



00-Information Security Policy

Approved by: William Voss

Review: Annual

Renewed By:

Effective: April 1, 2024

Revised:

Renewed:

Warranty & Limitations of Liability

This Information Security Policy is developed specifically for River City TMS, PLLC, is current as of (PLEASE APPROVE A POLICY BEFORE EDITING THIS POLICY TO GENERATE A DATE), and is valid for a period of 12 months from this date. It is the recommendation of Medcurity that these policies and procedures be re-evaluated at a minimum of annually in order to ensure HIPAA compliance. HIPAA regulations change frequently and, therefore, this policy is current in accordance with the HIPAA and HITECH Act as of this date but will require modification to reflect any future changes in law, internal processes, etc. It is the responsibility of River City TMS, PLLC to maintain this Information Security Policy in a state current to both federal and state laws. If River City TMS, PLLC undergoes any changes in personnel, systems, or processes it is highly recommended that a re-evaluation of the content of this document be requested as soon as possible to address policy modification needs for continued compliance. Examples of situations that may require a re-assessment and subsequent policy modifications include, but are not limited to, the following:

- Change in the role of the Privacy and/or Security Officer
- Change in the hosting environment of the electronic health record
- Introduction of new software, systems, or mobile devices
- Change in practice location or expansion
- Change in IT software/vendor
- Change in back-up/recovery processes
- Change in the Emergency Plan
- Findings during the Security Risk Analysis process

Table of Contents

<p>Introduction to the Information Security Policy</p> <ul style="list-style-type: none"> • Scope • Privacy & Security Officers §164.530(a), §164.308(a)(2) • Risk Management Team 	<p>Policy 1</p>
<p>Security Management Process §164.308(a)</p> <ul style="list-style-type: none"> • Policy Statement • Risk Management §164.308(a)(1)(ii)(B) • Risk Analysis §164.308(a)(1)(ii)(A) • Security Incident Procedures §164.308(a)(6)(i), §164.308(a)(6)(ii) • Information System Activity Review §164.308(a)(1)(ii)(D) • Evaluation of Security Controls & Processes §164.308(a)(8) • Policy & Procedure Requirements §164.316(b)(1) 	<p>Policy 2</p>
<p>Workforce Security §164.308(a)(3)(i)</p> <ul style="list-style-type: none"> • Policy Statement • Authorization & Supervision §164.308(a)(3)(ii)(A) • Workforce Clearance §164.308(a)(3)(ii)(B) • Termination Procedures §164.308(a)(3)(ii)(C) • Confidentiality Agreement §164.308(a)(3)(ii)(B) 	<p>Policy 3</p>
<p>Sanctions §164.308(a)(1)(ii)(C)</p> <ul style="list-style-type: none"> • Policy Statement • Violations §164.308(a)(1)(ii)(C) • Recommended Disciplinary Actions §164.308(a)(1)(ii)(C) 	<p>Policy 4</p>
<p>Security Awareness & Training §164.308(a)(5)(i)</p> <ul style="list-style-type: none"> • Policy Statement • Security Training Program §164.308(a)(5)(i) • Security Reminders §164.308(a)(5)(ii)(A) • Protection from Malicious Software §164.308(a)(5)(ii)(B) • Log-in Monitoring §164.308(a)(5)(ii)(C) • Password Management §164.308(a)(5)(ii)(D) • Breach Notification Rule §164.530(b) 	<p>Policy 5</p>
<p>Facility Access Controls §164.310(a)(1)</p> <ul style="list-style-type: none"> • Policy Statement • Contingency Operations §164.310(a)(2)(i) • Facility Security Plan §164.310(a)(2)(ii) • Access Control & Validation Procedure §164.310(a)(2)(iii) • Maintenance Records §164.310(a)(2)(iv) 	<p>Policy 6</p>

<p>Workstation & Device Security §164.310(b), §164.310(c), §164.310(d)(1)</p> <ul style="list-style-type: none"> • Policy Statement • Workstation Use §164.310(b) • Workstation Security §164.310(c) • Device & Media Controls §164.310(d)(1) • Disposal of External Media §164.310(d)(2)(i) • Media Reuse §164.310(d)(2)(ii) • Accountability §164.310(d)(2)(iii) • Data Backup & Storage §164.310(d)(2)(iv) 	<p>Policy 7</p>
<p>Access Management & Controls §164.308(a)(4)(i)</p> <ul style="list-style-type: none"> • Policy Statement • Access Authorization §164.308(a)(4)(ii)(B) • Access Establishment & Modification §164.308(a)(4)(ii)(C) • Access Control §164.312(a)(1) • Unique User Identification §164.312(a)(2)(i) • Emergency Access §164.312(a)(2)(ii) • Automatic Logoff §164.312(a)(2)(iii) • Encryption & Decryption §164.312(a)(2)(iv) • Audit Controls §164.312(b) • Person or Entity Authentication §164.312(d) 	<p>Policy 8</p>
<p>Data & Transmission Integrity §164.312(c)(1), §164.312(e)(1)</p> <ul style="list-style-type: none"> • Policy Statement • Mechanism to Authenticate ePHI §164.312(c)(2) • Transmission Security §164.312(e)(1) • Transmission Integrity Controls §164.312(e)(2)(i) • Encryption §164.312(e)(2)(ii) 	<p>Policy 9</p>
<p>Contingency Plan §164.308(a)(7)(i)</p> <ul style="list-style-type: none"> • Policy Statement • Data Backup Plan §164.308(a)(7)(ii)(A) • Disaster Recovery Plan §164.308(a)(7)(ii)(B) • Emergency Mode Operations Plan §164.308(a)(7)(ii)(C) • Testing & Revision Procedure §164.308(a)(7)(ii)(D) • Application & Data Criticality Analysis §164.308(a)(7)(ii)(A) 	<p>Policy 10</p>
<p>Business Associate Contracts §164.308(b)(1), §164.314(a)(1)</p> <ul style="list-style-type: none"> • Policy Statement • Business Associate Contracts & Other Arrangements • Security in Third Party Contracts 	<p>Policy 11</p>

<p>Breach Notification</p> <ul style="list-style-type: none"> • Policy Statement • Training §164.530(b) • Complaints §164.530(d) • Sanctions §164.530(e) • Refraining from Retaliatory Acts §164.530(g) • Waiver of Rights §164.530(h) • Notice to Individuals §164.404(a) • Notification to Media §164.406 • Notification to Secretary §164.408 • Notification to Business Associates §164.410 • Law Enforcement Delay §164.412 • Burden of Proof §164.414(b) 	<p>Policy 12</p>
Appendix A – RMT Meeting Attendance Log	
Appendix B – Audit Log	
Appendix C – Confidentiality Form	
Appendix D – Network Access Request Form	
Appendix E – Background Check Authorization	
Appendix F – Employee Hiring & Termination Checklist	
Appendix G – Workforce Training Log	
Appendix H – Security Incident Report	
Appendix I – Media Disposition Log	
Appendix J – Emergency Plan	
Appendix K – Backup Test Log	
Appendix L – Breach Assessment	
Appendix M – Security Log	
Appendix N – Media Outlets	
Appendix O – IS Inventory	
Appendix P – Business Associates Listing	
Appendix Q – Business Associate Contract	
Appendix R – Visitor Log	
Appendix S – Maintenance Log	

Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

Availability – Refers to data or information that is accessible and useable upon demand by an authorized person.

Breach – Unauthorized or reasonable belief of unauthorized acquisition, access, use or disclosure of Personal Information, Personally Identifiable Information, and /or Protected Health Information that compromises its security, confidentiality or integrity.

Business Associate – With respect to a covered entity, a person who performs or assists in the performance of a function or activity involving the use or disclosure of Individually Identifiable Health Information.

Confidentiality – Refers to data or information that is not made available or disclosed to unauthorized persons or processes.

Covered Entity – A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic format.

DoD – Department of Defense

Electronic Health Record (EHR) – An EHR is a record of patient encounters in a healthcare delivery setting. An electronic health record typically consists of information including patient demographics, progress notes, medication history, vital signs and laboratory results.

Electronic Protected Health Information (ePHI) – PHI in electronic format.

Encryption – Process of transforming information using an algorithm to make it unreadable to anyone other than those who have a specific ‘need to know’.

External Media – CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

FAT – File Allocation Table; the FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Financial/accounting records – Any records related to the accounting practices or financial statements of the Practice.

Firewall – Dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP – File Transfer Protocol

HIPAA – Health Insurance Portability and Accountability Act

Individually Identifiable Health Information (IIHI) – Personally Identifiable Information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and relates to the past, present or future physical or mental health or treatment, payment or provision of health care to the identified individual.

Integrity – Refers to data or information that has not been altered or destroyed in an unauthorized manner.

IT – Information Technology

LAN – Local Area Network; a computer network that covers a small geographic area, i.e. a group of buildings, an office.

NTFS – New Technology File Systems; NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus

additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Practice.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following, which could be used to identify an individual and poses a risk of identity theft: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or any other information.

Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Practice.

PO – Privacy Officer; responsible for HIPAA privacy compliance issues and annual security training for all staff on confidentiality issues.

Practice Management System (PM) – A PM is usually a computer based system used to manage the day-to-day operations of a healthcare practice. Tasks typically performed by a PM system include scheduling appointments, maintaining patient and insurance information, billing functions and generating various reports.

President – Responsible for the overall privacy and security practices of the organization.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Individually Identifiable Health Information and Protected Health Information collectively.

Privileged Users – system administrators and others specifically identified and authorized by Organization management.

Protected Health Information (PHI) – Individually Identifiable Health Information that is electronically transmitted, maintained electronically, or transmitted or maintained in any other form. Protected Health Information excludes Individually Identifiable Health Information in education and employment records.

RMT – Risk Management Team

Sensitive Information – Includes, but is not limited to, the following:

SO – Security Officer; responsible for security policies and procedures and is involved in IT security purchasing and investment.

SOW – Statement of Work; agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

Unsecured Protected Health Information – Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology.

User – Any person authorized to access an information resource.

Users with edit/update capabilities – individuals who are permitted, based on job assignment, to add, delete, or change records in a database.

Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

Virus – Software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

VLAN – Virtual Local Area Network; logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

VPN – Virtual Private Network; provides a secure passage through the public Internet.

WAN – Wide Area Network; computer network that enables communication across a broad area, i.e. regional, national.

Workforce Member – Includes employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers and staff from third party entities who provide service to the covered entity.