	Privacy	Rio Grande Valley HIE	Policy: P9
	Effective Date 11/06/2015	**Last Date Revised/Updated** 11/06/2015	**Date Board Approved:** 11/06/2015
Subject: Business Associate Agreements			

FEDERAL AND STATE REGULATIONS:

45 CFR 164.502(e)(1)(ii)
45 CFR 164.504(e)(1)(iii); (e)(5)
45 CFR 164.308(b)(2)
45 CFR 164.314(a)
45 CFR 160.103, definition of Business Associate

POLICY:

RGV HIE is a Business Associate of Participating Providers who are Covered Entities and will execute a Business Associate Agreement (BAA) with each of its Participants before receiving any protected health information (PHI) from a Participant. Additionally, RGV HIE will execute a BAA with any subcontractor that RGV HIE delegates a function, activity, or service, other than in the capacity of a workforce member, that involves the creation, receipt, maintenance, or transmission of PHI. RGV HIE will execute a BAA with technology vendors that receive PHI. *See the BAA Template attached for reference.*

PROCEDURE:

1. **Participant BAAs**. RGV HIE will execute a BAA with each of its Participating Providers prior to receiving any PHI from the Participant, that contains all the provisions required by HIPAA and state law.

2. **Subcontractor BAAs**. RGV HIE will execute a BAA with any entity that receives PHI from RGV HIE and performs a function on behalf of the HIE, that contains all the provisions required by HIPAA and state law.

   A. **Identification of Subcontractors**. The RGV HIE Executive Director will review all uses and disclosures by subcontractors; determine which receive, access or otherwise use PHI on behalf of RGV HIE; and negotiate appropriate BAAs and amendments. RGV HIE will include in the BAA with subcontractors any applicable limitations on its uses and disclosures included in its BAA with Participating Providers.

   B. **Subcontractor's Obligations**. RGV HIE will include in the BAA the requirement that subcontractor assist RGV HIE in a timely manner whenever one of the Participating Provider's patients seeks to exercise his or her privacy rights regarding health information that is maintained by the subcontractor. This includes the ability to do the following:

i.   Provide the patient with copies or access to any PHI about the patient that the subcontractor maintains in a "designated record set," upon RGV HIE's request.

ii. Amend any PHI about the patient that the subcontractor maintains in a designated record set, upon RGV HIE's request.

iii. Maintain an accounting of all disclosures for purposes other than for treatment, payment, and health care operations, and provide the accounting upon RGV HIE's request.

iv. Comply with all the Participating Providers' requests regarding confidential communications and restrictions on the use and disclosure of PHI.

C. **Notification to Subcontractor**. HIE should notify its subcontractors in writing whenever it changes its policies or procedures in a manner that affects the subcontractor. RGV HIE will document the name of the person notified and the date when the subcontractor was notified of the change.

D. **Minimum Necessary Disclosures**. All disclosures to subcontractors must be limited to the minimum amount of information needed for the subcontractor to carry out its functions on behalf of HIE, unless an exception to the minimum necessary rule applies by law and pursuant to HIE's policies.

E. **Violations by Subcontractor**. If HIE learns, or has reason to believe, that the subcontractor is in violation of the BAA, or is in any way jeopardizing the privacy and confidentiality of HIE's Participant's information, the subcontractor must be notified immediately to cease such activities.

i.   If the violation is not remedied, the agreement with the subcontractor must be terminated. A reasonable cure period may be allowed.

ii. If termination is not feasible because the subcontractor is the only qualified and available vendor for such services, the Executive Director must notify the Secretary of Health and Human Services of the problem, and shall continue to seek to require the subcontractor to remedy the violations.

F. **Termination of BAA with a Subcontractor**. If the BAA is terminated for any reason, the subcontractor must do the following:

i.   Return all PHI still in its possession, or assure that the information is properly destroyed in a manner that protects the confidentiality of the information. The subcontractor must provide a certificate of destruction showing that the information has been properly destroyed.

ii. If any of the information cannot be returned or destroyed for example, because the subcontractor is required to maintain certain information for inspection by regulatory agencies, the subcontractor may retain the information as long as it continues to protect the information in accordance with the terms of the subcontractor BAA and to use the information only for the purposes that make return or destruction infeasible.

G. **Documentation.** This version of the policy, together with any forms and other documentation obtained in accordance with the policy, shall be retained for a minimum of six years.

BUSINESS ASSOCIATE AGREEMENT TEMPLATE

This Business Associate Agreement ("BA Agreement") is entered into by and between _____ [referred to as "Covered Entity" in this BA Agreement] and Rio Grande Valley Health Information Exchange ("RGV HIE"), a Texas non-profit health information exchange organization, located at 1413 Stuart Place Rd., Ste. C Harlingen, Texas 78552. This BA Agreement is effective as of the execution date.

RECITALS

WHEREAS, Business Associate provides services to its members, each of whom are Covered Entities under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA");

WHEREAS, Covered Entity is required to protect the privacy and security of Protected Health Information, including Electronic Protected Health Information, (collectively "PHI"), and to obtain written assurances that Business Associate will protect the privacy and security of PHI disclosed to or created by Business Associate on its behalf in compliance HIPAA, The Health Information Technology for Economic and Clinical Health ("HITECH") Act, and regulations by the U.S. Department of Health and Human Services, and other applicable federal and state privacy and security laws; and

WHEREAS, the HIPAA Privacy Rule and Security Rules and HITECH require Covered Entity and Business Associate to enter into this BA Agreement containing specific requirements prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.502(e) and 164.504(e) of the Code of Federal Regulations ("CFR");

WHEREAS, HITECH imposes penalties against both Covered Entity and Business Associate for breach of unsecured PHI; and

WHEREAS, Covered Entity and Business Associate are required to protect the security of PHI pursuant to HIPAA, HITECH and other state and federal privacy laws;

NOW, THEREFORE, in consideration of the mutual promises below and other consideration contained herein, the sufficiency of which is hereby acknowledged, the parties agree as follows:

I. DEFINITIONS

1. *"Business Associate"* shall have the meaning given to the term "Associate" under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

2. *"Covered Entity"* shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

3. *"Electronic Protected Health Information"* or *"EPHI"* shall have the meaning given to such term under the HIPAA Rule, including but not limited to 45 CFR Parts 160, 162, and 164, and under HITECH.

4. *"Privacy Rule"* shall mean the HIPAA Regulation that is codified at 45 CFR Parts 160, 162 and 164.

5. *"Security Rule"* shall mean the HIPAA regulation that is codified at 45 C.F.R. Part 164.

6. *"Protected Health Information"* or *"PHI"* means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501. *[45 CFR §§160.103 and 164.501.*

7. The Health Information Technology for Economic and Clinical Health ("HITECH") Act shall mean Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). The U.S. Department of Health and Human Services ("HHS") interim final rule at 74 Fed. Reg. 42,740 implements the security breach notice provisions of HITECH.

II. OBLIGATIONS OF BUSINESS ASSOCIATE

Business Associate shall maintain the security and confidentiality of PHI received from or created on behalf of Covered Entity as required by applicable laws and regulations, including HIPAA and HITECH, the regulations promulgated thereunder, and applicable state law. Without limiting the foregoing, Business Associate agrees to the following:

1. **Use of PHI:** Business Associate shall not use and shall ensure that its directors, officers, employees, contractors, and agents, do not use PHI other than as expressly permitted by this BA Agreement, by the Services Agreement, or as required by law. Further, Business Associate shall not use PHI in any manner that would constitute a

violation of the Privacy Rule if so used by Covered Entity, except that Business Associate may use PHI for the purposes of managing and administering its internal business processes relating to its responsibilities under this BA Agreement and to carry out the legal responsibilities of the Business Associate as set forth therein. In addition, Business Associate may use PHI to provide data aggregation services relating to health care operations of the Covered Entity, if Covered Entity elects to receive such services.

2. **Disclosure of PHI:**

    a. *Disclosure to Third Parties.* Business Associate shall not [and shall provide that its directors, officers, employees, subcontractors, and agents, do not] disclose PHI to any other person (other than members of their respective workforce as specified in subsection b. of this Section), unless disclosure is required by law or authorized by the person whose PHI is to be disclosed, provided however, Business Associate may disclose PHI which does not arise from Opt Out Health Data to other providers participating in the health information exchange managed by Business Associate.

    b. Any such disclosure other than as specifically permitted in the immediately preceding sentences shall be made only if such disclosee has previously signed a written agreement that:

        i.   Binds the disclosee to the provisions of this BA Agreement pertaining to PHI, for the express benefit of Covered Entity, Business Associate and, if disclosee is other than Business Associate, the disclosee.

        ii. Contains assurances from disclosee that the PHI will be held confidential as provided in this BA Agreement, and only disclosed as required by law for the purposes for which it was disclosed to disclosee; and

        iii. Obligates disclosee to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent disclosee has obtained knowledge of such breach.

    c. *Disclosure to Workforce.* Business Associate shall not disclose PHI to any member of its workforce and shall provide that its subcontractors and agents do not disclose PHI to any member of their respective workforces, unless Business Associate or such subcontractor or agent has advised such person of Business Associate's obligations under this BA Agreement, and of the consequences for such person and for Business Associate or such subcontractor or agent of violating them. Business Associate shall take and shall provide that each of its subcontractors and agents take appropriate disciplinary action against any member of its respective workforce who uses or discloses PHI in contravention of this BA Agreement.

d. *Disclosure for Marketing Purposes.* Business Associate shall not sell PHI provided by Covered Entity for any purpose or share such PHI with any third party for marketing purposes unless the Board of Directors decide to engage in such activities. In this instance, this BA Agreement will be amended to reflect the use of PHI provided by Covered Entity for these purposes.

e. *Disclosure for Fundraising Purposes.* The RGV HIE Board of Directors may decide to approve the use, or disclosure to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for RGV HIE without an authorization: Demographic information relating to an individual; and dates of health care provided to the individual. However, no PHI shall be used in grant applications or other proposals which would be available to the general public.

f. *Disclosure for Research Purposes.* Any program or project in which individually identifiable data that includes data obtained from Covered Entity is requested by researchers or entities that are not participants of RGV HIE's must be regarded as research that must be approved by the Board of Directors. The Board of Directors may approve use of data for clinical trials, provided all HIPAA requirements are met. Any request for individually identifiable data from a RGV HIE participant must also follow this process, with regard to patients who are not the participant's patients. Covered Entity will be notified and their approval obtained, prior to releasing location specific data regarding services at Covered Entity's facilities to either another RGV HIE participant or non RGV HIE participant. Such data includes the name and/or address of a Covered Entity facility linked with the data regarding patient utilization.

3. **HIPAA Safeguards:** Business Associate shall implement all appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this BA Agreement. Business Associate shall provide Covered Entity with such information concerning such safeguards as Covered Entity may from time to time request. Business Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Covered Entity's PHI and EPHI.

4. **Accounting of Disclosures:**

a. Business Associate shall maintain a record of all PHI disclosures made under this BA Agreement, including the date of disclosure, the name and, if known, the address of the recipient of PHI, a brief description of the PHI disclosed, and the purposes of the disclosures.

b. Within ten (10) days of notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of disclosures of PHI regarding an individual, Business Associate and its agents or subcontractors

shall make available to Covered Entity such information as is in Business Associate's possession and that is required for Covered Entity to make the accounting.

c. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall prepare and deliver any such accounting requested in accordance with the requirements of 45 CFR Section 164.528.

5. **Reporting of Disclosures of Protected Health Information in violation of HIPAA:**

Business Associate shall, within three (3) days of becoming aware of a disclosure of PHI or EPHI in violation of this BA Agreement by Business Associate, (its officers, directors, employees, contractors, or agents,) or by a third party to which Business Associate disclosed PHI, report such disclosure in writing to the Covered Entity and the remedial action taken or proposed to be taken with respect to such use or disclosure. Business Associate shall take all commercially reasonable action to mitigate any harm caused by inappropriate disclosure.

6. **Reporting Breaches of Protected Health Information in violation of HITECH**:

Business Associate shall:

a. Secure PHI (including data in motion, data at rest, data in use and data disposed), created by Business Associate, or accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used, or disclosed by Business Associate, on behalf of Covered Entity, by encrypting data whenever appropriate as determined by RGV HIE's security risk assessment and in compliance with standard business practices and HIPAA guidance for security requirements.

b. Under HITECH, a breach occurs when there is an unauthorized acquisition, access, use or disclosure of unsecured PHI, including ePHI, which compromises the security or privacy of the PHI/ePHI. A breach compromises the security or privacy of PHI/ePHI if it poses a significant risk of financial, reputational, or other harm to the individual whose PHI/ePHI was compromised.

1. Business Associate agrees to:
   a. implement a system to detect breaches of PHI/ePHI within Business Associate's business;
   b. maintain written documentation with respect to all suspected and confirmed breaches for six (6) years;
   c. provide access to such documentation to Covered Entity upon request;
   d. develop breach notification policies and procedures,;

e. train workforce members on, and have sanctions for failure to comply with, these policies and procedures;

f. allow workforce members to file complaints regarding these policies and procedures or a failure to comply with them, and refrain from intimidating or retaliatory acts towards its workforce members;

2. In the event that there is a breach of unsecured PHI/ePHI, Business Associate agrees to:

a. notify Covered Entity on the first day that a breach is known to Business Associate, or by exercising reasonable diligence, would have been known to Business Associate;

b. provide Covered Entity, to the extent possible, with the identity of each individual whose unsecured PHI/ePHI has been, or is reasonably believed to have been, breached. The Parties agree that the breaching Party shall be responsible for the costs of notifying individuals.

c. cooperate in conducting a risk assessment, as instructed by, and under the direction of, Covered Entity, to determine whether the privacy or security of individuals' PHI/ePHI was compromised as a result of the breach,

d. mitigate any harm to individuals whose PHI/ePHI has been breached;

e. comply with HIPAA requirements regarding breach notification to the U.S. Department of Health and Human Services

3. comply with the HIPAA obligations of Paragraph 5 above related to unauthorized use and disclosures of PHI,

4. destroy all paper, film, or other hard copy media by shredding or destruction, and destroy electronic media by clearing, purging or destruction consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

7. **Agreements by Third Parties:** Business Associate shall enter into a written agreement with any agent or subcontractor that will have access to PHI or EPHI that is received from, or created or received by Business Associate on behalf of Covered Entity pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms, and conditions that apply to Business Associate pursuant to this BA Agreement.

8. **Disclosure to U.S. Department of Health and Human Services:** Business Associate shall make its internal practices, books, and records relating to the use and disclosures of PHI available to the Secretary of the United States Department of Health and Human Services, for purposes of determining compliance with HIPAA. Business Associate shall provide to Covered Entity a copy of any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary of the United States Department of Health and Human Services.

9. **Access by Individuals:** Within fifteen (15) days of receipt of a request by Covered Entity or an individual, Business Associate shall permit Covered Entity and any individual whose PHI is maintained by Business Associate to have access to and to copy his or her PHI, in the format requested, unless it is not readily producible in such format, in which case it shall be produced in hard copy format. RGV HIE will not make independent decisions with respect to the denial of access to Protected Health Information (PHI) with respect to data which is excepted from disclosure or to which the Covered Entity may deny access under HIPAA. RGV HIE will comply with the decision of the Member to deny access. Business Associate will consult with Covered Entity before providing any requested information.

10. **Amendment of PHI**: Within fifteen (15) days of receipt of a request from Covered Entity for an amendment of PHI or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable the Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to 45 CFR Section 164.526. If any individual requests an amendment of PHI directly from Business Associate, Business Associate must notify Covered Entity in writing within five (5) days of the request and comply with Covered Entity's directions regarding such amendment where HIPAA allows the provider discretion.

11. **Minimum Necessary**: Business Associate and its agents or subcontractors shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure in accordance with 45 CFR §164.514(d)(3).

12. **Data Ownership**: Business Associate acknowledges that Business Associate has no ownership rights with respect to PHI provided by Covered Entity.

13. **Termination**: If either Party becomes aware of a pattern of activity or practice that constitutes a material breach or violation of the obligations under the provisions of this BA Agreement, either Party has the option to terminate the Agreement upon demanding a cure within ten (10) days of obtaining such knowledge. If the other Party fails to cure such breach within the ten (10) day period, Covered Entity has the right to terminate the Agreement immediately. Any breaches or violations of the obligations under this BA Agreement are subject to the indemnification provisions set forth in Section II, Paragraph 15, below, and such indemnification obligations shall survive the termination of the Agreement.

14. **Procedure Upon Termination**:

a. Upon termination of this BA Agreement for any reason, the Business Associate, and its subcontractors or agents, shall return or destroy all PHI (at the discretion of the Business Associate) that it maintains in any form, and shall retain no copies of such information. If Business Associate elects to destroy the PHI in its sole

discretion, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

b. Business Associate shall continue to extend the protections of this BA Agreement to any information that remains in the Business Associate's possession after termination, if any, and the applicable provisions of this BA Agreement relating to protecting such remaining information shall survive termination of this Agreement.

15. **Indemnification**: To the extent caused by such party, the parties agree to indemnify, defend, and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents, or other members of its workforce against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from any negligence or wrongful acts or omissions by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce during its performance of this Agreement. The indemnifying party shall reimburse for all actual and direct losses, liabilities, fines, penalties, costs or expenses including reasonable attorney fees, which may be imposed as a result of an indemnifying party's actions except that no consequential or punitive damages shall be recoverable. The parties' obligation to indemnify shall survive the expiration or termination of this Agreement.

16. **No Third Party Beneficiaries**: Nothing express or implied in this BA Agreement is intended to confer, nor shall anything in this document confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

17. **Effect on Agreement**: Except as specifically required to implement the purposes of this BA Agreement, or to the extent inconsistent with this BA Agreement, all other terms of the Agreement shall remain in force and effect.

III.   MISCELLANEOUS

1. **Notice:** All notices, requests, demands and other communications required or permitted to be given hereunder shall be sent by (a) certified mail, return receipt requested, or (c) commercial carrier that provides a signed receipt verifying actual delivery at the address set forth below. Such notices shall be deemed given five (5) business days after being deposited in the United States mail or when receipt acknowledged, if sent by facsimile:

If to Business Associate:	If to Covered Entity:
RGV HIE:_____	Name/Title:_____
Telephone:_____	Telephone:_____
Facsimile: _____	Facsimile:_____

2.	**Governing Law:** This BA Agreement shall be construed, and the rights and liabilities of the parties hereto determined, in accordance with the internal laws of the State of Texas.

3.	**Titles and Headings:** Titles and headings to sections herein are for purposes of reference only, and shall in no way limit, define, or otherwise affect the provisions herein.

4.	**Entire Agreement:** This BA Agreement, constitutes the entire agreement between the parties, and supersedes all prior agreements, whether written or oral, between the parties.

5.	**No Third Party Rights:** The parties agree that it is their specific intention to create no third party rights by virtue of this BA Agreement.

6.	**References to Time:** All references to days in this BA Agreement shall be references to calendar days, unless expressly stated otherwise.

7.	**Independent Contractors:** The parties are and shall be independent contractors to one another, and nothing in this BA Agreement shall be deemed to cause this BA Agreement to create an agency, partnership, or joint venture between the parties. Except as expressly provided herein, neither party shall be liable for any debts, accounts, obligations, or other liabilities of the other party.

8.	**Assignment:** This BA Agreement shall be binding on the parties and their successors and assigns, provided that neither party shall assign any of its rights under this BA Agreement to any other party without the prior written consent of the other party.

9.	**Severability:** In the event that any court or any governmental authority or agency declares all or party of any section of this BA Agreement to be unlawful or invalid, such unlawfulness or invalidity shall not serve to invalidate any other section of this BA Agreement, and in the event that only a portion of any section is so declared to be unlawful or invalid, such unlawfulness or invalidity shall not serve to invalidate the balance of such section.

10.	**Counterparts:** This BA Agreement may be executed in two or more counterparts, each of which shall be deemed to be an original, but all of which shall constitute one and the same agreement.

        IN WITNESS WHEREOF, the parties hereto have duly executed this BA Agreement as of the date first set forth above.

COVERED ENTITY   **BUSINESS ASSOCIATE**
                                           RIO GRANDE VALLEY HIE

By:_____   By:_____

Name: _____   Name: _____

Title: _____   Title: _____

Date of Execution:_____   Date of Execution: _____