



11-Business Associates Contracts

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Business Associates Contracts

Policy Statement

It is the policy of River City TMS, PLLC to implement with its business associates and contractors a formal contract or other arrangement that complies with the applicable requirements of the Security Rule.

Procedure

- **Business Associate Contracts and Other Arrangements**

- Contract [§164.314\(a\)\(1\)](#), [§164.308\(b\)\(3\)](#) – River City TMS, PLLC shall use a standard business associate contract with business associates and subcontractors to which it discloses ePHI ([Appendix Q – BAA](#)) that complies with the applicable requirements of the Security Rule. Any agreements that deviate from standard business associate contracts shall be evaluated by the RMT before approval is granted. River City TMS, PLLC will retain a file of all business associate contracts.
- Business Associates [§164.308\(b\)\(1\)](#), [§164.314\(a\)](#) – River City TMS, PLLC shall permit its business associate to create, receive, maintain, or transmit ePHI on River City TMS, PLLC's behalf only after obtaining satisfactory assurance through a written contract that the business associate will comply with the applicable requirement of the Security Rule and will appropriately safeguard the information. Contracts shall be evaluated by the Bryan Gosling, lawyer to ensure compliance and shall be signed by the CEO, Business Owner or an individual with legal authority.
- Subcontractors [§164.308\(b\)\(2\)](#), [§164.314\(a\)](#) – The business associate of River City TMS, PLLC shall obtain satisfactory assurance through a written contract from its subcontractors that create, receive, maintain, or transmit ePHI on the business associate's behalf, that the subcontractor will comply with the applicable requirement of the Security Rule and will appropriately safeguard the information.

- Annual Review – Business Associate Agreements and other arrangements shall be reviewed annually during the Security Risk Analysis process to ensure all Business Associate Agreements are accounted for. This annual review will include, but will not be limited to:
 - Identification of all business associates with any outsourced functions involved with ePHI ([Appendix P – BA Listing](#)).
 - Verification that legal documents are active and signed by the River City TMS, PLLC's legal authority.
 - Evaluation of contract termination thresholds for any agreement that does not comply with the contract and does not adhere to the regulations.
- Security Incident Reporting [§164.314\(a\)\(2\)\(i\)\(C\)](#) – Business associates shall report to River City TMS, PLLC any security incidents of which it becomes aware, including breaches of unsecured PHI.

- **Security in Third Party Contracts**

Access to River City TMS, PLLC computer systems or corporate networks shall not be granted until a review of the following concerns have been made and appropriate restrictions or covenants are included in a statement of work ("SOW") with the party requesting access:

- Applicable sections of River City TMS, PLLC Information Security Policy have been reviewed and considered.
- Policies and standards established in River City TMS, PLLC information security program have been enforced.
- There has been a risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities will be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents will be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- There will be a description of each service to be made available.
- Each service, access, account, and/or permission made available will only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to River City TMS, PLLC computer systems will be maintained and auditable.
- If required under the contract, permission will be sought to screen authorized users.
- Dates and times when the service is to be available will be agreed upon in advance.
- Procedures regarding protection of information resources will be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.

- The right to monitor and revoke user activity will be included in each agreement.
- Language on restrictions on copying and disclosing information will be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance will be understood and agreed upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract will be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these will be included in the agreement.
- A formal method to grant and authorize users who will have access to the data collected under the agreement will be formally established before any users are granted access.
- Mechanisms will be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulations, a formal procedure will be established to ensure that the training takes place and that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement will be published in advance of the agreement.