

BUSINESS ASSOCIATE AGREEMENT

INSERT NAME OF ENTITY OR PERSON

This Business Associate Agreement (the "Agreement") is made by and among **GREAT RIVERS BEHAVIORAL HEALTH ORGANIZATION**, (herein referred to as "Covered Entity") and **INSERT NAME OF ENTITY OR PERSON** (hereinafter known as "Business Associate"). Covered Entity and Business Associate shall collectively be known herein as the "Parties".

WHEREAS, Covered Entity wishes to commence a business relationship with Business Associate that shall be memorialized in a separate agreement (the "Underlying Agreement") pursuant to which Business Associate may be considered a "business associate" of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") including all pertinent regulations (45 CFR Parts 160 and 64) issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5); and

WHEREAS, the nature of the prospective contractual relationship between Covered Entity and Business Associate may involve the exchange of Protected Health Information ("PHI") as that term is defined under HIPAA; and

For good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this agreement for the purpose of ensuring compliance with the requirements of HIPAA, its implementing regulations, the HITECH Act;

NOW THEREFORE, the premises having been considered and with acknowledgment of the mutual promises and of other good and valuable consideration herein contained, the Parties, intending to be legally bound, hereby agree as follows:

I. DEFINITIONS. Capitalized terms used in this Agreement, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the HIPAA Privacy Regulations and the HIPAA Security Regulations. Unless otherwise stated, a reference to a "Section" is to a Section in this Agreement. For purpose of this Agreement, the following terms shall have the following meaning.

A. **Individual.** "Individual" shall have the same meaning as the term "individual" in 45 CFR §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

B. **Breach.** "Breach" means the acquisition, access, Use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR §164.402.

C. **Designated Record Set.** "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

D. **Privacy Rule.** “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E, as amended by the HITECH Act and as may otherwise be amended from time to time.

E. **Protected Health Information.** “Protected Health Information” or “PHI” means individually identifiable health information (including ePHI) created, received, maintained or transmitted by a Business Associate on behalf of a health care component of the Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for provision of health care to an Individual. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. PHI does not include Information regarding a person who has been deceased for more than fifty (50) years; employment records held by Covered Entity in its role as employer; or Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and student records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

F. **Required By Law.** “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR §164.501.

G. **Secretary.** “Secretary” shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.

H. **Security Incident.** “Security Incident” shall mean the attempted or successful unauthorized access, Use, disclosure, modification or destruction of information or interference with system operations in an information system.

I. **Subcontractor.** “Subcontractor” means a Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of another Business Associate.

J. **Unsecured Protected Health Information.** “Unsecured Protected Health Information” or “Unsecured PHI” shall mean PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in the §13402(h) of the HITECH Act.

K. **Use.** “Use” includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information.

II. USE OR DISCLOSURE OF PHI BY BUSINESS ASSOCIATE.

A. Except as otherwise limited in this Agreement, Business Associate may only Use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement, provided that such Use or disclosure would not violate the Privacy Rule.

B. Business Associate shall only Use and disclose PHI if such Use or disclosure complies with each applicable requirement of 45 CFR §164.504(e).

C. Business Associate shall be directly responsible for full compliance with the relevant requirements of the Privacy Rule to the same extent as Covered Entity.

III. DUTIES OF BUSINESS ASSOCIATE RELATIVE TO PHI.

A. **Limitation on Uses and Disclosures.** Business Associate shall not Use or disclose PHI other than as permitted or required by this Agreement or as required by law.

B. Safeguards. Business Associate shall protect PHI from, and shall Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to EPHI, to prevent the unauthorized Use or disclosure of PHI other than as provided for in this Agreement or as required by law, for as long as the PHI is within its possession and control, even after the termination or expiration of this agreement.

Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Specifically, and without intending to alter the generality of its responsibilities set forth in this Section III.B, Business Associate shall implement the safeguards required under **Exhibit A**. Business Associate acknowledges and agrees that the standards set forth in **Exhibit A** are solely minimum standards of Covered Entity and that compliance with the same does not substitute for Business Associate's obligation to comply with the requirements of this Agreement or applicable law.

C. Minimum Necessary Standard. Business Associate shall apply HIPAA minimum necessary standard to any Use or disclosure of PHI necessary to achieve the purpose of the Underlying Agreement. See 45 CFR §164.514 (d)(2) through (d)(5).

D. Impermissible Use or Disclosure of PHI. Business Associate shall immediately notify by email to Covered Entity of all Uses and disclosures of PHI not provided for by this Agreement within one (1) business day of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required by 45 CFR 164.410 (Notification by Business Associate), as well as any Security Incident of which it becomes aware. Upon request by Covered Entity, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

E. Subcontracts and other Third Party Agreements. In accordance with 45 CFR 164.502(e)(1)(II), 164.504(e)(1)(i), and 164.308(b)(2) Business Associate agrees to ensure that any agents, Subcontractors, independent contractors or other third create, receive, maintain or transmit PHI on Business Associate on behalf of Covered Entity agrees to enter into a written contract that contains the same terms, restrictions, requirements and conditions that apply through this Agreement to Business Associate with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR §164.314(a)(2)(b) and 164.504(e)(5).

F. Access. To the extent applicable, Business Associate shall provide access to PHI in a Designated Record Set at reasonable times, at the request of Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524.

When the request is made by the Individual to the Business Associate or if Covered Entity asks the Business Associate to respond to a request, the Business Associate shall comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by Covered Entity, the Business Associate shall provide the records to Covered Entity within ten (10) business days.

G. Amendment. To the extent applicable, Business Associate shall make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of Covered Entity or an Individual.

H. Accounting of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for a

Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528.

Business Associate agrees to within ten (10) business days of request from Covered Entity provide Covered Entity with information in a format and manner sufficient to respond in a timely manner to the Individual's request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR §164.504(e)(2)(ii)(G) and 164.528(b)(1).

At the request of Covered Entity or in response to a request made directly to the Business Associate by an Individual, Business Associate shall respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

Business Associate record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

I. **Consent to Review.** Business Associate shall, upon request with reasonable notice, provide Covered Entity and or Department of Social and Health Services (DSHS) access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI.

J. **Consent to Audit.** Business Associate shall make its internal practices, books, records, and any other material requested by the Secretary relating to the Use, disclosure, and safeguarding of PHI received from Covered Entity available to the Secretary for the purpose of determining compliance with the Privacy Rule. The aforementioned information shall be made available to the Secretary in the manner and place as designated by the Secretary or the Secretary's duly appointed delegate. Under this Agreement, Business Associate shall comply and cooperate with any request for documents or other information from the Secretary directed to Covered Entity that seeks documents or other information held by Business Associate.

K. **Federal and State Authorities.** Business Associate may Use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. §164.502(j)(1).

L. **Use for Proper Management and Administration.** Except as otherwise limited in this Agreement, Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate.

M. **Disclosure for Proper Management and Administration.** Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and Used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

N. **Failure to Cure.** If TRSN learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this Agreement and reasonable steps by TRSN do not end the violation, TRSN shall terminate the Underlying Agreement, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate's obligations

under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate shall terminate the subcontract, if feasible.

O. **Liability.** Within ten (10) business days, Business Associate must notify Covered Entity of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform Covered Entity of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

IV. OBLIGATION OF COVERED ENTITY.

A. **Requested Restrictions.** Covered Entity shall notify Business Associate, in writing, of any restrictions on the Use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, which permits an Individual to request certain restrictions of uses and disclosures, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

B. **Changes in or Revocation of Permission.** Covered Entity will notify Business Associate in writing of any changes in, or revocation of, permission by an Individual to Use or disclose PHI, to the extent that such changes or revocation may affect Business Associate's use or disclosure of PHI.

C. **Permissible Requests by Covered Entity.** Covered Entity shall not request Business Associate to Use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Regulations and HIPAA Security Regulations if done by Covered Entity, except to the extent that Business Associate will Use or disclose PHI for or management and administrative activities of Business Associate.

V. TERM AND TERMINATION.

A. **Term.** The Term of this Agreement shall be effective as of the date the Underlying Agreement is effective, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section IV.

B. **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, terminate this Agreement;

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure is feasible, report the violation to the Secretary.

C. **Effect of Termination.**

1. Except as provided in paragraph C(2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on

behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall not retain any copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. After written notification that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further Uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

3. Should Business Associate make a disclosure of PHI in violation of this Agreement, Covered Entity shall have the right to immediately terminate any contract, other than this Agreement, then in force between the Parties, including the Underlying Agreement.

VI. CONSIDERATION. Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

VII. IN EVENT OF A BREACH.

A. In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from Covered Entity or involving Covered Entity clients, Business Associate will take all measures required by state or federal law.

B. Business Associate will notify Covered Entity within one (1) business day by telephone and in writing of any acquisition, access, Use or disclosure of PHI not allowed by the provisions of this Agreement or not authorized by HIPAA Rules or required by law of which it becomes aware which potentially compromises the security or privacy of the Protected Health Information as defined in 45 CFR 164.402 (Definitions).

C. Business Associate shall promptly notify Covered Entity by telephone or email of any potential Breach of security or privacy of PHI by the Business Associate or Business Associate's employee, office or agents. Business Associate's notification to Covered Entity hereunder shall:

1. Be made to Covered Entity no later than one (1) business day after discovery of the Breach, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security;
2. Include the individuals whose Unsecured PHI has been, or is reasonably believed to have been, the subject of a Breach; and
3. Be in substantially the same form as Exhibit B hereto.

D. In the event of an unauthorized Use or disclosure of PHI or a Breach of Unsecured PHI, Business Associate shall mitigate, to the extent practicable, any harmful effects of said disclosure that are known to it.

E. If Covered Entity determines that Business Associate or its Subcontractor(s) or agent(s) is responsible for a Breach of unsecured PHI:

1. requiring notification of Individuals under 45 CFR 164.404 (Notification to Individuals), Business Associate bears the responsibility and costs for notifying the affected

Individuals and receiving and responding to those Individuals' questions or requests for additional information;

2. requiring notification of the media under 45 CFR 164.406 (Notification to the media), Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;

3. requiring notification of the U.S. Department of Health and Human Services Secretary under 45 CFR 164.408 (Notification to the Secretary), Business Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and Covered Entity will take appropriate remedial measures up to termination of this Underlying Agreement.

VIII. MODIFICATION. This Agreement may only be modified through a writing signed by the Parties and, thus, no oral modification hereof shall be permitted. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

IX. INTERPRETATION OF THIS CONTRACT IN RELATION TO OTHER CONTRACTS BETWEEN THE PARTIES. Should there be any conflict between the language of this contract and any other contract entered into between the Parties (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement shall control and prevail unless the Parties specifically refer in a subsequent written agreement to this Agreement by its title and date and specifically state that the provisions of the later written agreement shall control over this Agreement.

X. COMPLIANCE WITH STATE LAW. The Business Associate acknowledges that by accepting the PHI from Covered Entity, it becomes a holder of medical records information and is subject to the provisions of State law. If the HIPAA Privacy or Security Rules and the State Law conflict regarding the degree of protection provided for protected health information, Business Associate shall comply with the more restrictive protection requirement.

XI. MISCELLANEOUS.

A. **Ambiguity.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

B. **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

C. **Survival.** The obligations of the Business Associate under this section shall survive the termination or expiration of the Underlying Agreement.

D. **Notice to Covered Entity.** Any notice required under this Agreement to be given Covered Entity shall be made in writing to:

Cover Entity Contact: GRBHO Compliance Officer
Address: PO Box 1447
Chehalis, WA 98532
Attention: Compliance Officer / Privacy Officer
Phone: (360) 795-5955
Email: MBollinger@greatriversbho.org

E. **Notice to Business Associate.** Any notice required under this Agreement to be given Business Associate shall be made in writing to:

Contact Title _____
Address: _____

Attention: _____
Phone: _____
Email: _____

IN WITNESS WHEREOF and acknowledging acceptance and agreement of the foregoing, the Parties affix their signatures hereto.

Great Rivers Behavioral Health Organization:	Insert Name of Entity or Person
By: _____	By: _____
Name: <u>Marc Bollinger</u>	Name: _____
Title: <u>Great Rivers BHO CEO</u>	Title: _____
Date: _____	Date: _____

EXHIBIT A

DATA SECURITY REQUIREMENTS

1. **Data Transport.** When transporting Confidential Information electronically, including via email, the data will be protected by:
 - a. Transporting the data within the (State Governmental Network) SGN or Business Associate's internal network, or;
 - b. Encrypting any data that will be in transit outside the SGN or Business Associate's internal network. This includes transit over the public Internet.

2. **Protection of Data.** The Business Associate agrees to store data on one or more of the following media and protect the data as described:
 - a. **Hard disk drives.** Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

 - b. **Network server disks.** Data stored on hard disks mounted on network servers and made available through shared folders. Access to the data will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For confidential data stored on these disks, deleting unneeded data is sufficient as long as the disks remain in a secured area and otherwise meets the requirements listed in the above paragraph. Destruction of the data as outlined in Section 4. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the secure environment.

 - c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** PHI data provided by on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a secure area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access PHI data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

 - d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** PHI data provided by on optical discs which will be attached to network servers and which will not be transported out of a secure area. Access to data on these discs will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which

is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents.** Any paper records must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

f. **Data storage on portable devices or media.**

(1) TRSN data shall not be stored by the Business Associate on portable devices or media unless specifically authorized within the contract. If so authorized, the data shall be given the following protections:

(a) Encrypt the data with a key length of at least 128 bits

(b) Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.

(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

Physically protect the portable device(s) and/or media by:

(d) Keeping them in locked storage when not in use

(e) Using check-in/check-out procedures when they are shared, and

(f) Taking frequent inventories

(2) When being transported outside of a secure area, portable devices and media with confidential data must be under the physical control of Business Associate staff with authorization to access the data.

(3) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers if those computers may be transported outside of a secure area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

EXHIBIT B

**FORM OF NOTIFICATION TO COVERED ENTITY OF
BREACH OF UNSECURED PHI**

This notification is made pursuant to Section III.E(3) of the Business Associate Agreement between:

Great Rivers Behavioral Health Organization (GRBHO), and
_____ (Business Associate).

Business Associate hereby notifies TRSN that there has been a breach of unsecured (unencrypted) protected health information (PHI) that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Detailed description of the breach: _____

Date and Time of the breach: _____

Date of the discovery of the breach: _____

Location and Nature of the PHI: _____

Number of individuals affected by the breach: _____

The types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code):

Origination and destination of PHI: _____

Description of what Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches:

For questions or to learn additional information:

Name: _____

Title: _____

Address: _____

Email Address: _____

Phone Number: _____