

WipeDrive and HIPAA Compliance

COMPLIANCE BACKGROUND

The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, verbal, electronic, etc.

First enacted in 1996, the HIPAA regulations have been regularly updated by the US legislation to specifically address the following:

- Provide the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs.
- Reduce health care fraud and abuse.
- Mandate industry-wide standards for health care information on electronic billing and other processes.
- Require the protection and confidential handling of protected health information.



WHAT IS PHI?

Protected Health Information

- Patient name
- Address
- Birthdate
- Social Security Number
- Physical or mental condition
- Care provided
- Payment information
- Other identifying information

PROTECTING PHI

An important part of the HIPAA regulation is the management and protection of protected health information (PHI), including:

- The patient's name, address, birth date and Social Security number.
- An individual's physical or mental health condition.
- Specifics about care provided to an individual.
- Information concerning the payment for the care provided to the individual that identifies the patient.
- Information for which there is a reasonable basis to believe could be used to identify the patient.

In 2016, the HIPAA legislation added the ability to fine and penalize organizations for the disclosure, breach or loss of PHI. When a breach occurs, organizations must notify the patients affected and the Office of Civil Rights. The OCR then reviews the policies of the organization and can decide if there is a need for fiscal penalties. The types of penalties are divided into different classes:

	Fine Per Violation	Annual Maximum
Unknowing violation of HIPAA	\$100	\$25,000
Reasonable cause for violating HIPAA	\$1,000	\$100,000
Willful neglect of HIPAA, corrected in given time period	\$25,000	\$250,000
Willful neglect of HIPAA, violation remains uncorrected	\$50,000	\$1,500,000
Maximum penalty for all of these violations	\$50,000	\$1,500,000

HOW DOES WIPEDRIVE COMPLY?

The WipeDrive software removes all data, including any PHI from the IT asset with an industry standard wiping protocol. After the wipe, WipeDrive verifies the media to ensure that the wipe is successful. WipeDrive will then provide an auditable Wipe Report as confirmation that all PHI and other data on the drive is securely erased. The organization can then present these reports as proof of HIPAA compliance in their IT Policy.

CONCLUSION

When enacted as part of an organization's Data Security Policy, WipeDrive provides proof of PHI erasure on the IT asset. Clients who have incorporated WipeDrive have been able to acquire and maintain HIPAA compliance.

Improperly erased drives can lead to data leaks that cost your organization hundreds of thousands of dollars. Don't put off your data security. Contact White Canyon Software today to learn more about how we can help you secure PHI.