



08-Access Management Controls

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Information Access Management

Policy Statement

It is the policy of River City TMS, PLLC to allow access only to those persons or software programs that have been granted access to electronic information systems that maintain ePHI consistent with applicable requirements of HIPAA, and to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain ePHI.

Procedure

- **Access Authorization** [§164.308\(a\)\(4\)\(ii\)\(B\)](#)

All requests for access to ePHI shall be authorized by River City TMS, PLLC Security Officer in conjunction with appropriate organizational leadership. The Security Officer will review any request for access to data, including clearinghouse data, and approve as appropriate to limit unnecessary or inappropriate access to ePHI.

- **Access Establishment & Modification** [§164.308\(a\)\(4\)\(ii\)\(C\)](#)

The Security Officer will establish, document, review, or modify a user's right of access to a workstation, transaction, programs, mobile devices, processes, or other mechanisms in the event the user requires more or less access to PHI, including termination in the event the user no longer needs or is authorized to have access.

Rules for access to resources (including internal and external telecommunications and networks) will be established by the information/application owner or manager responsible for the resources. Access will be granted only by the completion of a Network Access Request Form ([Appendix D](#)). This form will only be initiated by authorized personnel and must be signed by the authorized personnel and the Security Officer.

- **Access Control** [§164.312\(a\)\(1\)](#)

Information resources shall be protected by the use of access control systems. Access control systems will include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.). Only mobile devices, laptops, smart phones, etc. which are approved and authorized by management will be allowed to connect to the network and EHR.

Rules for access to resources (including internal and external telecommunications and networks) will be established by the Security Officer. Access will be granted by the completion of a Network Access Request Form ([Appendix D](#)), which will be initiated by Office Manager member's supervisor, since the Office Manager member's supervisor is the person who most closely recognizes a workforce member's need to access data. Users may be added to the information system, network, or EHR upon the signature of the Security Officer or the Office Manager member's supervisor, who will be responsible for adding the workforce member to the network in a manner and fashion that ensures the workforce member is granted access to data only as specifically requested, and must be signed by the Office Manager member's supervisor and the Security Officer. The IS Inventory ([Appendix O](#)) in combination with the Network Access Request Form ([Appendix D](#)) shall be used to review and document the control of access to ePHI systems.

• **Unique User Identification** [§164.312\(a\)\(2\)\(i\)](#)

The Security Officer in conjunction with the System Administrator will assign individual users unique logon IDs and passwords following access authorization, which will be required in order to gain access to all River City TMS, PLLC networks and workstations. An access control system shall identify each user and prevent unauthorized users from entering or using information resources.

Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- All user logon IDs will be audited as needed and all inactive logon IDs will be revoked. The Office Manager member's supervisor will notify the Security Officer upon the departure of all workforce members and contractors, at which time logon IDs will be revoked.
- The logon ID will be locked or revoked after a maximum of 3 unsuccessful logon attempts, which will then require the passwords to be reset by the appropriate Administrator.
- Users shall be responsible for the use and misuse of their individual logon ID.
- Third party contracts will follow business associates policies.

All passwords will be restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords will conform to restrictions and limitations that are designed to make the password difficult to guess. Users will be required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level.

Security requirements for passwords include:

- Password Length – Passwords will be required to be a minimum of 8 characters.
- Content Requirements – Passwords will contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Change Frequency – Passwords will be changed every 90 days. Compromised passwords shall be changed immediately.
- Restrictions on Sharing Passwords – Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.
- Restrictions on Recording Passwords – Passwords will be masked or suppressed on all online screens and will never be printed or included in reports or logs.

- **Emergency Access** [§164.312\(a\)\(2\)\(ii\)](#)

River City TMS, PLLC shall have formal, documented emergency access procedures enabling River City TMS, PLLC workforce members to obtain required ePHI during a medical emergency. Such access will be authorized by appropriate River City TMS, PLLC management or designated personnel. The procedures shall be outlined in the Emergency Plan ([Appendix J](#)) and shall include:

- Identifying and defining River City TMS, PLLC workforce members that are authorized to access ePHI during an emergency.
- Identifying and defining manual and automated methods to be used by authorized River City TMS, PLLC workforce members to access ePHI during a medical emergency.
- Identifying and defining appropriate logging and auditing that must occur when authorized River City TMS, PLLC workforce members access ePHI during an emergency.

Regular training and awareness on the emergency access procedure will be provided to all River City TMS, PLLC workforce members.

All appropriate River City TMS, PLLC workforce members will have access to a current copy of the procedure and an appropriate number of current copies of the procedure will be kept off-site.

- **Automatic Logoff** [§164.312\(a\)\(2\)\(iii\)](#)

All electronic sessions will be terminated after a predetermined time of inactivity as appropriate for user role and security.

- **Encryption and Decryption** [§164.312\(a\)\(2\)\(iv\)](#)

Sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. River City TMS, PLLC will employ several methods of secure data transmission, including but not limited to the following:

- Installation of authentication and encryption certificates on the e-mail system – Any user desiring to transfer secure e-mail with a specific identified external user may

request to exchange public keys with the external user by contacting the Security Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

- ■ Hushmail Email Encrypted Account
- File Transfer Protocol (FTP) – Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Security Officer or appropriate personnel.
- Secure Socket Layer (SSL) Web Interface – Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form ([Appendix D](#)) and have appropriate approval from the supervisor or department head as well as the Security Officer or appropriate personnel before any access is granted.

- **Audit Controls** [§164.312\(b\)](#)

River City TMS, PLLC shall implement hardware, software, and/or procedural mechanisms to record and examine activity over all information systems that contain ePHI.

River City TMS, PLLC shall determine the audit control capabilities available within its information systems and shall generate the required audit reports from the system in the frequency required to appropriately examine information system activity.

River City TMS, PLLC shall maintain documentation of its systems audit control capabilities and activity audits ([Appendix B](#) – Audit Log).

- **Person or Entity Authentication** [§164.312\(d\)](#)

Prior to granting access to ePHI, River City TMS, PLLC management shall verify that the person or entity seeking access to ePHI is the one claimed and will communicate with the Security Officer who the appropriate person or entity is, the exact access required, and duration.