



10-Contingency Plan

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Contingency Plan

Policy Statement

It is the policy of River City TMS, PLLC to maintain formal practices for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems containing ePHI.

Procedure

- **Data Backup Plan** [§164.308\(a\)\(7\)\(ii\)\(A\)](#)

River City TMS, PLLC, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.

- Designated personnel shall backup all servers containing ePHI either to a cloud solution, another secure location, or both at the end of the week. 7 days of the backup data will be maintained at all times in a remote location.
- Backup media shall be physically secured, stored offsite and encrypted.
- Multiple backups shall be maintained as a failsafe.
- Backup media that is no longer in service will be disposed of in accordance with the Disposal of External Media/Hardware policy.
- The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.
- Files identified as critical shall be documented and listed in the backup configuration.
- For hosted EHR solutions the Security Officer will ensure the vendor agreement outlines appropriate backups and recovery are being performed.

- **Disaster Recovery Plan** [§164.308\(a\)\(7\)\(ii\)\(B\)](#)

The Security Officer shall be responsible for developing and regularly updating the written disaster recovery plan for the purpose of restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner.

- The Security Officer shall monitor all recovery operations.
- All staff will be trained and will understand their Disaster Recovery Plan duties.
- A copy of the recovery plan shall be safely stored offsite at With business owner.
- System restore procedures shall be known to at least one trusted party outside River City TMS, PLLC, who is:

Neurostar/ Trakstar/ Care Cloud Omni Billing

lisa@omnimbs.com

206-201-3314

- Designated personnel shall restore data on all servers with the most recent backup data as per the Data Backup Plan.
- Current copies of the information systems inventory and network configuration shall be maintained.
- Current inventory of hard copy forms that are necessary for River City TMS, PLLC function shall be maintained, such as clinical, registration and financial interactions with patients. Current inventory of hard copy forms will be located at Seattle, Washington Office.
- Data that was collected while the EHR is inaccessible shall be entered once the system is restored.
- The RMT is identified in [Policy 1: Introduction to the Information Security Policy](#) and shall be responsible for:
 - Determining the impact of a disaster and/or system unavailability on River City TMS, PLLC operations.
 - In the event of a disaster, securing the site and providing ongoing physical security.
 - Retrieving lost data.
 - Taking steps necessary to restore operations.

• **Emergency Mode Operations Plan** [§164.308\(a\)\(7\)\(ii\)\(C\)](#)

The Security Officer and RMT shall be responsible for developing and regularly updating the emergency mode operations plan for the purpose of enabling the continuation of critical business processes while information systems are unavailable.

The Security Officer/RMT shall:

- Identify and implement appropriate “work-arounds” during such time information systems are unavailable.

- Identify workforce members who will need access to the facility in the event of an emergency ([Appendix J – Emergency Plan](#)).
- Determine alternative source of power in the event of a power outage.
- Determine alternative site.
- Compile and distribute to appropriate employees emergency contact information for all persons to be contacted in the event of a disaster, including the following:
 - Members of the Risk Management Team (RMT),
 - Facilities at which backup data is stored,
 - Information systems vendors, and
 - All current workforce members.

- **Testing and Revision Procedure** [§164.308\(a\)\(7\)\(ii\)\(D\)](#)

- The Security Officer shall periodically test backup procedures as reasonable and appropriate to ensure the disaster recovery plan is effective. Such testing shall be documented by the Security Officer ([Appendix K – Backup Test Log](#)).
- The RMT shall meet at least every six months or sooner if needed to:
 - Review the effectiveness of the plan in responding to any disaster or emergency experienced by River City TMS, PLLC;
 - In the absence of any such disaster or emergency, drills shall be planned to test the effectiveness of the plan and evaluate the results of such drills; and
 - Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining the minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the RMT.

- **Application and Data Criticality Analysis** [§164.308\(a\)\(7\)\(ii\)\(A\)](#)

The RMT will identify the order in which data is to be restored based on the criticality analysis performed as part of River City TMS, PLLC risk analysis. Data critical for patient care will be restored first and remaining data triaged in order of operational needs. The RMT will identify hardware, software and personnel that are critical to daily operations.

- **Workforce Member Roles**

The RMT shall oversee and coordinate procedures in the event of an emergency or another occurrence. Roles and responsibilities shall include, but shall not be limited to:

- Privacy Officer
 - Shall notify all management and staff when contingency operations are in use during an event
- Security Officer

- Shall identify and train designated workforce members responsible for procedures in contingency processes
- Shall coordinate management in contingency processes
- Shall coordinate Business Associates in contingency processes
- Shall determine appropriate steps in contingency processes
- Shall determine frequency of review and updating of contingency procedures
- Shall determine frequency of testing of the contingency plan
- The Clinical Officer will ensure all paper charting forms are available and appropriate staff are trained in manual documentation during contingency operations.