RIVERSIDE CORPORATE WELLNESS, LLC

Privacy Policies & Procedures

Effective Date: December 12, 2012

Reviewed on: September 1, 2019

These HIPAA Privacy Policies and Procedures ("Policy") implement our obligations to protect the privacy of individually identifiable health information that we create, receive or maintain as a business associate on behalf of covered entities. We implement this Policy as a matter of sound business practice, to protect the interests of individuals, and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996, as amended, ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("Privacy Rules") and the Health Information Technology for Economic and Clinical Health Act ("HITECH").

You are obligated to comply with this Policy. Failure to do so can result in disciplinary action, including termination of your employment.

If you have questions about any use or disclosure of individually identifiable health information or about your other obligations under this Policy, the Privacy Rules, HITECH or other federal or state law, consult our Privacy Official—Teresa Pulvermacher—at 608-782-5029 Ext. 3439 before you act.

1. GOALS OF THIS POLICY

a. To protect the privacy, confidentiality and security of Protected Health Information ("PHI") that we create, receive or maintain on behalf of covered entities.

b. To describe our objectives and policies regarding maintaining the privacy of PHI.

c. To comply with HIPAA and HITECH.

2. SCOPE

a. You must not use or disclose PHI except as this Policy permits or requires.

b. This Policy applies to all of our employees, management, contractors, student interns, and volunteers.

c. Each member of our workforce with access to PHI must, at all times, comply with this Policy.

d. Our Privacy Official is responsible for developing, maintaining, and implementing this Policy, and for overseeing our full compliance with this Policy and applicable federal and state privacy law.

Privacy Official: Teresa Pulvermacher
Telephone: 608-782-5029 Ext. 3439
Fax:
E–mail: tpulvermacher@rcwlacrosse.com

3. PROTECTED HEALTH INFORMATION

Protected Health Information, or PHI, includes, but is not limited to, a patient's name, address, birth date, admission/discharge date, date of death, phone/fax number, email address, social security number, account numbers, license numbers, medical record identification number, and other unique identifiers. PHI may be written or oral, paper or electronic.

4. RESPONSIBILITIES

a. Executives/Management

i. Establish program objectives

ii. Approve this Policy

iii. Provide training for work force

iv. Enforce sanctions

v. Designate Privacy Official

b. Privacy Official

i. Develops privacy policies and procedures

ii. Coordinates and implements this Policy throughout the organization

iii. Oversees training

iv. Receives and processes privacy complaints

v. Processes patients' rights requests

vi. Ensures retention of HIPAA policies and procedures, complaints, and investigative materials to meet compliance requirements.

vii. Develops and implements privacy training program

viii. Documents the delivery of privacy training to all work force members

ix. In conjunction with legal counsel, process Business Associate Agreements

c. Employee responsibilities

i. Understand and comply with this Policy

5. DESIGNATED RECORD SET

a. Medical records

b. Admission forms

c. Electronic storage

6. NOTICE OF PRIVACY PRACTICES

a. **FORM**: Notice of Privacy Practices

b. As a business associate we will maintain a Privacy Practices Notice ("Notice"). That Notice must give individuals written notice of the uses and disclosures of PHI that we may make, our legal duties with respect to PHI, and individuals' privacy rights and how to exercise them. We must use and disclose PHI consistently with our Notice.

c. We will regularly review and promptly revise our Notice.

d. Our Privacy Official will ensure proper distribution of our Notice by:

i. Disseminating the Notice to each individual who receives health services at our facility.

ii. Notifying our then current individuals who receive services at our facility, at least once every 3 years, that our Notice is available on request, explaining how it may obtain.

iii. Ensuring that our Notice is prominently posted and electronically available on each web site we maintain.

iv. Disseminating our revised Notice, resulting from any material change we adopt in our privacy practices within 60 days of the material change.

v. Furnishing our Notice to any person on request.

vi. Emailing our Notice to any individual who has agreed to electronic notification and not withdrawn that agreement and provide a paper copy if you know the individual did not receive the transmission or if the individual requests a paper copy.

e. We will make our "best effort" to receive acknowledgment of receipt of the Notice from each recipient and document such receipt.

7. MINIMUM NECESSARY POLICY

a. We must make reasonable efforts to use, to disclose, and to request only the minimum necessary PHI to accomplish the intended purpose. This generally will consist of the PHI contained in a limited data set, although it can be more if needed to accomplish the intended purpose of such use, disclosure or request.

b. There is no minimum necessary limitation for:

i. Disclosure to or a request by a health care provider for treatment.

ii. Use with and disclosure to an individual.

iii. Use/disclosure pursuant to an authorization by an individual.

iv. Disclosure to HHS for complaint investigation or compliance enforcement or review.

v. Use/disclosure required by law.

vi. Use/disclosure required for compliance with HIPAA Administrative Simplification Rules.

c. Our Privacy Official will identify and document:

i. Those workforce members (or classes of workforce members) who need access to PHI to perform their duties;

ii. The categories of PHI needed by each of those workforce members (or those classes of workforce members) to perform those duties; and

iii. Any conditions appropriate to each workforce member's access to those categories of PHI.

d. Our Privacy Official will identify and document:

i. Our routine or recurring disclosures and requests for PHI;

ii. The categories of PHI needed to accomplish the purpose of each of these routine or recurring disclosures and requests; and

iii. Any conditions appropriate to each routine or recurring disclosure and request for those categories of PHI.

8. USE AND/OR DISCLOSURE OF PHI

Authorization is not needed from an individual for the following uses and/or disclosures:

a. Routine uses

   i. Treatment- we may disclose PHI, without the individual's permission, for any health care provider's treatment activities.

   ii. Payment- we may disclose the minimum necessary PHI, without the individual's permission, for the payment activities of a covered entity for whom we are a business associate.

   iii. Operations- we may use and disclose PHI, without the individual's permission, for our own payment activities and our own operations.

b. Disclosures to the individual

c. Disclosures to HHS

d. Informal Permission

   i. Disclosures to family members and close personal friends if:

      1. Individual identifies which family members or close friends may receive the communication;

      2. The family member or close friend is involved with the individual's health care or payment;

      3. Only the minimum necessary is disclosed; and

      4. Disclosure is limited to notifications of location, general condition or death.

   ii. Emergency Situations

      1. Individual provides informal permission or if unable to provide permission;

      2. The disclosure is in the individual's best interests; and

      3. Only the minimum necessary is disclosed.

e. Personal representatives

   i. We may disclose PHI to the individual's personal representative, as relevant to the scope of the representation.

   ii. We must consider a personal representative to be the individual for all purposes, unless we conclude that the *personal representative* may be abusive.

f. Minors. Unless State or other law (including case law) permits or requires parental control of an unemancipated minor's *PHI*, the unemancipated minor has, to the extent consistent with applicable State or other law (including case law), the authority to control and have access to his or her own *PHI*.

g. In the public interest (for example, workers' compensation, as required by law, health oversight activities, law enforcement, judicial and administrative proceedings)

h. Disclosures to our business associates

i. Incidental to otherwise permitted or required uses and disclosures

j. Disclosures of de-identified information

All other uses and/or disclosures require the individual's authorization

a. **FORM**: Authorization

b. **FORM**: Authorization Revocation

c. Verify identity of the individual

d. If a personal representative is involved, verify the identity and source of authority

e. We may not rely on an authorization we know has been revoked or has expired. An individual may revoke authorization at any time. Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation.

9. INDIVIDUAL RIGHTS

a. Right to access/copy PHI

i. In accordance with the terms of the applicable business associate agreement, we will allow an individual to inspect and to obtain a copy of his or her PHI for as long as we maintain that PHI in designated record sets or we will provide a copy of the designated record set to the covered entity for transmission to the individual.

ii. We must respond to the individual's request for access within 30 days of its receipt or sooner as may be required by the applicable business associate agreement.

iii. We may charge a reasonable, cost–based fee for providing access, including copying and mailing of the requested PHI, and for preparing a summary or explanation of the requested PHI. We may not charge for retrieving the requested PHI. Our Privacy Official will determine any charges and inform covered entity or individual in advance so that the covered entity or individual may elect to withdraw or modify the request to reduce or avoid the fee.

iv. Under certain circumstances a covered entity may deny an individual access to certain records. In these circumstances it may be appropriate to deny access without right of review:

1. Research

2. Psychotherapy notes

3. Obtained from sources other than the provider or patient

4. Compiled for use in civil, criminal or administrative action or proceeding

5. Endanger the safety of the individual or another

6. Discuss with counsel prior to denying access right

b. Right to amend PHI

i. In accordance with procedures set forth in the applicable business associate agreement, we will allow an individual to request to amend his or her PHI for as long as we maintain the PHI in designated record sets.

ii. We may decline to amend PHI if:

1. We did not create the information;

2. The information is not part of a designated record set maintained by us; or

3. Information may be withheld from the right of access (see above).

c. Right to restrict use or disclosure

i. We will allow an individual to request that we restrict our use or disclosure of his or her PHI for treatment, payment, health care operations, or with specified family members or others. Except as noted below, we have no obligation to agree to such request.

ii. If the disclosure is to a health plan for purposes of carrying out payment or health care operations (and not for purposes of carrying out treatment) and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full, then we are obligated to agree to the request.

d. Right to confidential communications. We will allow an individual to request confidential communications (that is, the use of alternative means or alternative locations when we communicate PHI to the patient), if the request is reasonable and in writing, and the patient gives us a clear statement that all or part of the PHI could endanger the patient if not communicated by the requested alternative means or to the requested alternative location.

e. Right to an accounting of disclosures

i. In accordance with the procedures set forth in the applicable business associate agreement, we will allow an individual to request an accounting of each disclosure that we make of the individual's PHI for up to 6 years prior to the request.

ii. We will respond to the individual's request for a disclosure accounting within 60 days of its receipt or we may respond to the covered entity to whom the request was made.

iii. We may not charge for an individual's first accounting in any 12 month period. We may charge a reasonable, cost–based fee for other accountings within that same 12-month period.

iv. Exempt disclosures include disclosures made:

1. to the individual or personal representative

2. for notification of or to persons involved in an individual's health care or payment related to that health care

3. pursuant to an authorization

4. in a limited data set

5. for national security or intelligence purposes

6. to correctional institutions or law enforcement officials regarding inmates or individuals in lawful custody

7. incident to otherwise permitted or required uses or disclosures

10. WORK FORCE TRAINING

a. Each member of our workforce who may have access to or use of PHI will receive training on this Policy, as necessary and appropriate for the member to carry out his or her job functions.

   i. New members of our workforce must receive privacy training before they may have access to or use of PHI.

   ii. Existing workforce members must receive retraining within a reasonable period of time after there is material change in their job functions or in this Policy that affects their access to or use of PHI.

b. Workforce members who violate this Policy or applicable federal or state privacy law will be subject to disciplinary action, including employment termination, consistent with the sanctions developed, documented, and disseminated by our Privacy Official.

c. 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 Privacy 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 Privacy Official or our legal advisers.

11. BUSINESS ASSOCIATE AGREEMENTS

a. **FORM:** HIPAA Subcontractor Associate Agreement

b. We will not disclose PHI to a subcontractor, or allow a subcontractor to create or receive PHI on our behalf, unless our Privacy Official or our legal advisers confirm that the subcontractor has entered into a compliant written contract with us.

c. If we learn that a subcontractor has materially breached the subcontractor contract, we will require the subcontractor to promptly cure the breach. If the subcontractor fails to cure the breach to our satisfaction, we will terminate the subcontractor contract and our subcontractor relationship with that subcontractor. If termination of the contract is not feasible, we will report the subcontractor's breach to HHS.

12. COMPLAINTS

a. **Form:** Complaint

b. We will timely investigate and appropriately respond to each written complaint received by our Privacy Officer or a workforce member regarding our compliance with this Policy and applicable state and federal privacy laws.

c. We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our patients.

13. BREACHES

a. We will develop policies and procedures to identify suspected breaches of PHI. Our Privacy Official will be responsible for such investigation and identification.

b. We will work with the applicable covered entity to notify all relevant parties of a breach of PHI, in accordance with HIPAA's rules and the applicable business associate agreement. Relevant parties include the U.S. Department of Health and Human Services, affected individuals and, for certain large breaches effecting 500 or more individuals, local media.

c. We will have and implement contingency plans to mitigate any deleterious effect of an improper use or disclosure of PHI by a member of our workforce. Our Privacy Official will coordinate with our legal advisers to develop contingency plans to mitigate, to the extent possible, any deleterious effect of improper use or disclosure of PHI.

14. OTHER

a. Remuneration. We will not directly or indirectly receive remuneration in exchange for any PHI of an individual unless we obtain from the individual a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that individual.

b. Record Retention. We will retain the documentation required by this Policy and the Privacy Rules until 6 years after the later of its creation or last effective date.

c. Waiver. We will not require an individual to waive any right under the Privacy Rules, including the right to complain to HHS, as a condition of providing claims payment, enrollment or benefits eligibility to the individual.

d. Retaliation. We will not, and we will not tolerate any workforce member who attempts to, intimidate, threaten, coerce, discriminate or retaliate against an individual who:

i. Exercises any right, including filing complaints, under any privacy laws.

ii. Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.

iii. Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of PHI).

e. Data Safeguards.

i. We will implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of PHI against any intentional or unintentional use or disclosure in violation of this Policy or the Privacy Rules. These safeguards will include reasonable limits to incidental uses or disclosures of PHI made as a result of otherwise permitted or required uses or disclosures.

ii. Our Privacy Official, in conjunction with our legal advisers, will augment this Policy with such additional data security policies and procedures as appropriate for our business to have reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the PHI we maintain against any reasonably anticipated unauthorized use or disclosure, intentional or unintentional, or any reasonably anticipated threat or hazard to the privacy, security or integrity of the PHI. These additional data security policies and procedures will ensure compliance by our workforce members with this Policy, the Privacy Rules, and such other policies and procedures as may be adopted to implement our compliance obligations under the Privacy Rules.