Is WinZip HIPAA compliant?

- WinZip
- WinZip Command Line Add-on
- WinZip Self-Extractor
- WinZip Courier
- WinZip Enterprise

In today's digital age, data security and privacy are of utmost importance, especially when it comes to sensitive information like personal health records. The Health Insurance Portability and Accountability Act (HIPAA) sets stringent standards to protect the confidentiality, integrity, and availability of protected health information.

WinZip software versions 9 and later include support for AES encryption, using either 128- or 256-bit keys. AES (which stands for the Advanced Encryption Standard) is the symmetric encryption algorithm approved as part of the Federal Information Processing Standard (FIPS) for use by U.S. Government organizations (and others) to protect sensitive information. WinZip's AES encryption feature is a significant advance on the previous Zip 2.0 encryption, which can help meet the need that many users have for protecting confidential information.

In addition to the information above, starting with WinZip version 18.5, WinZip Courier version 7.0, and WinZip Command Line Support Add-on version 5.0, **WinZip Enterprise** can be deployed to take advantage of the Windows FIPS 140-2 validated cryptographic modules when they have been enabled for use on Windows 10/11, Windows 8, or Windows 7 systems through the local or group security policy. If compliance with FIPS 140-2 is a goal, WinZip Enterprise can help ensure that your organization meets government requirements.

However, assuring compliance with HIPAA through the implementation of appropriate policies and procedures to protect personal health information, including administrative, technical and physical safeguards, is the responsibility of each organization subject to the HIPAA requirements. Each operational situation is unique, and each organization needs to evaluate for themselves how WinZip's data encryption features will fit into their environment.

The encryption algorithm used in WinZip is only one part of the overall data protection equation, and there are other considerations to keep in mind. For example, WinZip uses password-based encryption, and even a strong encryption algorithm like AES is of little or no benefit if the passwords used are weak, or if one does not keep track of them securely.

It should be noted that WinZip's encryption applies only to the contents of files stored within a Zip file (.zip or .zipx). Information about an encrypted file, such as its name, date, size, attributes, and compression ratio, is stored in unencrypted form in the Zip file's directory and can be viewed, without a password, by anyone who has access to the Zip file.

Also, WinZip's encryption method is not the same thing as an authentication method for the Zip file. WinZip's encryption scheme is intended to prevent someone who does not know the correct password from finding out the contents of your encrypted data. The password is not needed, however, for actions that do not involve decryption of the encrypted contents of a Zip file. In particular, encrypted files can be deleted from a Zip file, or renamed within the archive, and new, unencrypted, files can be added to the Zip file, without a password.

This Statement does not constitute a warranty or extend the terms of any existing warranty. Unless one has a different license agreement signed by WinZip Computing, use of WinZip software is governed by the terms in the license agreement included with the product. One should consult legal counsel for specific questions related to one's use of WinZip software in a particular HIPAA compliance plan.
