General Rules of Behavior for Users of eScribers' Systems that Access, Store, Receive, or Transmit Sensitive Information

Rules of behavior regarding the access of eScribers' systems (TABula) and the use of its IT resources are a vital part of the eScribers IT Security Program.

Rules of behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

Rules of behavior inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing eScribers' systems for accessing, storing, receiving, or transmitting sensitive information.

These rules of behavior apply to eScribers' employees and contractors who access TABula and other IT systems.

The rules of behavior apply to users in any location including, but not limited to eScribers offices, home or a satellite or customer site.

System Access

- I understand that I am given access to only those systems for which I require access to perform my duties as an employee or contractor.

- I will not attempt to access systems I am not authorized to access.

Passwords and Other Access Control Measures

- I will choose passwords that are at least eight characters long and have a combination of letters (upper- and lower-case) and numbers.

- I will protect passwords and access numbers from disclosure. I will not record passwords or access control numbers on paper or in electronic form and store them on or

with workstations, laptop computers, or PEDs. To prevent others from obtaining my password via “shoulder surfing,” I will shield my keyboard from view as I enter my password.

- I will promptly change a password whenever the compromise of that password is known or suspected.

- I will not attempt to bypass access control measures.

Data Protection

- I will protect sensitive information from disclosure to unauthorized persons or groups.

- I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area, even for a short time; I will log off when I leave for the day.

- I will not email unencrypted copies of transcripts (even partial transcripts) under any circumstances. Files must be securely uploaded and downloaded to and from TABula.

- I will securely delete (not just move to recycle bin) copies of audio and transcripts from my computer once I have uploaded and completed a job and it has been processed and removed from my job queue.

- I will upload my work product to TABula at the end of each workday, even if it is a new job or it is only a few pages, so that if I should suffer a power outage or any other emergency that prevents me from working, the partial transcript and all relevant information is available for the Operations/Production team to re-assign the job.

Software

- I agree to comply with all software copyrights and licenses.

Telecommuting (Including Working at Home)

Employees and contractors who are telecommuting must adhere to the following rules of behavior:

- I will physically protect any laptops or PEDs I use for telecommuting when they are not in use.

- I will protect sensitive data at my telecommuting workplace. This includes properly disposing of sensitive information (e.g., by shredding).

Laptop Computers and Portable Electronic Devices

Rules of behavior that specifically apply to laptop computers and portable electronic devices (PEDs) are listed below.

- I will keep the laptop or PED under my physical control at all times, or I will secure it in a suitable locked container under my control.

- I will take all necessary precautions to protect the laptop/PED against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.

- I will keep antivirus and firewall software on the laptop up to date.

- I will not program the laptop with sign-on sequences, passwords, or access phone numbers.

- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be encrypted.

- I understand and will comply with the requirement that sensitive information processed; stored, or transmitted on wireless devices must be encrypted using approved encryption methods.

Incident Reporting

- I will promptly report IT security incidents.

Accountability

- I understand that I have no expectation of privacy while accessing eScribers' IT systems.

- I understand that I will be held accountable for my actions while accessing and using eScribers IT systems.

Acknowledgment Statement

I acknowledge that I have read the rules of behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of system access, criminal or civil prosecution, or termination.

Name of User (printed):_____

User's Phone Number: _____

User's Email Address: _____

Supervisor: _____

_____ _____

User's Signature Date