



HIPAA Compliance Requirements

MedXsecure allows you to meet HIPAA electronic compliance requirements by providing a secure network to transmit email, documents, audio files, video files, imaging files and more to anyone who can access an email address.

This document demonstrates how the medXsecure™ HIPAA Compliance utility helps you adhere to regulatory requirements for the electronic transfer of PHI.

§ 164.306 Security standards: General rules.

Individuals and Covered Entities are granted custody of PHI (Protected Health Information, specifically associated with an individual) to perform a service or task. As such, they come under the regulatory requirements of HIPAA (Health Insurance Portability and Accountability Act of 1996)

as a covered entity. (HIPAA, Title II) requires the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data.

- (a) General requirements. Covered entities must do the following: This utility addresses the communication and document transmission system. The entity is required to address the specific work station(s).

HIPAA REQUIREMENTS	How The SafetySend Utility Allows Documented Conformance to § 164.306 Security standards
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.	Use of a secure electronic method to transfer PHI from sender via interim custody and delivery. Validate transfer of custody to authenticated recipient at each interval. Provide remote storage of PHI in secure fashion in an uncorrupted form; transmission is required via encrypted channel to a verified recipient.
(2) Protect against any reasonably anticipated threats or hazards to the security of such information. This specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information;	<p>1. SafetySend Authentication is required to access any secured data on the system.</p> <p>2. Each data exchange is verified by the system during a documents transfer of custody and summarily applied to an accessible audit trail. This dynamic authentication method is established by the creation and use of a personal password system including generation of temporary passwords to assigned known recipients.</p> <p>3. A timed "log out" from the work station and communication link is included to protect against unauthorized system access at defined intervals or by manual exit.</p> <p>4. The communication system provides automatic virus filtering and updating; Spam filtering; spyware removal on demand.</p>
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	The SafetySend work communication system requires user authentication upon each timed entrance to the secure communication system.
(4) Ensure compliance with this subpart by its workforce.	<p>If the custody is held by or communication is done by other than a sole practice business associate:</p> <p>A sanction process can be established by the System Administrator to the covered entity; compliance is under purview of entity designated "System Administrator". Executed at the direction of the System Administrator.</p>

approach.	
(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	<p>If the regulations change, the business associate must modify activities to comply. SafetySend implements the communication changes – The entity is responsible for ‘work station’ implementation.</p> <p>Work procedures must be adaptable to evolution of HIPAA regulation with or without need for software upgrades to individual user terminals or computers. Adaptations are implemented throughout the system to all users.</p> <p>Changes or modification of HIPAA regulation are implemented for all client users.</p>
(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.	How scalable is the communication system? SafetySend is scalable to well in excess of 100,000 client users per Domain.
(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.	SafetySend does not rely on client hardware or software and are the updates integrated in a timely manner established specifically for this purpose?
(iii) The costs of security measures	SafetySend costs are reasonable and customary for the market without undue hardship to the covered entity and business associate.
(iv) The probability and criticality of potential risks to electronic protected health information	The SafetySend system reduces the risk of loss probability with identified controls of access and untraceable dissemination. Access is limited; transmissions are auditable; receipts are auditable; users are authenticated and identifiable.

safeguards.	
A covered entity must, in accordance with § 164.306:	Covered entities and their business associates must conform to § 164.306
(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	SafetySend security procedures are implemented and designed to detect and record attempts at unauthorized access and immediately notify network administrators of excessive password violations, attempted transfer of computer viruses, containment of potentially harmful files and renders activities to a security log. Individual tools are made available to each user for the detection and removal of viruses, spyware and other compromising software.
(A) Risk analysis (Required). Conduct 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.	The SafetySend communication network: allows only authenticated users; provides continuous encryption of internal and external transmission of PHI; conduct daily modification of intrusion and invasion by outside parties by conducting modification of code algorithms to negate intrusion.
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)	SafetySend require two levels of authentication initiate user identification; multi-challenge verification to change password. The use encryption code; application of processing algorithms, virus filters, and secure firewall are updated no less than once per day.
(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	A sanction policy must be established by the business associate or covered entity on the communication system – termination or suspension is established by entity “system administrator”. In the case of an individual client or the identified violation by a client user within the entity, the individual is responsible for compliance with the policies and procedures. that are in concert with HIPAA. Violation of those policies and procedures constitutes immediate suspension of privileges of use.
(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	SafetySend provides system activity review under an “audit trail” by retained history of “secure” transmissions outside the system as well as equal history transmissions within the system.
(2) Standard: 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.	The entity designates their “System Administrator” who becomes the assigned responsible party. This system administrator has access to review, modify or suspend user privileges.
(3)(i) Standard: 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.	Specific access is authorized by the System Administrator. Non Access and Sanction policy is established by the covered entity – termination or exclusion is established by entity “system administrator”. Authorized access requires two levels of authentication initiate client user identification; dual identity verification to change password

(ii) Implementation specifications:	
(A) Authorization and/or supervision (Addressable). 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.	Authorization is addressed in (2) & (3)(i)(a)(4)
(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	System Administrator establishes clearance procedure and authorizes access to system. Individual client users self administrate.
(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or required by paragraph (a)(3)(ii)(B) of this section.	<p>Multiple entities and business associates working together must have a Non Access and Sanction policy is established in behalf of the covered entity – termination or exclusion is established by entity “system administrator”.</p> <p>Authorized access to must require two levels of authentication initiate client user identification; dual identity verification to change password.</p> <p>System Administrator must have authority to deny access to any user. In the case of an individual client or the identified violation by a client user within the entity, the individual is responsible for compliance with the policies and procedures of the business associates that are in concert with HIPAA.</p> <p>Violation of those policies and procedures constitutes suspension of privileges.</p>
(4) (i) Standard: 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	The System Administrator must implement policies and procedures are consistent with subpart E.
(ii) Implementation specifications:	
(A) Isolating health care clearinghouse functions (Required). 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.	SafetySend allows “blocking” from unauthorized access by the “larger organization”.