operations Policy	The purpose is to 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	The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Access Control and Validation	The purpose is to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision.
Maintenance Records	The purpose is to 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).
<i>Workstation Use</i>	The purpose is to 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 sensitive information.
<i>Workstation Security</i>	The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to authorized users.
<i>Device and Media Controls</i>	The purpose is to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of these items within a facility.
Disposal	The purpose is to implement policies and procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored.
Media Re-Use	The purpose is to implement procedures for removal of sensitive information from electronic media before the media are made available for re-use.
Accountability	The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data Backup and Storage	The purpose is to create a retrievable, exact copy of sensitive information, when needed, before the movement of equipment.
<i>Access Control</i>	The purpose is to implement technical policies and procedures for electronic information systems that maintain sensitive information to allow access only to those persons or software programs that have been granted access rights as specified by regulation or business process.

Unique User Identification	The purpose is to assign a unique name and/or number for identifying and tracking user identity.
Emergency Access Procedure	The purpose is to establish and implement as necessary sensitive information during an emergency.
Automatic Logoff	The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Encryption and Decryption	The purpose is to implement a mechanism to encrypt and decrypt sensitive information.
<i>Audit Controls</i>	The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.
<i>Integrity</i>	The purpose is to implement policies and procedures to protect sensitive information from improper alteration or destruction.
Mechanism to Authenticate Electronic Protected Health Information	The purpose is to implement electronic mechanisms to corroborate that sensitive information has not been altered or destroyed in an unauthorized manner.
<i>Person or Entity Authentication</i>	The purpose is to implement procedures to verify that the person or entity seeking access to sensitive information is the one claimed.
<i>Transmission Security</i>	The purpose is to implement technical security measures to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network.
Integrity Controls	The purpose is to implement security measures to ensure that electronically transmitted sensitive information is not improperly modified without detection until disposed of.
Encryption	The purpose is to implement a mechanism to encrypt sensitive information whenever deemed appropriate.
<i>Policies and Procedures Standard</i>	The purpose is to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of impacted regulations.
<i>Documentation</i>	The purpose is to maintain the policies and procedures implemented to comply with the impacted regulation in written (or electronic) form and if an

	action, activity or assessment is required to maintain a written (which may be electronic) record.
Information Classification	The purpose is to assist employees of the organization to make decisions regarding what information may and may not be released to the public or disclosed to any individual outside of the organization.
Network Security	The purpose is to secure communication devices and data on the organization's network.
E-mail Security	The purpose is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.
Remote Access	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to the organization's enterprise infrastructure to a reasonable and appropriate level.
Portable Devices	The purpose is to secure the use of portable devices used by members of the workforce.
VPN	The purpose is to implement security measures sufficient to reduce the risks and vulnerabilities of the organization's VPN infrastructure to a reasonable and appropriate level.
Wireless Security	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the organization's wireless infrastructure to a reasonable and appropriate level.
Wireless IP Phone	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the organization's wireless IP phones to a reasonable and appropriate level. To ensure the reasonable and appropriate use of wireless IP telephones and to provide guidance for the use of such devices.
Data Breach Discovery	The purpose is intended to provide guidance to the employees of the organization in defining and identifying potential security breaches of protected information, such as Protected Health Information (PHI), personal information or other confidential information.
Data Breach Management	The purpose is intended to assist employees responsible for managing breach related activities of the organization when making decisions after a data

	breach has been identified.
Data Breach Notification	The purpose is intended to assist employees responsible for addressing breach notifications of the organization when making decisions regarding the notification actions required after a breach of protected information is discovered.
Data Breach Notification to HHS	The purpose is to assist employees responsible for addressing breach notifications of the organization and provide specific guidance on when and how to notify the Department of Health and Human Services (HHS).
Data Breach Notification to Patient	The purpose is to assist employees responsible for addressing breach notifications of the organization and provide specific guidance on when and how to notify HHS.
Data Breach Notification to Media	The purpose is to assist employees responsible for addressing breach notifications of the organization and provide specific guidance on when and how to notify the media.

Figure 1: Summary of Information Security Policies