EL RIO COMMUNITY HEALTH CENTER
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is entered into on this _____day of _____**, 20**___, between El Rio Santa Cruz Neighborhood Health Center the (Covered Entity), and _____. ("Business Associate"), with an effective date of _____. This Agreement sets out the responsibilities and obligations of Business Associate as a business associate of Covered Entity under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

RECITALS:

A. Business Associate may provide services to Covered Entity under a written agreement entered into before the effective date of this Agreement. If so, Written Agreement is titled_____, and has an effective date of_____.

B. Business Associate performs the services described in Written Agreement. If there is not a Written Agreement, Business Associate provides the following services to Covered Entity including but not limited to the following, and as may change from time to time: **Please see written "Agreement"**

C. Covered Entity may make available and/or transfer to Business Associate Protected Health Information ("PHI") of Individuals in conjunction with Services, which Business Associate will use or Disclose only in accordance with this Agreement.

AGREEMENT:

Business Associate and Covered Entity agree to the terms and conditions of this Agreement in order to comply with the rules on handling of Protected Health Information ("PHI") under the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Standards"), the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Standards"), and the HIPAA Breach Notification Regulations, 45 C.F.R. Part 164, Subpart D ("Breach Notification Regulations"), all as amended from time to time.

1. DEFINTIONS

a. **Terms Defined in Regulation:** Unless otherwise provided, all capitalized terms in this Agreement will have the same meaning as provided under the Privacy Standards, the Security Standards and the Breach Notification Regulations.

b. Protected Health Information or PHI: Protected Health Information or PHI, as defined by the Privacy Standards, for this Agreement means PHI that is received or created on behalf of Covered Entity by Business Associate.

2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

a. Performance of Services: Business Associate will Use or Disclose PHI only for those purposes necessary to perform Services, or as otherwise expressly permitted in this Agreement or required by law, and will not further Use or Disclose such PHI.

b. Subcontractor or Agent Performance of Services: Business Associate agrees that anytime it provides PHI to a subcontractor or agent to perform Services for Covered Entity, Business Associate first will enter into a contract or confidentiality agreement with such subcontractor or agent that contains the same terms, conditions, and restrictions on the Use and Disclosure of PHI as contained in this Agreement.

c. Business Associate Management, Administration and Legal Responsibilities: Business Associate may Use or Disclose PHI for Business Associate's management and administration, or to carry out Business Associate's legal responsibilities. Business Associate may Disclose PHI received from Covered Entity to a third party for such purposes only if: (1) the Disclosure is required by law; or (2) Business Associate secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) Use or Disclose the PHI only as required by law or for the purposes for which it was Disclosed to the recipient; and (iii) notify the Business Associate of any other Use or Disclosure of PHI.

d. Data Aggregation: Business Associate may Use PHI to perform data aggregation services as permitted by 45 CFR § 164.504(e)(2)(i)(B).

3. SAFEGUARDS FOR PROTECTED HEALTH INFORMATION

a. Adequate Safeguards: Business Associate will implement and maintain appropriate safeguards to prevent any Use or Disclosure of PHI for purposes other than those permitted by this Agreement, including administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any electronic protected health information ("ePHI"), if any, that Business Associate creates, receives, maintains, and transmits on behalf of Covered Entity. Upon request of Covered Entity, Business Associate will provide evidence to Covered Entity that these safeguards are in place and are properly managed.

b. Compliance with HIPAA Security Standards: Business Associate will comply with 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316, as of the date by which Business Associate is required to comply with such regulations.

4. REPORTS OF IMPROPER USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION, SECURITY INCIDENTS AND BREACHES

a. Use or Disclosure Not Permitted by This Agreement: Business Associate will report in writing to Covered Entity any Use or Disclosure of PHI for purposes other than those permitted by this Agreement within 5 business days of Business Associate's learning of such Use or Disclosure.

b. Security Incidents: Business Associate will report in writing to Covered Entity any Security Incident of which Business Associate becomes aware. Specifically, Business Associate will report to Covered Entity any successful unauthorized access, Use, Disclosure, modification, or destruction of ePHI or interference with system operations in an information system containing ePHI of which Business Associate becomes aware within 5 five business days of Business Associate learning of such Security Incident. Business Associate also will report the aggregate number of unsuccessful, unauthorized attempts to access, Use, Disclose, modify, or destroy ePHI or interfere with system operations in an information system containing ePHI, of which Business Associate becomes aware, provided that: (i) such reports will be provided only as frequently as the parties mutually agree, but no more than once per month; and (ii) if the definition of "Security Incident" under the Security Standards is amended to remove the requirement for reporting "unsuccessful" attempts to Use, Disclose, modify or destroy ePHI, the portion of this Section 4 addressing the reporting of unsuccessful, unauthorized attempts will no longer apply as of the effective date of such amendment.

c. **Breaches of Unsecured PHI:** Business Associate will report in writing to Covered Entity any Breach of Unsecured Protected Health Information, as defined in the Breach Notification Regulations, within 5 business days of the date Business Associate learns of the incident giving rise to the Breach. Business Associate will provide such information to Covered Entity as required in the Breach Notification Regulations. Business Associate will reimburse Covered Entity for any reasonable expenses Covered Entity incurs in notifying Individuals of a Breach caused by Business Associate or Business Associate's subcontractors or agents, and for reasonable expenses Covered Entity incurs in mitigating harm to those Individuals. Business Associate also will defend, hold harmless and indemnify Covered Entity and its employees, agents, officers, directors, shareholders, members, contractors, parents, and subsidiary and affiliate entities, from and against any claims, losses, damages, liabilities, costs, expenses, penalties or obligations (including attorneys' fees), which the Covered Entity may incur due to a Breach caused by Business Associate or Business Associate's subcontractors or agents.

5. ACCESS TO PROTECTED HEALTH INFORMATION

a. **Covered Entity Access**: Within 5 business days of a request by Covered Entity for access to PHI, Business Associate will make requested PHI available to Covered Entity.

b. **Individual Access**: If an Individual makes a request for access directly to Business Associate, Business Associate will within 5 business days forward such request in writing to Covered Entity. Covered Entity will be responsible for making all determinations regarding the grant or denial of an Individual's request for PHI and Business Associate will make no such determinations. Only Covered Entity will release PHI to an Individual pursuant to such a request.

6. AMENDMENT OF PROTECTED HEALTH INFORMATION

a. **Covered Entity Request:** Within 5 business days of receiving a request from Covered Entity to amend an Individual's PHI, Business Associate will provide such information to Covered Entity for amendment. Alternatively, if Covered Entity's request includes specific information to be included in the PHI as an amendment, Business Associate will incorporate such amendment within 5 business days of receipt of the Covered Entity request.

b. **Individual Request:** If an Individual makes a request for amendment directly to Business Associate, Business Associate will within 5 business days forward such request in writing to Covered Entity. Covered Entity will be responsible

for making all determinations regarding amendments to PHI and Business Associate will make no such determinations.

7. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

a. Disclosure Records: Business Associate will keep a record of any Disclosure of PHI that Business Associate makes to its agents, subcontractors or other third parties, if Covered Entity is required to provide an accounting to Individuals of such Disclosures under 45 C.F.R. § 164.528. Business Associate will maintain its record of such Disclosures for six years from the termination of this Agreement.

b. Data Regarding Disclosures: For each Disclosure for which it is required to keep a record under paragraph 7(a), Business Associate will record and maintain the following information: (1) the date of Disclosure; (2) the name of the entity or person who received the PHI and the address of such entity or person, if known; (3) a description of the PHI Disclosed; and (4) a brief statement of the purpose of the Disclosure.

c. Provision to Covered Entity: Within 5 business days of receiving a notice from Covered Entity, Business Associate will provide to Covered Entity its Disclosure records.

d. Request by Individual: If an Individual requests an accounting of Disclosures directly from Business Associate, Business Associate will forward the request and its Disclosure record to Covered Entity within 5 business days of Business Associate's receipt of the Individual's request. Covered Entity will be responsible for preparing and delivering the accounting to the Individual. Business Associate will not provide an accounting of its Disclosures directly to any Individual.

8. ACCESS TO BOOKS AND RECORDS

a. Covered Entity Access: Business Associate will, within 5 business days of Covered Entity's written request, make available during normal business hours at Business Associate's offices, all records, books, agreements, policies and procedures relating to the Use or Disclosure of PHI for the purpose of allowing Covered Entity or its agents or auditors to determine Business Associate's compliance with this Agreement.

b. Government Access: Business Associate will make its internal practices, books and records on the Use and Disclosure of PHI available to the Secretary

of the Department of Health and Human Services to the extent required for determining compliance with the Privacy Standards, Security Standards, or Breach Notification Regulations. Notwithstanding this provision, no attorney-client, accountant-client or other legal privilege will be deemed waived by Business Associate or Covered Entity as a result of this Section.

9. TERMINATION

Covered Entity may terminate the Written Agreement, if any, and this Agreement upon written notice to Business Associate if Covered Entity determines that the Business Associate or its subcontractors or agents has breached a material term of this Agreement. Covered Entity will provide Business Associate with written notice of the breach of this Agreement and afford Business Associate the opportunity to cure the breach to the satisfaction of Covered Entity within 30 days of the date of such notice. If Business Associate or its subcontractors or agents fail to timely cure the breach, as determined by Covered Entity in its sole discretion, Covered Entity may terminate the Written Agreement, if any, and this Agreement.

10. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

a. Return or Destruction of PHI: Within 30 days of termination of this Agreement, Business Associate will return to Covered Entity all PHI that Business Associate or its subcontractors or agents maintain in any form or format. Alternatively, Business Associate may, upon Covered Entity's written consent, destroy all such PHI and provide written documentation of such destruction. Business Associate will be responsible for recovering any PHI from its subcontractors or agents, or documenting their destruction of such PHI, consistent with the terms of this Section.

b. Retention of PHI if Return or Destruction is Infeasible: If Business Associate believes that returning or destroying PHI at the termination of this Agreement is infeasible, it will provide written notice to Covered Entity within 30 days of the effective date of termination of this Agreement. Such notice will set forth the circumstances that Business Associate believes makes the return or destruction of PHI infeasible and the measures that Business Associate will take for assuring the continued confidentiality and security of the PHI. Covered Entity promptly will notify Business Associate of whether it agrees that the return or destruction of PHI is infeasible. If Covered Entity agrees that return or destruction of PHI is infeasible, Business Associate may keep the PHI but will extend all protections, limitations and restrictions of this Agreement to Business Associate's Use or Disclosure of PHI retained after termination of this Agreement and will limit further Uses or Disclosures

to those purposes that make the return or destruction of the PHI infeasible. Business Associate will also ensure that any such extended protections, limitations and restrictions apply to its subcontractors or agents for whom return or destruction of PHI is determined by Covered Entity to be infeasible. If Covered Entity does not agree that the return or destruction of PHI from Business Associate or its subcontractors or agents is infeasible, Covered Entity will provide Business Associate with written notice of its decision, and Business Associate and its subcontractors and agents will proceed with the return or destruction of the PHI pursuant to the terms of this Section within 30 days of the date of Covered Entity's notice.

11. RESTRICTIONS ON USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

If Covered Entity advises Business Associate of any changes in, or restrictions to, the permitted Use or Disclosure of PHI, Business Associate will restrict the Use or Disclosure of PHI consistent with the Covered Entity's instructions.

12. MITIGATION PROCEDURES

Business Associate will mitigate, to the maximum extent practicable, any deleterious effect from its or its subcontractors' or agents' Use or Disclosure of PHI in a manner that violates this Agreement.

13. OBLIGATIONS REGARDING BUSINESS ASSOCIATE PERSONNEL

Business Associate will inform all of its Workforce Members, subcontractors and agents ("Business Associate Personnel"), whose services may be used to satisfy Business Associate's obligations under the Written Agreement, if any, or this Agreement, of the Business Associate's obligations under this Agreement. Business Associate represents and warrants that the Business Associate Personnel are under legal obligation to Business Associate, by contract or otherwise, sufficient to enable Business Associate to fully comply with the provisions of this Agreement. Business Associate will maintain a system of sanctions for any Business Associate Personnel who violates this Agreement.

14. COMPLIANCE WITH HITECH ACT AND REGULATIONS

Business associate will comply with the requirements of Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Business Associate, and will comply with all regulations issued by the Department of Health and Human Services (HHS) to implement these referenced statutes, as of

the date by which Business Associate is required to comply with such referenced statutes and HHS regulations.

15. MISCELLANEOUS

a. COMPLIANCE WITH LAWS: The parties are required to comply with federal and state laws. If this Agreement must be amended to secure such compliance, the parties will meet in good faith to agree upon such amendments. If the parties cannot agree upon such amendments, then either party may terminate this Agreement upon 30 days' written notice to the other party.

b. CONSTRUCTION OF TERMS: The terms of this Agreement will be construed in light of any applicable interpretation or guidance on the Privacy Standards, Security Standards or Breach Notification Regulations issued by the Department of Health and Human Services.

c. NO THIRD PARTY BENEFICIARIES: Nothing in this Agreement will confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

d. NOTICES: All notices required under the Agreement will be given in writing and will be delivered by (1) personal service, (2) first class mail, or (3) messenger or courier. All notices shall be addressed and delivered to the contact designated in the signature block, or other address provided by the party from time to time in writing to the other party. Notices given by mail will be deemed for all purposes to have been given forty-eight hours after deposit with the United States Postal Service. Notices delivered by any other authorized means will be deemed to have been given upon actual delivery.

e. ENTIRE AGREEMENT: This Agreement constitutes the entire agreement between the parties with regard to the Privacy Standards, Security Standards and Breach Notification Regulations, there are no understandings or agreements relating to this Agreement that are not fully expressed in this Agreement and no change, waiver or discharge of obligations arising under this Agreement will be valid unless in writing and executed by the party against whom such change, waiver or discharge is sought to be enforced.

f. WRITTEN AGREEMENT: This Agreement will be considered an attachment to Written Agreement, if any, and is incorporated as though fully set forth within the Written Agreement. This Agreement will govern in the event of conflict or inconsistency with any provision of Written Agreement.

g. COUNTERPARTS AND SIGNATURE: This Agreement may be executed in two or more counterparts, each of which shall be deemed an original and when taken together shall constitute one agreement. Facsimile and electronic signatures shall be deemed to be original signatures for all purposes of this Agreement.

h. CHOICE OF LAW: Governing Law: The validity, construction and effect of this Agreement will be governed by the laws of the State of Arizona, without giving effect to that state's conflict of laws rules. Any Dispute will be resolved in a forum located in the State of Arizona.

BUSINESS ASSOCIATE	**COVERED ENTITY** **El Rio Santa Cruz Neighborhood Health Center**
By:_____	By:_____
Print Name:_____	Print Name: Mark Hodges
Title:_____	Title: Corporate Compliance Officer
Date: _____	Date: _____

Contacts for Notices under this Agreement:

Print Name:_____	Print Name: Mark Hodges
Title:_____	Title: Corporate Compliance Officer
Address: _____	Address: 839 W. Congress St. Tucson, Arizona 85745
_____	_____
_____	_____
Phone: _____	Phone: (520) 670-3830

Security Risk Analysis
Business Associate Agreement (BAA) Requirements

El Rio Community Health Center (ERCHC) may permit a business associate to create, receive, maintain, or transmit ePHI on ERCHC's behalf **only if** ERCHC obtains satisfactory assurances in accordance with HIPAA Security Rule §164.314(a), that the business associate will appropriately safeguard the information by entering into a Business Associate Agreement. To comply with HIPAA rules, ERCHC must also conduct a due diligence process with all business associates to include, but not limited to, obtaining the following HIPAA Security Rule safeguard assurances from each business associate:

1- During the last 12 months has your business been independently audited (i.e. via a security risk analysis) for the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI)?

	No		Yes

If yes, were any high level identified during your security risk analysis? Please explain:

_____

_____

_____

2- Does your business have written policies and procedures that address and comply with the HIPAA Breach Notification Rule and the Security Rule's administrative, technical, organizational and physical safeguard requirements?

	No		Yes

_____

_____

_____

3- Has your business implemented a HIPAA-compliant security awareness and training program and trained all employees?

	No		Yes

_____

_____

4- Does your business have IT services that meet HIPAA compliant security standards for protecting ePHI?

	No		Yes

_____

_____

_____ _____

Company Name **Date**

_____ _____

Signature **Please Print Name Here**

Definition of a Business Associate
§160.103 of title 45, Code of Federal Regulations

Business Associate means, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 Code of Federal Regulations § 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 Code of Federal Regulations), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business Associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.