Healthcare Compliance Solutions

Protected Trust®

Protecting the Privacy of
Digital Information Assets

Let Protected Trust be your "Safe Harbor"

In the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the U.S. Department of Health and Human Services (HHS) was appointed by the U.S. Congress to issue regulations requiring breach notifications for unsecured protected health information (PHI).

The HHS has defined unsecured PHI as protected health information "that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through a technology or methodology."1 Only encryption and destruction are approved methods to render PHI as secure. Because of this, basic access controls and firewalls are not enough to secure PHI.

The final rule makes it clear that the HITECH act does not require PHI encryption. However, the safe harbor rule allows that if PHI is secured (encrypted), then any data breach does not have to be disclosed since no harm will come to an individual if the lost or stolen data cannot be linked to a particular person.

Keeping PHI secure in transit over electronic networks is also critical to comply with the HITECH safe harbor rule. Appropriate steps must be taken to ensure that PHI sent through email or other networks remain secure. Encryption of email messages in an easy way to ensure the security of PHI in transit, as well as at rest.

1. HHS. 45 CFR φ164.402

HITECH Act. Penalties:

General failure to comply is $100 per penalty; violations of an identical requirement may not exceed $25,000 per year. More severe penalties also apply to more important HIPAA violations resulting in a $25,000 to $50,000 and punishable with one to ten years imprisonment.

More than just a Vendor

Before HITECH, there was no accountability for Business Associates (BA) to comply with the existing HIPAA rules. Now that the HITECH Act is in effect, BAs are required to follow the same regulations as the Covered Entities (CE) they work with. In other words: The covered entity and provider share more responsibilities. The act requires, for example, the BA to report security breaches to CEs consistent with their notification requirements. In addition, the BA is liable to the same legal consequences as the CE.

Under section 164.314 of the HIPAA security rules, BAs are required to implement "administrative, physical and technical safeguards [to ensure] the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity." This means that Business Associates are obligated to maintain reasonable and appropriate security practices. On the following pages you will find a detailed explanation of our safeguards and controls to help you comply with the new requirements imposed by HITECH.

"Our guiding principles focus on the privacy of personal information and on the right to securely communicate. We care about protecting information in your email. This is what forms trust."

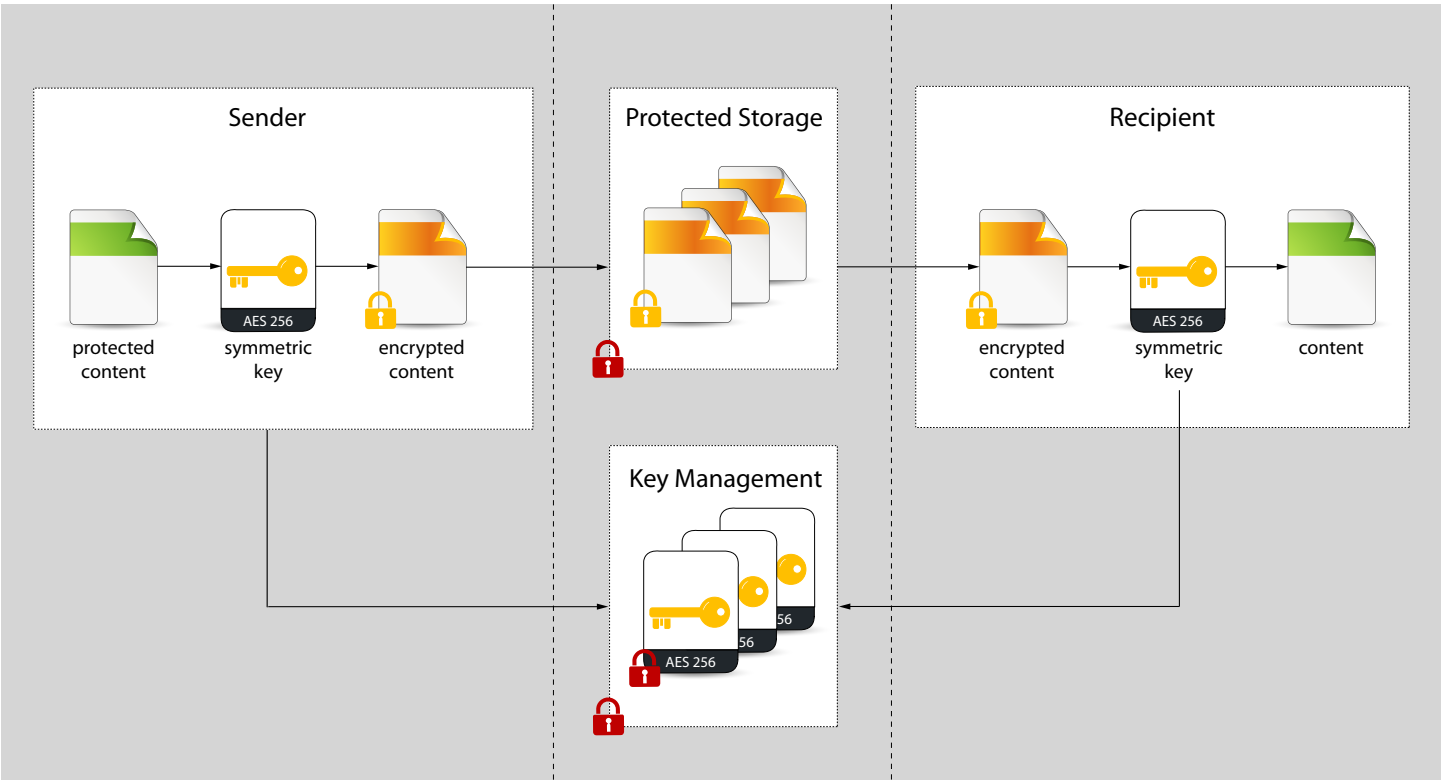
Ingram Leedy
@protectedtrust

Protected Trust Email Encryption's response to the HIPAA Administrative Simplification Code of Federal Regulations, Title 45, Part 164: Security & Privacy

Organizational Requirements (see 164.314)				
Sections	Standards	Implementation Specifications		Application Functionality
§164.314(a)(1)	Business associate contracts or other arrangements	Business associate contracts	Required	Protected Trust implements **administrative**, **physical**, and **technical safeguards** that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that a covered entity creates, receives, maintains, and transmits thru the Protected Trust service.
Technical Safeguards (see 164.312)				
Sections	Standards	Implementation Specifications		Application Functionality
§164.312(a)(1)	Access Control	Unique User Identification	Required	Use of unique user identification and authorization for registered users. Unregistered user identification policy options: •Phone verification using SMS or voice verification code •Shared secret or passphrase (e.g. account number, password, identifiable information) •Email address only verification
		Emergency Access Procedure	Required	Protected email communications can be accessed from any location via secure Internet connection with the proper security authorization.
		Automatic Logoff	Addressable	Use of policy controlled automatic inactivity logoff for private and public workstations.
		Encryption and Decryption	Addressable	Encryption technologies are used with one or more cryptographic keys to encrypt and decrypt data at rest and at transit. Key Management is based on NIST SP 800-57. Additionally, Transport Layer Security (TLS) cryptographic protocols are used for all transport communications security.
§164.312(b)	Audit Control	-	Required	Detailed audit reports are available of use, delivery, logins, and inactivity.
§164.312(c)(1)	Integrity	Mechanism to Authenticate ePHI	Addressable	Cryptographic hashing technologies ensure that information in transit and at rest have not been altered or destroyed in an unauthorized manner.
§164.312(d)	Person or Entity Authentication	-	Required	Use of unique user identification and authorization for registered users. Unregistered user identification policy options: •Phone verification using SMS or voice verification code •Shared secret or passphrase (e.g. account number, password, identifiable information) •Email address only verification
§164.312(e)(1)	Transmission Security	Integrity Controls	Addressable	Cryptographic hashing technologies ensure that information in transit and at rest have not been altered or destroyed in an unauthorized manner.
		Encryption	Addressable	The Advanced Encryption Standard (AES) specifies a FIPS-approved (FIPS PUB 197) cryptographic algorithm used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm uses a cryptographic key of 256 bits to encrypt and decrypt data.
Physical Safeguards (see 164.310)				
Sections	Standards	Implementation Specifications		Application Functionality
§164.310(a)(1)	Facility Access Controls	Contingency operations	Addressable	Protected Trust has established policies and procedures to that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode plan in the event of an emergency.
		Facility Security Plan	Addressable	Protected Trust has implemented policies and procedures to safeguard the facilities and equipment from unauthorized physical access, tampering, and theft.
		Access control and validation procedures	Addressable	Protected Trust has implemented procedures to control and validate personnel access to facilities based on their role and function, including visitor control, and control of access to software systems.
		Maintenance records	Addressable	Protected Trust has implemented policies and procedures to document repairs and modifications to the physical components of facilities which are related to security.
§164.310(d)(1)	Device and media controls	Disposal	Required	Protected Trust implements policies and procedures to address the final disposition of electronic protected health information, and the hardware and electronic media on which it is stored.
		Media re-use	Required	Protected Trust has implemented procedures for removal of electronic protected health information from electronic media before the media is made for re-use.
		Accountability	Addressable	Protected Trust maintains records of the movements of hardware, electronic media, and personnel.
		Data backup and storage	Addressable	Protected Trust can create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Administrative Safeguards (see 164.308)				
Sections	Standards	Implementation Specifications		Application Functionality
§164.308(a)(1)	Security Management Process	Risk Analysis	Required	We place great emphasis on information security and privacy. We have developed a robust, multi-faceted information risk and security program, which incorporates world-class security practices and operating procedures.
		Risk Management	Required	With the commitment of top-level management, we have put in place a strong security organization using international standards to guide policy development from which crucial security processes are identified.
		Sanction Policy	Required	Protected Trust works with the CE to comply with their sanction policies and procedures.
		Information System Activity Review	Required	Protected Trust provides comprehensive reports of activity and regular review of system activity, such as audit logs, access reports, and security incident tracking reports.
§164.308(a)(2)	Assigned Security Responsibility	-	Required	Protected Trust personnel will work with the CE's Security Officer to ensure that data protection policies adhere to the policy and procedures of the CE.
§164.308(a)(3)	Workforce Security	Authorization and/or Supervision	Addressable	Protected Trust services are designed to ensure that only those personnel with appropriate application rights have access to ePHI.
		Workforce Clearance Procedure	Addressable	Protected Trust ensures our personnel have proper security screening and clearance.
		Termination Procedures	Addressable	As a part of the CE's termination procedures, Protected Trust and service solutions allow authorized CE personnel to de-authorize access to electronic protected health information of CE's employees. Additionally, Protected Trust implements procedures and policies for terminating personnel.
§164.308(a)(4)	Information Access Management	Isolating Health care Clearinghouse Function	Required	Protected Trust and service allows the CE to isolate data protection to authorized personnel and protect the electronic protected health information from the larger organization.
		Access Authorization	Addressable	Protected Trust and service allow the CE to implement policies and procedures for granting access to electronic protected health information.
		Access Establishment and Modification	Addressable	Protected Trust and service allow the CE to implement policies and procedures for granting and modifying a user's access to electronic protected health information and encryption protection.
§164.308(a)(5)	Security Awareness and Training	Security Reminders	Addressable	Protected Trust will participate in a CE's periodic security updates on an as needed basis.
		Malicious Software Protection	Addressable	Protected Trust maintains procedures for guarding against, detecting, and reporting from malicious software.
		Log-in Monitoring	Addressable	Protected Trust records log on activity. This activity information can be provided to the covered entity as needed.
		Password Management	Addressable	Protected Trust architecture is designed specifically so that only those personnel with appropriate rights as well as encryption passwords have access to ePHI.
§164.308(a)(6)	Security Incident Procedures	Response and Reporting	Required	Protected Trust continuously identifies, responds, and documents suspected or known security incidents and their outcomes.
§164.308(a)(7)	Contingency Plan	Data Backup Plan	Required	Protected Trust has implemented procedures to create and maintain backup copies of electronic protected health information.
		Disaster Recovery Plan	Required	Protected Trust has established and implemented procedures to restore any loss of data.
		Emergency Mode Operation Plan	Required	Protected Trust has established and implemented procedures to enable continuation of critical business processes for protection of security of electronic protected health information while operating in emergency mode.
		Testing and Revision Procedure	Addressable	Protected Trust implements, periodically tests, and revises continuity plans.
		Applications and Data Criticality Analysis	Addressable	Protected Trust assesses the relative criticality of specific applications and data to support contingency plans.
§164.308(a)(8)	Evaluation	-	Required	CE can contract with Protected Trust Professional Services for periodic evaluation of backed up data integrity and the recovery process.
§164.308(b)(1)	B.A. Contracts and Other Arrangement	Written Contract or Other Arrangement	Required	Protected Trust will work with the CE to provide assurances that appropriate safeguards are met through a written contract or other arrangements per applicable requirements of §164.314(a).

Email Encryption - Architecture



A client may be in the form of Microsoft Outlook 2007, Microsoft Outlook 2010 (x32)/(x64) using the **Protected Trust Email Encryption add-in** or **web-based portal** for Microsoft Internet Explorer, Apple Safari, Google Chrome, or Mozilla Firefox browsers.

Each **(1) message is encrypted by the sending client** with a **(2) unique symmetric key** to create **(3) encrypted content**. The content is sent to the **(4) Protected Trust storage service** and made available for the recipient until expiration.

The sending client transfers the symmetric key to the **(5) Protected Trust Email Encryption key management service** and discards the original key.

On proper recipient authentication and rights authorization, the encryption key is provided to the recipient and combined with the encrypted content to reconstitute the original content data.

About Protected Trust

Protected Trust brings to the market the synergy between several products and services focused on just one thing – risk management for a company's digital assets. Protected Trust combines operational experience, a physically secure infrastructure, cloud based managed services, and an expert culture of security and privacy.

Protected Trust | Protecting the Privacy of Digital Information Assets