



12-Breach Notification

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Breach Notification

Policy Statement

It is the policy of River City TMS, PLLC to notify affected individuals of a breach of protected information under the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, which requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

An impermissible acquisition, access, use or disclosure of unsecured protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Procedure

- **Training** [§164.530\(b\)](#)

All workforce members shall receive training pertaining to the Breach Notification Rule. A record of the training materials and workforce members' attendance at trainings shall be maintained ([Appendix G](#) – Workforce Training Log).

- **Complaints** [§164.530\(d\)](#)

Any complaints about River City TMS, PLLC's compliance with the Breach Notification Rule shall be submitted to the Privacy Officer or RMT. The Privacy Officer and RMT shall investigate the complaint and take appropriate remedial action.

- **Sanctions** [§164.530\(e\)](#)

Workforce members who fail to comply with River City TMS, PLLC's policies and procedures as they relate to the Breach Notification Rule are subject to discipline up to and including termination in accordance with River City TMS, PLLC Sanctions, [Policy 4](#).

- **Refraining from Retaliatory Acts** [§164.530\(g\)](#)

River City TMS, PLLC will not enforce any retaliatory acts against a workforce member for exercising a right or participating in a process or for opposing an act or practice that the workforce member believes in good faith violates the Breach Notification Rule.

- **Waiver of Rights** [§164.530\(h\)](#)

River City TMS, PLLC shall not require an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

- **Documentation** [§164.530\(i\)](#)

River City TMS, PLLC will maintain its policies and procedures, in written or electronic form, until 6 years after the later of the date of their creation or the last effective date.

- **Reporting and Tracking a Possible Breach**

Any workforce member who becomes aware of a possible breach of privacy involving Private Information in the custody or control of River City TMS, PLLC will immediately inform the office manager/workforce member's supervisor and the Privacy Officer.

- Notification will occur immediately upon discovery of a possible breach or before the end of the employee's shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
- The office manager/workforce member's supervisor will verify the circumstances of the possible breach and inform the Privacy Officer and the Risk Management Team (RMT) within twenty-four (24) hours of the initial report.
- In notifying the Privacy Officer the employee will:
 - Provide the Privacy Officer with as much detail as possible.
 - Be responsive to requests for additional information from the Privacy Officer.
 - Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.

The Privacy Officer will:

- Log and conduct a rigorous analysis of each incident of a possible breach ([Appendix L – Breach Assessment](#)).

- In conjunction with River City TMS, PLLC Risk Management Team (RMT) and the owner/CEO, will decide whether or not to contact Legal Counsel by taking into consideration the seriousness and scope of the breach.
- Determine, along with the RMT and Legal Counsel when Breach Notification is triggered. Legal Counsel for River City TMS, PLLC is:

Brian Gosline

Brian Gosline

601 W Main Avenue

509-747-2002

- **Containing the Breach**

The Privacy Officer will work with the appropriate workforce member to immediately contain the breach so as to limit its scope and effect. Examples include, but are not limited to:

- Stopping the unauthorized practice
- Recovering the records, if possible
- Shutting down the system that was breached
- Mitigating the breach, if possible
- Correcting weaknesses in security practices
- Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

- **Investigating and Evaluating the Risks Associated with the Breach**

To determine what other steps are immediately necessary, the Privacy Officer in collaboration with River City TMS, PLLC RMT and affected department(s) and administration, will investigate the circumstances of the breach.

A team will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan. The Privacy Breach Assessment tool will help aid the investigation.

The Privacy Officer, in collaboration with River City TMS, PLLC RMT, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:

- Contractual obligations
- Legal obligations – River City TMS, PLLC Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the RMT
- Risk of identity theft or fraud because of the type of information lost, such as social security number, banking information, identification numbers
- Risk of physical harm if the loss puts an individual at risk of stalking or harassment

- Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
- Number of individuals affected

- **Prevention**

Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.

- If necessary, this will include a security audit of physical, organizational, and technological measures.
- This may also include a review of any mitigating steps taken.

The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches. Procedures will be reviewed, updated, and implemented to reflect the lessons learned from the investigation. The resulting plan will also include audit recommendations, if appropriate.

- **Notice to Individuals** [§164.404\(a\)\(1\)](#)

The required elements of notification vary depending on the type of breach and which law is implicated. As a result, River City TMS, PLLC Privacy Officer, RMT, and Legal Counsel will work closely to draft any notification that is distributed. Indirect notification, such as website information, posted notices and media, will generally occur only where direct notification could cause further harm or contact information is lacking.

If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.

- **Timeliness of Notification** [§164.404\(b\)](#) – Affected individuals will be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
- **Content of Notification** [§164.404\(c\)\(1\)](#) – Notices will be in plain language and will include the following:
 - Brief description of the breach, including date of the breach and date of the discovery of the breach, if known
 - Types of unsecured PHI involved
 - Steps affected individuals should take to protect themselves from potential harm
 - Steps the covered entity is taking to investigate the breach, mitigate the harm, and prevent further breaches
 - Contact information for the covered entity (or business associate)
- **Methods of Notification** [§164.404\(d\)](#) – Notices will be sent by first-class mail or, if the individual agrees, electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice will occur as specified below:

- For fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.
- For 10 or more individuals, the covered entity will provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals are likely to reside. The covered entity will include a toll-free phone number that remains active for at least 90 days where the individuals can learn if their information was involved in the breach.

- **Notification to Media [§164.406\(a\)](#)**

If a breach involves more than five-hundred (500) individuals of a State or jurisdiction, River City TMS, PLLC will notify a prominent media outlet serving the State or jurisdiction. Notice will be provided in the form of a press release. Media outlets in the State or jurisdiction are listed in [Appendix N](#). Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notification to Secretary [§164.408](#)**

Following the discovery of a breach of unsecured protected health information River City TMS, PLLC shall notify the Secretary of Health & Human Services via the HHS website as follows:

- For breaches of unsecured protected health information involving 500 or more individuals, notification to the Secretary shall be provided without unreasonable delay and in no case later than 60 days following a breach.
- For breaches of unsecured protected health information involving less than 500 individuals, documentation of the breach shall be maintained and the Secretary will be notified on an annual basis, no later than 60 days after the end of the calendar year.

HHS website: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>

Questions:

HHS OCR toll-free 1-800-368-1019

OCRPrivacy@hhs.gov

- **Notification by a Business Associate [§164.410](#)**

If a breach of unsecured protected health information occurs at or by a business associate, the business associate will:

- Notify the covered entity following the discovery of the breach without unreasonable delay and no later than 60 days from the discovery of the breach.
- To the extent possible, provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to

be provided by the covered entity in its notification to affected individuals.

- Cooperate with the River City TMS, PLLC in investigating and mitigating the breach.

The Privacy Officer will periodically review these requirements with the business associates to ensure that both parties will meet their notification obligations.

- **Law Enforcement Delay** [§164.412](#)

If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.

- **Burden of Proof** [§164.414\(b\)](#)

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. With respect to an impermissible use or disclosure, a covered entity, or business associate, will maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of “breach”.