



05-Security Awareness and Training

Approved by: William Voss

Review: Annual

Renewed By:

Effective: March 9, 2025

Revised: April 29, 2025

Renewed:

Security Awareness and Training

Policy Statement

It is the policy of River City TMS, PLLC that all workforce members shall receive appropriate training concerning River City TMS, PLLC security policies and procedures. Such training shall be provided on an ongoing basis to all new workforce members and shall be repeated annually for all workforce members.

Procedure

- **Security Training Program** [§164.308\(a\)\(5\)\(i\)](#)

The Security Officer or designee shall have responsibility for the development and delivery of security training provided to all workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats. Security training shall be provided to new workforce members as part of the orientation process and to all workforce members on an ongoing basis. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer or designee shall be responsible for maintaining appropriate documentation of all training activities ([Appendix G](#) – Workforce Training Log).

The Security Training Program will address all aspects of the *Information Security Policy*, which should include, but not be limited to, the following topics.

- **Security Reminders** [§164.308\(a\)\(5\)\(ii\)\(A\)](#)

The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, and discussions during staff meetings, screensavers, log-in banners, newsletter/intranet articles, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic

security reminders ([Appendix G](#) – Workforce Training Log).

The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

• **Protection from Malicious Software** [§164.308\(a\)\(5\)\(ii\)\(B\)](#)

The Security Officer shall provide training concerning the prevention, detection, containment and eradication of malicious software. Such training shall address the following:

- The malicious software protection mechanism that is in place
- The workforce members' roles in malicious software protection procedures, i.e., how to recognize suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail; instructions to never download files from unknown or suspicious sources; guidance on the damage caused by viruses and worms; guidance on recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software
- Actions to be taken in response to malicious software detection
- The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current
- The importance of backing up critical data on a regular basis and storing the data in a safe place

• **Log-in monitoring** [§164.308\(a\)\(5\)\(ii\)\(C\)](#)

The Security Officer shall provide training on workforce members' roles and responsibilities in monitoring log-in attempts and reporting discrepancies. Such training shall include the following:

- Identification of how log-in monitoring is conducted
- How to identify an inappropriate or attempted log-in
- Action to be taken in response to an inappropriate or attempted log-in

• **Password Management** [§164.308\(a\)\(5\)\(ii\)\(D\)](#)

The Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the requirements relating to passwords. The following processes may be addressed:

- Commonly used words, names, initials, birthdays or phone numbers shall not be used as passwords.
- Passwords shall be required to be a minimum of 8 characters.
- Passwords shall contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Passwords shall not be shared, written down, posted or exposed in an insecure manner, such as on a notepad or posted on the workstation, and shall not be stored within a file or database on a workstation.
- Passwords shall be masked or suppressed on all online screens and will never be printed or included in reports or logs.
- Passwords shall not be disclosed to other workforce members (including anyone claiming to need a password to "fix" a computer or handle an emergency situation) or

individuals, including family members.

- A password shall be promptly changed if it is suspected of being disclosed or known to have been disclosed.
 - Passwords shall be changed Every 90 days Compromised passwords shall be changed immediately.
 - Employees shall refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
 - Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.
- **Breach Notification Rule** [§164.530\(b\)](#)

All workforce members shall receive training pertaining to the Breach Notification Rule ([Policy 12](#)). A record of the training materials and workforce members' attendance at trainings shall be maintained ([Appendix G](#) - Workforce Training Log).