RIVERSIDE CORPORATE WELLNESS, LLC

HIPAA Security Policy

Effective Date: January 24, 2013

Reviewed on: September 1, 2019

PURPOSE: The security rule defines the standards which require covered entities to implement basic safeguards to protect the confidentiality, integrity, and availability of protected health information (PHI). This policy has been developed in conjunction with Riverside Corporate Wellness, LLC's Privacy Policy, which addresses the HIPAA privacy rule.

The purpose of this document is to create standards to ensure the privacy and security of health information that is transmitted or stored electronically within Riverside Corporate Wellness.

This policy covers all PHI, whether in electronic form or hardcopy, and any system which accesses, processes or saves corporate or patient data. It applies to:

1. All PHI, in any form, and in any medium;
2. All network systems, internet and personal computer environments;
3. All creation, communication, distribution, storage and disposal of PHI;
4. All managers, employees, volunteers, vendors, members, consultants, contractors, healthcare providers, or others who use or have access to Riverside Information Systems.

SCOPE:

1. You must not use or disclose PHI except as this Policy permits or requires.
2. This Policy applies to our entire workforce, including employees, volunteers, students, instructors, alternative therapy staff, and independent contractors of Riverside Corporate Wellness, LLC; Riverside Corporate Wellness Primary Health; Riverside Corporate Wellness Fitness Facility, and Riverside Corporate Wellness Alternative Therapy, collectively "Riverside Corporate Wellness" or "RCW".
3. Each member of our workforce with access to PHI must, at all times, comply with this Policy.

DEFINITIONS:

PHI: PHI includes any computer data relating to the past, present, or future mental or physical health, health care treatment, or payment of health care. PHI includes information that can identify an individual, such as name, social security number, address, date of birth, medical history, medical history number, and includes information transmitted or maintained in electronic format.

Confidentiality/Privacy: Information shall not be made available or disclosed to unauthorized individuals, entities, given the potential adverse impact on RCW, its members, or its mission and values. All events and information relating to services provided to members are considered confidential and private.

RESPONSIBILITY OF RIVERSIDE CORPORATE WELLNESS:

The HIPAA security rule requires RCW to put into place the appropriate administrative, physical and technical safeguards to protect the integrity, confidentiality and availability of PHI that is created, received or managed by RCW's covered components. RCW has reviewed the HIPAA security rule and evaluated which safeguards must be in place given the type and nature of PHI held and accessed by RCW.

1. Every component of RCW with access to PHI is required to adhere to all HIPAA mandates. Violation of this Policy may result in disciplinary action up to and including termination of employment, vendor or independent contract and/or legal action. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties and criminal sanctions including fines and imprisonment.
2. RCW will implement and maintain a security awareness and training program for all members of the workforce, including management.

RCW will document the satisfactory assurances of a written contract with business associates that receive, maintain or transmit PHI on RCW's behalf to ensure that the business associate will appropriately safeguard the information and will adhere to all RCW privacy and security guidelines. **Workforce Security and Information Access:**

RCW will establish procedures to ensure only authorized personnel have access to systems that manage PHI, and will include:

1. Establishing a procedure that requires managerial approval before any person is granted access to systems managing PHI;
2. Performing appropriate background checks, where appropriate, before any person is granted access to systems managing PHI;
3. Limiting authorized persons' access to PHI to the extent that access to this information achieves the requirements of the person's job responsibilities;
4. Implementing procedures for terminating access to PHI when the employment of a person ends, or the job responsibilities no longer warrants access to PHI;
5. Periodically reviewing the accounts on systems managing PHI to ensure that only currently authorized personnel access;
6. All RCW covered components will adhere to RCW's procedures for passwords on systems managing PHI, and passwords must be forced to change periodically;
7. All RCW covered components will notify privacy and security officer when a system managing PHI is involved is a security incident, including virus or worm infections, accounts being compromised, and server damaged from a denial of service attack;

RCW must have a procedure in place to respond to an emergency that may damage systems managing PHI, and have a procedure for restoring any loss of data.

Administrative Safeguards:

1. RCW will perform a yearly risk analysis which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI managed by RCW.
2. RCW will implement measures to reduce computer risks and vulnerabilities, including identifying and documenting potential risks and vulnerabilities that could impact systems managing PHI; performing annual technical security assessments of systems managing PHI in order to identify and remedy detected security vulnerabilities.
3. Our Security Official is also assigned security responsibility for developing, maintaining, and implementing this Policy, and for overseeing our full compliance with this Policy and applicable federal and state privacy law.
4. Security Official: Teresa Pulvermacher; Telephone: 608-782-5029 Ext. 3439; Fax: 608782-5032; E–mail: tpulvermacher@rcwlacrosse.com
5. RCW will periodically review information systems activity records, including audit logs, access reports, and security incident tracking reports to ensure that implemented security controls are effective.
6. Each member of our workforce is obligated to report promptly any suspected violation of this Policy or applicable federal or state privacy law to our Security Official or our legal advisers. Reports may be made anonymously.
7. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Security Official or our legal advisers.

Physical Safeguards:

1. RCW will ensure that systems that manage PHI are kept in areas with physical security controls that restrict access.
2. RCW will follow all implemented facility policies and procedures to document repairs and modifications to the physical components of the RCW facility that are related to security, including hardware, walls, doors and locks.
3. RCW will establish procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of the RCW facility, and the movement of these items within the facility.

Technical Safeguards:

1. RCW will periodically review information systems activity records, including audit logs, access reports, and security incident tracking reports to ensure that implemented security controls are effective.
2. Each member of our workforce is obligated to report promptly any suspected violation of this Policy or applicable federal or state privacy law to our Security Official or our legal advisers. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Security Official or our legal advisers.
3. RCW will ensure that only designated workstations possessing appropriate security controls will be used to access and manage PHI, and that these workstations are not used in publicly accessible areas or used by multiple users not authorized to access PHI. This security measure extends to the use of laptops and home machines.

4. RCW will have audit controls that will allow an independent reviewer to review system activity.
5. RCW will have controls in place to verify that a person seeking access to PHI is the one claimed.
6. RCW will have the ability to encrypt emails that contains PHI, but the use of email in the transmission of PHI is discouraged.
7. System and network administrators will administer systems and networks in a manner that protects the confidentiality, integrity, and availability of the PHI that is stored in them or transmitted through them.