



02-Security Management Process

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Security Management Process

Policy Statement

It is the policy of River City TMS, PLLC to prevent, detect, contain, and correct security violations to maintain the confidentiality, integrity and availability of ePHI held by River City TMS, PLLC, and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Procedure

- **Risk Management** [§164.308\(a\)\(1\)\(ii\)\(B\)](#)

River City TMS, PLLC has established a risk management process that includes:

- Risk Management Team (RMT) to identify areas of concern within the River City TMS, PLLC and to act as the first line of defense in enhancing the appropriate security posture;
- Risk management framework for implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
- Regular assessment of risk by performing a security risk analysis and ongoing security evaluations;
- Response, containment and correction of risk; and
- Monitoring of risk over time.

The RMT is defined in [Policy 1: Introduction to the Information Security Policy](#). The RMT will:

- Address security issues in the Security Incident Report ([Appendix H](#)) as they arise.
- Recommend and approve immediate security actions to be undertaken.
- Schedule meetings Quarterly for the purpose of discussing privacy and security issues and to review concerns that arose since the previously scheduled meeting.

- Track RMT meeting attendance via the RMT Meeting Attendance Log ([Appendix A](#))
- Identify areas that should be addressed during annual training.
- Review/update privacy and security policies as necessary.
- Be responsible for maintaining a log of security concerns or confidentiality issues ([Appendix M](#) – Security Log). This log will be maintained on a routine basis and will include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed periodically.
- After the appropriate systems and the corresponding threats have been identified, the RMT will evaluate the extent to which the failure of these systems will impact the River City TMS, PLLC. In minimizing exposure to handle the risk, there is the option to accept the risk and do nothing if the system or equipment will not be worth the resources it will require to protect them from the security risk. The choice to mitigate the risk by selecting appropriate security measures to be put into place will be prioritized by determining their centrality to business operations both operationally and financially and how it would impact the ability to deliver quality health services.

- **Security Risk Analysis** [§164.308\(a\)\(1\)\(ii\)\(A\)](#)

River City TMS, PLLC shall assess annually, or as necessary considering changes to business practices and technological advancements, the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards. This assessment will be completed to determine the extent to which security safeguards are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. River City TMS, PLLC will use a Security Risk Analysis tool by which it will help determine the probability and criticalities generating a risk score for each identified risk.

The Security Officer shall be responsible for coordinating River City TMS, PLLC risk analysis and shall identify appropriate persons within River City TMS, PLLC to assist with the risk analysis. The Security Officer shall evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis.

The risk analysis shall also include the following documentation:

- Identified threats and vulnerabilities, assessment of current security measures, impact and likelihood analysis, and risk rating.
 - Inventory of all information systems that create, transmit, maintain, or transmit ePHI (i.e., network devices, workstations, printers, scanners, mobile devices, operating systems, various applications, interfaces), including date acquired, location, vendor, licenses, maintenance schedule, and function.
 - Network diagram illustrating how River City TMS, PLLC information system network is configured.
 - List of current business associates
- **Security Incident Procedures** [§164.308\(a\)\(6\)\(i\)](#), [§164.308\(a\)\(6\)\(ii\)](#)
A security incident is an event that impacts the confidentiality, integrity, or availability of ePHI. A security incident may include, but is not limited to:

- ePHI data loss due to disaster, system failure, or user error
- Password sharing
- Unauthorized persons/visitors/vendors/contractors accessing a system, or in an area containing ePHI
- Virus, worm, or other malicious code attacks
- Network or system intrusions
- Persistent intrusion attempts from a particular entity
- Theft or vandalism

Workforce members are responsible for the day-to-day, hands-on security of an information resource. It is the responsibility of each River City TMS, PLLC workforce member or contractor to report perceived security incidents immediately and on a continuous basis to the Security Officer or a member of the RMT. Members of the RMT are specified in [Policy 1: Introduction to the Information Security Policy](#). An incident report form ([Appendix H – Security Incident Report](#)) will be filled-out that captures the date the incident occurred, the workforce member involved with the incident, the nature of the incident, and any ePHI that was accessed or inappropriately disclosed. The RMT will review the incident report and will determine the appropriate steps for mitigation of the incident.

Reports of security incidents shall be escalated as quickly as possible. Each member of the River City TMS, PLLC RMT must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents shall be logged ([Appendix M – Security Log](#)) and the remedial action indicated. It shall be the responsibility of the RMT to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the River City TMS, PLLC Security Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

- **Information System Activity Review** [§164.308\(a\)\(1\)\(ii\)\(D\)](#)

The Security Officer shall on a periodic basis review records of information system activity, such as audit logs, access reports and security incident tracking reports, or those deemed appropriate as determined by vendor agreements. The Security Officer will maintain a record of these reviews ([Appendix B – Audit Log](#)). The reviews shall include, but shall not be limited to:

- Logins – Identify multiple failed login attempts, account lockouts, and unauthorized access.
- Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
- User Accounts – Review user accounts within all systems to ensure users who no longer have a business need for information systems no longer have such access to the information and/or system.

- **Evaluation of Security Controls & Processes** [§164.308\(a\)\(8\)](#)

The Security Officer shall be responsible for identifying appropriate times to conduct periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security Rule, and subsequently in response to environmental or operational changes affecting the security of ePHI. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. The Security Officer shall coordinate such evaluations and identify appropriate persons within River City TMS, PLLC to assist with such evaluations.

Follow-up evaluations shall include the following:

- Inspections, reviews, interviews, and analysis to assess the adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for accuracy and completeness; and inspection and analysis of training, incident, and media logs for compliance.
- Analysis to assess the adequacy of controls within the network, operating systems and applications. As appropriate, River City TMS, PLLC shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvements.

- **Policy & Procedure Requirements [§164.316\(b\)\(1\)](#)**

River City TMS, PLLC will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule.

- Time Limit [§164.316\(b\)\(2\)\(i\)](#) – Documentation will be retained of policies, procedures, actions, activities or assessments required by the HIPAA Security Rule for six years from the date of its creation or the date when it last was in effect, whichever is later.
- Availability [§164.316\(b\)\(2\)\(ii\)](#) – Documentation will be made available to those persons responsible for implementing the procedures to which the documentation pertains.
- Updates [§164.316\(b\)\(2\)\(iii\)](#) – Periodic review of documentation will occur and will be updated as needed in response to environmental or operational changes affecting the security of ePHI.