



## 07-Workstation, Device Security

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

---

# Workstation & Device Security

## Policy Statement

The first line of defense in data security is each individual user within River City TMS, PLLC. A User is any person (River City TMS, PLLC workforce member or contractor) authorized to access an information resource. It is the policy of River City TMS, PLLC to ensure that proper functions are in place and the physical attributes of the surroundings of a workstation are addressed in order to prevent unauthorized access to ePHI.

It must be assumed that any external media in the possession of a workforce member is likely to contain either protected health information ("PHI") or other sensitive information. It is the policy of the River City TMS, PLLC to govern the receipt and removal of hardware and electronic media that contain ePHI into and out of the facility and the movement of these items within the facility.

## Procedure

- **Workstation Use** [§164.310\(b\)](#)

- **Inventory**

An inventory () shall be maintained and periodically updated of the location and types of each workstation and shall include:

- Classification of each workstation based on workstation capabilities, connection, and allowable activities

- **Prohibited Activities**

Workforce members will be prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document:

- Deliberately crashing an information system.
    - Attempting to break into an information resource or to bypass a security feature, including running password-cracking programs or sniffer programs, and

attempting to circumvent file or other resource permissions.

- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system

Exception: Authorized information system support personnel, or others authorized by River City TMS, PLLC Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

- The willful, unauthorized access or inspection of confidential or sensitive information to which the workforce member has not been approved on a "need to know" basis is prohibited.
- Use of personal software is prohibited. All software installed on River City TMS, PLLC computers must be approved by River City TMS, PLLC.
- Violating or attempting to violate the terms of use or license agreement of any software product used by River City TMS, PLLC is strictly prohibited.
- Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of River City TMS, PLLC is strictly prohibited.

#### • **Electronic Communications, E-mail, Internet Usage**

As a productivity enhancement tool, River City TMS, PLLC encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by River City TMS, PLLC-owned equipment are considered the property of River City TMS, PLLC, not the property of individual workforce member. Consequently, this policy applies to all River City TMS, PLLC workforce members and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

River City TMS, PLLC provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services, are intended for business purposes. However, incidental personal use is permissible as long as:

- it does not consume more than a trivial amount of employee time or resources,
- it does not interfere with staff productivity,
- it does not preempt any business activity,
- it does not violate any of the following:
  - Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
  - Illegal activities – Use of River City TMS, PLLC information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.

- Commercial use – Use of River City TMS, PLLC information resources for personal or commercial profit is strictly prohibited.
- Political Activities – All political activities are strictly prohibited on River City TMS, PLLC premises.
- Harassment – River City TMS, PLLC strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, River City TMS, PLLC prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
- Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited.

Generally, while it is NOT the policy of River City TMS, PLLC to monitor the content of any electronic communication, River City TMS, PLLC is responsible for servicing and protecting River City TMS, PLLC equipment, networks, data, and resource availability and, therefore, may be required to access and/or monitor electronic communications from time to time. River City TMS, PLLC reserves the right, at its discretion, to review any workforce member’s files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as River City TMS, PLLC policies. Workforce members will structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Special precautions are required to block Internet (public) access to River City TMS, PLLC information resources not intended for public access, and to protect confidential River City TMS, PLLC information when it is transmitted over the Internet. The following security and administration issues shall govern Internet usage:

- Prior approval of River City TMS, PLLC Security Officer or appropriate personnel authorized by River City TMS, PLLC shall be obtained before an Internet, or other external network connection, is established;
- Prior approval of River City TMS, PLLC Security Officer or appropriate personnel authorized by River City TMS, PLLC shall be obtained before River City TMS, PLLC information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Workforce members may not install or download any software (applications, screensavers, etc.). If users have a need for additional software, the user is to contact the Security Officer;

- Use shall be consistent with the goals of River City TMS, PLLC. The network can be used to market services related to River City TMS, PLLC, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services shall be encrypted before being transmitted through the Internet.

The Internet access provided by River City TMS, PLLC will not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, to constantly monitor the weather or stock market results, etc.

- Workforce members must understand that individual Internet usage is monitored, and if a workforce member is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.
- Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by River City TMS, PLLC routers and firewalls. This list is constantly monitored and updated as necessary. Any workforce member visiting pornographic sites will be disciplined and may be terminated.

- **Reporting Software Malfunctions**

Workforce members will inform the appropriate River City TMS, PLLC personnel when the workforce member's software does not appear to be functioning correctly. The malfunction, whether accidental or deliberate, may pose an information security risk. If the workforce member, or the Office Manager, suspects a computer virus infection, River City TMS, PLLC computer virus policy will be followed and these steps will be taken immediately:

- Stop using the computer.
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or River City TMS, PLLC Security Officer as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The Security Officer will monitor the resolution of the malfunction or incident and report to the RMT the result of the action with recommendations on action steps to avert future similar occurrences.

- **Transfer of Sensitive/Confidential Information**

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All workforce members must recognize the sensitive nature of data maintained by River City TMS, PLLC and hold all data in the strictest confidence. Any purposeful release of data to which a workforce member may have access is a violation of River City TMS, PLLC policy and will result in personnel action, and may result in legal action.

- **Home Use of River City TMS, PLLC Corporate Assets**

Only computer hardware and software owned by and installed by River City TMS, PLLC will be permitted to be connected to or installed on River City TMS, PLLC equipment. Only software that has been approved for corporate use by River City TMS, PLLC will be installed on River City TMS, PLLC equipment. Personal computers supplied by River City TMS, PLLC will be used solely for business purposes. All workforce members and contractors must read and understand the list of prohibited activities. Modifications or configuration changes are not permitted on computers supplied by River City TMS, PLLC for home use.

- **Transferring Software and Files between Home and Work**

Personal software shall not be used on River City TMS, PLLC computers or networks. If a need for specific software exists, the workforce member should submit a request to the Office Manager. Workforce members shall not use River City TMS, PLLC purchased software on home or on non-River City TMS, PLLC computers or equipment.

River City TMS, PLLC proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of River City TMS, PLLC without written consent of the Office Manager. It is crucial to River City TMS, PLLC to protect all data and, in order to do that effectively River City TMS, PLLC must control the systems in which it is contained. In the event that the Office Manager receives a request to transfer River City TMS, PLLC data to a non-River City TMS, PLLC computer system, the Office Manager should notify the Security Officer or appropriate personnel of the intentions and the need for such a transfer of data.

River City TMS, PLLC Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since River City TMS, PLLC does not control non-River City TMS, PLLC personal computers, River City TMS, PLLC cannot be sure of the methods that may or may not be in place to protect River City TMS, PLLC sensitive information, hence the need for this restriction.

- **Use of Mobile Devices / Bring Your Own Device (BYOD)**

Mobile and BYOD devices are not allowed for any River City TMS, PLLC workforce members

- **Installation of authentication and encryption certificates on the e-mail system**

Any workforce member desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

- **E-mail Encryption Method**

- Hushmail Email Account. We also have access to Efax to read faxes

- **Retention of Ownership**

All software programs and documentation generated or provided by workforce members, consultants, or contractors for the benefit of River City TMS, PLLC shall be the property of River City TMS, PLLC unless covered by a contractual agreement. Nothing contained herein shall apply to software purchased by River City TMS, PLLC employees at their own expense.

- **Workstation Security [§164.310\(c\)](#)**

- **Unrecognized Personnel**

It is the responsibility of all River City TMS, PLLC workforce members to take positive action to provide physical security. If an unrecognized person is seen in a restricted River City TMS, PLLC office location, the workforce member will challenge them as to their right to be there. All visitors to River City TMS, PLLC offices will check in at the front desk. All other personnel must be workforce members of River City TMS, PLLC. Any challenged person who does not respond appropriately will be immediately reported to supervisory staff.

- **Securing Equipment**

Equipment located in high traffic or less secured areas will be physically secured. For example, cable locks may be used on laptop computers or servers to help thwart the theft of sensitive data.

- **Unattended Computers**

Unattended computers will be locked by the workforce member when leaving the work area. This feature will be discussed with all workforce members during yearly security training. River City TMS, PLLC policy states that all computers will have the automatic screen lock function set to automatically activate upon 5 minutes of inactivity. Workforce members will not be allowed to take any action which would override this setting.

- **Monitor Screen Positions**

Monitor and laptop screens will be positioned so that unauthorized users cannot view the screen from office doors, lobby areas, hallways, etc. As needed, privacy screens will be used.

- **Device & Media Controls** [§164.310\(d\)\(1\)](#)

- **Disposal of External Media** [§164.310\(d\)\(2\)\(i\)](#)

It is the responsibility of each employee to identify media which should be disposed of properly and to utilize this policy in its destruction.

All equipment to be disposed of or re-used will be wiped of all data and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

The following steps will be followed as appropriate for circumstances:

- External media will not be thrown into the trash.
- When no longer needed, all forms of external media will be sent to the Security Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.
- A certificate of proper disposal will be obtained from the entity completing the disposal.
- A back-up copy of information will be taken, if necessary, prior to removal.
- CD media will be disposed in the shred bin with other PHI
- Documentation will be made of hardware and electronic media and person responsible for movement of ePHI, equipment and media. ([Appendix I](#) – Media Disposition Log)

- **Media Re-Use** [§164.310\(d\)\(2\)\(ii\)](#)

Before any River City TMS, PLLC computers, hardware, media, devices or other ePHI-containing equipment will be made available for reuse, the Security Officer shall ensure it is wiped clean according to NIST 800-88 guidelines.

- **Accountability** [§164.310\(d\)\(2\)\(iii\)](#)

The Security Officer in conjunction with all applicable workforce members shall maintain a record of the movement into and out of the facility, and the disposition and reuse of all hardware and electronic media that contain ePHI (e.g. Backup tapes, USB drives, CDs, thumb drives, disks, etc.) and the person responsible ([Appendix I](#) – Media Disposition Log) or [Appendix O](#) – IS Inventory.

- **Data Backup and Storage** [§164.310\(d\)\(2\)\(iv\)](#)

River City TMS, PLLC will create a retrievable, exact copy of ePHI information, as needed, before movement of equipment and will keep a record of the ePHI data backup to include:

- When data backups will be conducted
- Type of data that will be backed up

- How data will be backed up, including use of encryption and encryption key management
- Backup data mechanism/solution
- How backup data is secured
- How and where backup ePHI data is physically stored and secured
- How frequently data backups are reviewed or assessed for verification of media reliability and data integrity