Wecounsel is committed to the security of the Protected Health Information that is stored and transmitted through our software and we maintain policies and procedures in keeping with regulatory requirements involving the following: Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d), HIPAA Security Rule as defined by the Code of Federal Regulations, 45 C.F.R. 160, 162 and 164 and Code of Federal Regulations, 45 C.F.R. 164.306(b)(2)(i).

Password Management Systems

- Enforces users to maintain accountability for individual user IDs and passwords.
- Allows users to select and change their own passwords and includes a confirmation procedure to allow for input errors.
- Requires quality, “strong”, passwords.
- Enforces password changes:
- Forces users to change temporary passwords at the first log-on.
- Maintains a record of previous user passwords and prevent re-use.
- Passwords cannot be displayed on the screen when being entered.
- Password files must be kept separately from application system data.
- Passwords that are stored and transmitted must be in protected (e.g. encrypted or hashed) form.

Session Time-Out

- Time-out facility parameters are set for access to information systems containing EPHI if users are idle for a defined period of inactivity.
- A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity.
- Time-out parameter set to 10 minutes.

PHI Storage/Backup

- We employ a **256 bit AES encryption**.
- A full backup of the system is required at least once daily.
- We require the servers to be stored in a secure location.
- All PHI on film, copy or paper is disposed of in house and EPHI is destroyed in accordance with NIST Special Publication 800-88, Guidelines for Media Sanction such that PHI cannot be retrieved.

Wecounsel requires a **Business Associate Agreement** to be signed by any vendor who may come in contact with PHI and we provide a BAA with all of our providers and partners. We also undergo a **3rd Party Annual Risk Assessment** at minimum to ensure compliance.