HIPAA COMPLIANCE & MyWorkDrive

HIPAA Compliance and MyWorkDrive

The HIPAA act of 1996 was updated and strengthened by the HITECH Act of 2009. Since 1996, HIPAA changed the way organizations create, receive, maintain, and transmit PHI. Efforts to protect United States citizens from data theft, and ensure sensitive healthcare information is only revealed to appropriate parties include the:

- Original HIPAA rule–August 21, 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act–February 18, 2009
- Final omnibus rule – January 25, 2013

These rules provide additional guidance and authority for the Office of Civil Rights (OCR) to enforce HIPAA compliance through audits and financial penalties

Compliance Requirements

The key is to ensure that you have the highest level of safeguards that allows your business to provide health services without impediment yet not be so costly as to divert excessive financial resources from health care. The HIPAA Security Rule includes very specific technical safeguards that any file storage and access solution needs to meet in order to keep your business from committing any violations.

MyWorkDrive enables healthcare organizations and their supporting business associates to implement controls in a manner that assists them in complying with HIPAA and HITECH. The following table demonstrates how the features of MyWorkDrive support each of the HIPAA technical safeguards.

Note: This white paper is intended to provide an overview of MyWorkDrive and is not intended to provide legal advice. For more comprehensive information on regulations and their implications, please consult your legal counsel.

MyWorkDrive

Wanpath, LLC
605 Market Street, Suite 410
San Francisco, CA 94105

Standards	Implementation Specifications	How MyWorkDrive Helps
Access Control 164.312(a)(1)	Unique User ID (R)	MyWorkDrive leverages Window's and Unix's systems to support unique user IDs for full accountability along the Identification --> Authentication --> Authorization --> Accounting (Auditing) chain to insure meeting the "identifying and tracking user identity" HIPPA requirement.
Access Control 164.312(a)(1)	Emergency Access Procedure (R)	MyWorkDrive's enhanced data retention and archiving features support many scenarios covered by HIPAA's Emergency Access Procedure (EAP) technical safeguard. Policies and procedures required by this safeguard are supported by easy-to-configure administrative settings. MyWorkDrive's stand-out feature of virtually universal access to data as needed, anywhere in the world with internet access, supports EAP incidents where a loss of a location occurs without compromising data security.
Access Control 164.312(a)(1)	Automatic Logoff (A)	MyWorkDrive furnishes a fully configurable automatic logoff feature that is centrally managed, which allows your business to set the amount of time for inactivity to require re-authenticating to access your protected files.
Access Control 164.312(a)(1)	Encryption and Decryption (A)	MyWorkDrive supports any Windows, SAMBA-related UNIX, or Application level encryption for data at rest without compromising data protection. Enabling secure access to your files from anywhere also gives your administrators flexibility of access of key storage systems.

MyWorkDrive

Wanpath, LLC
605 Market Street, Suite 410
San Francisco, CA 94105

Standards	Implementation Specifications	How MyWorkDrive Helps
Audit Controls 164.312(b)	Also supporting - Information System Activity Review 164.308(a)(1)(ii)(D)	MyWorkDrive provides a detailed logging function that meets or exceeds HIPAA standards for auditing. Audit logs can be searched based on keywords or exported as needed for additional discovery.
Integrity 164.312(c)	Prevent or detect improper alteration and destruction -Mechanism to authenticate ePHI (A)	MyWorkDrive implements contingencies to help you avoid accidental file deletion and irreparable data loss. Options to restrict opportunities to exfiltrate protected ePHI from the system are available through features to disable downloading through our data loss prevention (DLP) feature.
Person or Entity Authentication 164.312(d)	STANDARD ONLY	MyWorkDrive supports complex password/ passphrase requirements and has implemented Duo Security for the option of Two Factor Authentication to meet HIPAA requirements for sensitive ePHI access.
Transmission Security 164.312(e)(1)	Integrity Controls (A) & Encryption (A)	MyWorkDrive insures all data connections are protected by TLS v1.2 level of encryption to "guard against unauthorized access to ePHI that is being transmitted over an electronic communications network."

**Please note that "addressable implementation specifications should not be thought of as optional - addressable means that covered entities are allowed to determine whether a given addressable specification is "reasonable and appropriate" for their specific business.*

MyWorkDrive

Wanpath, LLC
605 Market Street, Suite 410
San Francisco, CA 94105