SecureShare Hipaa Guide

SecureShare is not a Hipaa compliant solution by itself. SecureShare is a way to help you become Hipaa compliant.

What is Hipaa:

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").1 The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

What Privacy Rules SecureShare can help you meet:

Standard	Section	Specification
Encryption and decryption	164.312 (iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.
Transmission security	164.312 (e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
Encryption	164.312 (ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

How SecureShare Helps Meet These Standards:

SecureShare uses Advance Encryption Standard (AES) approved by U.S. National Institute of Standards and Technology (NIST) in 2001. SecureShare uses this standard to secure your private data in two ways.

1. Secure your data while it's in transit or transmission by encrypting your data and producing a file. You then can transport this file in many ways. Examples include but not limited to: Email, FTP, Dropbox, CD-R/CD-RW, USB/Jump drive and portable hard drives.
2. Secure your data while it is at rest. As long as you have created a backup of your encryption keys, you can secure your file to Network Attached Storage (NAS), CD-R/CD-RW, USB/Jump drive and portable hard drives.

Your data is encrypted before it leaves your computer and only decrypted when it reaches the intended recipient. You can control who can decrypt your files by the method of encryption keys. You can send your encryption keys to only individuals that need to decrypt your files.