HIPAA Compliance

Safeguarding client data, including Protected Health Information (PHI), is a top priority at SpeakWrite. Our privacy & security policies and procedures adhere to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 as outlined below.

The HIPAA Privacy Rule

SpeakWrite does not facilitate health care treatment, payment or operations for our clients but does process client dictations and documents that may contain Protected Health Information (PHI). Therefore, we approach HIPAA's Privacy Rule with the level of emphasis that is expected from all business associates of covered entities. Specifically, we use appropriate safeguards to prevent unauthorized use or disclosure of PHI and treat all of our confidential customer data as though it contained PHI, whether it does or not.

In addition to maintaining strict technical standards under the HIPAA Security Rule, SpeakWrite employees and typists must master an extensive set of procedures which include information pertaining to security, privacy and confidentiality. Examples of activities that are specifically prohibited include:

- Disclosing any client information, including PHI, for any purpose
- Discussing client information in public or private with any person for any reason
- Attempting to contact or contacting clients or anyone connected to them for any reason
- Generating written or printed copies of any client work
- Maintaining any computer file or other record of client materials
- Leaving client information open to view by unauthorized persons

SpeakWrite educates all employees and typists on the importance of protecting client information. All SpeakWrite employees and typists take annual HIPAA training, and sign confidentiality agreements that reinforce our privacy policies and procedures.

The HIPAA Security Rule

This rule concerns security of Electronic Protected Health Information. There are three types of security safeguards outlined in HIPAA: Administrative, Physical and Technical.

Administrative Safeguards

• SpeakWrite has a designated Privacy Officer responsible for developing HIPAA policies and monitoring compliance.

• The Privacy Officer oversees HIPAA and security awareness training for employees and typists.

• The Privacy Officer and Director of Technology jointly conduct ongoing security risk assessments and manage risk mitigation efforts.

• SpeakWrite follows procedures for preventing, detecting, containing, and correcting security violations.

• Documenting the permitted and required uses of PHI, as required by the Privacy Rule

• Contractually agree that SpeakWrite will not use or further disclose the PHI other than as permitted or required by the contract or as required by law

Physical Safeguards

• Restricted access to PHI: SpeakWrite limits PHI access to individuals with the required access authority and appropriate clearances.

• Data center operations: Systems are deployed through Microsoft Azure's Government Cloud, leveraging Azure best practices for physical security and data center operations.

Technical Safeguards

• Encryption: All data is encrypted during transmission and at rest using industry best practices.

• Policies & updates: Security policies and procedures are maintained and regularly reviewed; systems are updated to follow current industry best practices and applicable laws.