SECURITY RULE

Security Standards: General Rules

General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all ***electronic protected health information*** (ePHI) the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threat or hazard to the security or integrity of ePHI.

(3) Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted

(4) Ensure that its employees are in compliance.

Flexibility of Approach.

(1) Covered entities may use any security measures that are ***reasonable and appropriate***

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability of potential risks to ePHI

A covered entity must comply with the standards outlined in the attached sheets with respect to all ePHI.

This is an informational document only and is not meant as legal advice. Our clients are encouraged to seek additional information through the following websites or their legal counsel regarding HIPAA compliance.

www.hhs.gov
www.hipaa.org
www.wedi.org
www.hipadvisory.com

This is a brief summary of the HIPAA Security Rule. It should not be construed as legal advice. If you have additional questions, we recommend contacting your legal counsel

Implementation specifications.

(1) Implementation specifications are **required** or **addressable.**

(a) When a standard is **required** a covered entity must comply

(b) When a standard is **addressable** a covered entity must assess whether each implementation specification is a reasonable and appropriate safeguard.

If an **addressable** specification is deemed reasonable and appropriate, it must be implemented.

If an **addressable** specification is deemed not reasonable and appropriate, it must be documented as to why it is not reasonable and appropriate and an alternative safeguard must be implemented if deemed reasonable and appropriate.

Maintenance

Security measures implemented to comply with the Security Rule must be reviewed periodically and modified as needed to continue to maintain compliance under this Rule.

Compliance dates for the initial implementation of the security standards.

Health plans

(1) A large health plan must comply no later than April 20, 2005. (Defined by HIPAA as having $5,000,000 or more in claims or premium)

(2) A small health plan must comply no later than April 20, 2006. (Defined by HIPAA as having less than $5,000,000 in claims or premium)

A Health care clearinghouse must comply no later than April 20, 2005.

A Health care provider must comply no later than April 20, 2005.

Administrative Safeguards

General requirements. Covered entities must do the following:

STANDARD	Security Management Process - Implement policies and procedures to prevent, detect, contain, and correct security violations.
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	RISK ANALYSIS: Conduct a thorough assessment of the potential risks/vulnerabilities to the confidentiality, integrity, and availability of ePHI that you have access to.
REQUIRED ❒	RISK MANAGEMENT: Implement reasonable and appropriate security measures to reduce risks and vulnerabilities.
REQUIRED ❒	SANCTION POLICY: Apply appropriate sanctions against employees who fail to comply with security policies and procedures.
REQUIRED ❒	INFORMATION SYSTEM ACTIVITY REVIEW: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
STANDARD	Assigned Security Responsibility -Identify a Security Official who is responsible for the development and implementation of the Security Rule.
STANDARD	Workforce Security - Implement policies and procedures to ensure that all employees have appropriate access to ePHI and to prevent those employees who should not have access from obtaining access to ePHI
	IMPLEMENTATION SPECIFICATIONS
ADDRESSABLE ❒	AUTHORIZATION AND/OR SUPERVISION: Implement procedures for the authorization and/or supervision of employees who work with ePH or are in locations where it might be accessed.
ADDRESSABLE ❒	WORKFORCE CLEARANCE PROCEDURE: Implement procedures to determine the access level to ePHI that is appropriate for each employee.
ADDRESSABLE ❒	TERMINATION PROCEDURES: Implement procedures for terminating access to ePHI when an employee is terminated or for any reason should no longer have access to ePHI

STANDARD	**Information Access Management -** Implement policies and procedures for authorizing access to ePHI.
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	ISOLATING HEALTH CARE CLEARINGHOUSE (HCC) FUNCTIONS: If a HCC is part of a larger organization, the HCC must implement policies and procedures that protect the ePHI of the HCC from unauthorized access by the larger organization.
ADDRESSABLE ❒	ACCESS AUTHORIZATION: Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
ADDRESSABLE ❒	ACCESS ESTABLISHMENT AND MODIFICATION: Implement policies and procedures that, based upon your access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
STANDARD	**Security Awareness And Training -** Implement a security awareness and training program for all employees (including management).
	IMPLEMENTATION SPECIFICATIONS
ADDRESSABLE ❒	SECURITY REMINDERS: Periodic security updates
ADDRESSABLE ❒	PROTECTION FROM MALICIOUS SOFTWARE: Implement policies and procedures for guarding against, detecting, and reporting malicious software.
ADDRESSABLE ❒	LOG-IN MONITORING: Implement policies and procedures for monitoring log-in attempts and reporting discrepancies.
ADDRESSABLE ❒	PASSWORD MANAGEMENT: Implement policies and procedures for creating, changing, and safeguarding passwords.
STANDARD	**Security Incident Procedures -**Implement policies and procedures to address security incidents
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	RESPONSE AND REPORTING: Identify and respond to suspected or known security incidents; mitigate, to the extent feasible, harmful effects of security incidents and document security incidents and their outcomes.
STANDARD	**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 ePHI.
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	DATA BACKUP PLAN: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.
REQUIRED ❒	DISASTER RECOVERY PLAN: Establish (and implement as needed) procedures to restore any loss of data.
REQUIRED ❒	EMERGENCY MODE OPERATION PLAN: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic ePHI while operating in emergency mode.

ADDRESSABLE ❒	TESTING AND REVISION PROCEDURES: Implement procedures for periodic testing and revision of contingency plans
ADDRESSABLE ❒	APPLICATIONS AND DATA CRITICALITY ANALYSIS: Assess the relative criticality of specific applications and data in support of other contingency plan components.
STANDARD	**Evaluation -** Perform periodic evaluations, to ensure that new threats/vulnerabilities are identified and addressed.
STANDARD	**Business Associate Contracts and Other Arrangements -** You may permit a business associate to create, receive, maintain, or transmit ePHI on your behalf only if the you obtains satisfactory assurances that the business associate will appropriately safeguard the information.
	This standard does not apply with respect to--
A	The transmission by a covered entity of ePHI to a health care provider concerning the treatment of an individual.
B	The transmission of ePHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor
C	The transmission of ePHI from or to other agencies when the covered entity is a health plan that is a government program providing public benefits
D	A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and Requirements of this Standard
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	Written Contract or Other Arrangement: A document that provides satisfactory assurances required by this Standard through a written contract or other arrangement with the business associate

Physical Safeguards

General requirements. Covered entities must do the following:

STANDARD	**Facility Access Controls - Implement policies and procedures to limit physical access to your electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**
	IMPLEMENTATION SPECIFICATIONS
ADDRESSABLE ❒	CONTINGENCY OPERATIONS: 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
ADDRESSABLE ❒	FACILITY SECURITY PLAN: Implement policies and procedures to safeguard your facility and equipment from unauthorized physical access, tampering, and theft.
ADDRESSABLE ❒	ACCESS CONTROL AND VALIDATION PROCEDURES: 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.
ADDRESSABLE ❒	MAINTENANCE RECORDS: Implement policies and procedures to document repairs and modifications to the physical aspects of your facility which are related to security (for example, hardware, walls, doors, and locks).
STANDARD	**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 workstations that can access ePHI**
STANDARD	**Workstation security - Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users only.**
STANDARD	**Device And Media Controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a worksite, and the movement of these items within the worksite.**
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	DISPOSAL: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
REQUIRED ❒	MEDIA RE-USE: Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
ADDRESSABLE ❒	ACCOUNTABILITY: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
ADDRESSABLE ❒	DATA BACKUP AND STORAGE: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Technical Safeguards

General requirements. Covered entities must do the following:

STANDARD	**Access Control - Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights**
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	UNIQUE USER IDENTIFICATION: Assign a unique name and/or number for identifying and tracking user identity
REQUIRED ❒	EMERGENCY ACCESS PROCEDURE: Establish (and implement as needed) procedures for obtaining necessary ePHI
ADDRESSABLE ❒	AUTOMATIC LOGOFF: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
ADDRESSABLE ❒	ENCRYPTION AND DECRYPTION: Implement a mechanism to encrypt and decrypt ePHI.
ADDRESSABLE ❒	
STANDARD	**Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.**
STANDARD	**Integrity - Implement policies and procedures to protect ePHI from improper alteration or destruction.**
	IMPLEMENTATION SPECIFICATIONS
ADDRESSABLE ❒	MECHANISM TO AUTHENTICATE ePHI: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
STANDARD	**Person Or Entity Authentication - Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.**
STANDARD	**Transmission Security - Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.**
	IMPLEMENTATION SPECIFICATIONS
ADDRESSABLE ❒	INTEGRITY CONTROLS: Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of.
ADDRESSABLE ❒	ENCRYPTION: Implement a mechanism to encrypt ePHI whenever deemed appropriate

Organizational Requirements

General requirements. Covered entities must do the following:

STANDARD	**Business Associate Contracts or Other Arrangements - The contract or other arrangement between a covered entity and its business associate must meet the requirements of this section, as applicable.**
	A covered entity is not in compliance with the Standards in this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful-- (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	**Business Associate Contracts - The contract between a covered entity and a business associate must provide that the business associate will--**
A	Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;
B	Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
C	Report to the covered entity any security incident of which it becomes aware;
D	Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

STANDARD	Requirements for Group Health Plans - A group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to Sec. 564.504(f)(1)(ii) or (iii)
Summary of Sec.164.504(f)(1) (ii) and (iii)	A Health Plan Sponsor can receive two types of PHI or ePHI from the Group Health Plan without needing to meet HIPAA's Privacy or Security compliance requirements. These are: 1)Eligibility and enrollment/dis-enrollment information 2)"Summary Health Information" that is received for the purpose of: a) Obtaining bids from health plans b)Modifying, amending or terminating the Group Health Plan
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to--
A	Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan;
B	Ensure that the adequate separation of plan sponsor and group health plan is supported by reasonable and appropriate security measures;
C	Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
D	Report to the group health plan any security incident of which it becomes aware.

Policies and Procedures and Documentation Requirements

General requirements. Covered entities must do the following:

STANDARD	**Policies And Procedures - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this Rule, taking into account the Flexibility of Approach (page 1). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this Rule. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this Rule.**
STANDARD	**Documentation - Maintain the policies and procedures implemented to comply with this Rule in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this Rule to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment**
	IMPLEMENTATION SPECIFICATIONS
REQUIRED ❒	TIME LIMIT: Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
REQUIRED ❒	AVAILABILITY: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
REQUIRED ❒	UPDATES: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.