Appendix B: Business Associate Agreement

I. Authority:

Pursuant to 45 C.F.R. § 164.502(e), the Indian Health Service (IHS), as a covered entity, is required to enter into an agreement with a "business associate," as defined by 45 C.F.R. § 160.103, under which the business associate must agree to appropriately safeguard Protected Health Information (PHI) that it will use and disclose when performing functions, activities or services pursuant to its contract with the IHS. By signing Contract No. _____ (Contract), _____ agrees that it is a Business Associate and will comply with the terms below, in addition to other applicable Contract terms and conditions, and applicable law, relating to the safekeeping, use, and disclosure of PHI. This Appendix comprises the Business Associate Agreement (Agreement).

II. Definitions:

The following terms shall have the same meaning as those terms in 45 C.F.R. Part 160 and Part 164, which are the federal regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended: Breach, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, PHI, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and Use.

A. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement shall mean _____.

B. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean the IHS.

C. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

D. Master Patient Index (MPI). The "Master Patient Index" or "MPI" is composed of a unique list of patients and a current list of medical centers where each patient has been seen. This enables the sharing of patient data between operationally and regionally diverse systems. Each record (or index entry) on the MPI contains a small amount of patient data used to identify individual entries.

The mission of the MPI is to uniquely identify a patient and to "link" that patient's data throughout the IHS facilities using the Integration Control Number (ICN). The MPI is the authoritative source of a patient's ICN, the enterprise-wide identifier for IHS facilities and the key to accessing a patient's record. The

accuracy of patient information and patient identification directly affects clinical, administrative, billing, and interdepartmental processes.

III. Obligations and Activities of Business Associate:

A. Compliance: Business Associate agrees not use or disclose PHI other than as authorized by the Agreement or as required by law. Business Associate acknowledges that it is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by the Agreement or required by law. Business Associate agrees that it will require all of its agents, employees, subsidiaries, and affiliates, to whom Business Associate provides PHI, or who create or receive PHI on behalf of Business Associate for Covered Entity, to comply with the HIPAA Rules and to enter into written agreements with Business Associate that provide the same restrictions, terms, and conditions as set forth in the Agreement.

B. Subcontractors: In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), which govern relations with subcontractors, Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, terms, and conditions that apply to Business Associate with respect to such PHI.

C. Safeguarding PHI: Business Associate shall develop and use appropriate procedural, physical, and electronic safeguards to protect against the use or disclosure of PHI in a manner not authorized by this Agreement or required by law. Business Associate will limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.

D. Safeguarding Electronic PHI: Business Associate agrees to use appropriate safeguards, as set forth in Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of electronic PHI other than as authorized by this Agreement or required by law.

E. Reporting Use or Disclosures Not Authorized By this Agreement or Required by Law: Business Associate agrees to report to Covered Entity any use or disclosure of PHI not authorized by this Agreement or required by law within thirty (30) days of discovering the use or disclosure, or any security incident of which it becomes aware. In addition, Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of the use, disclosure, or security incident.

F. Reporting of Breach: In accordance with the policy of the Department of Health and Human Services, Business Associate will report, within one hour of discovery, all suspected or confirmed breaches to Covered Entity.

G. Notification of Breach of Unsecured PHI: In addition to the above, Business Associate shall notify Covered Entity of a breach, as set forth in 45 C.F.R. § 164.410, of the security of any unsecured PHI that Business Associate received from, or created or received on behalf of, Covered Entity within thirty (30) calendar days after the discovery of the breach by Business Associate, its employees, officers, and/or other agents, unless notification is specifically excepted by 45 C.F.R. § 164.412.

1. Requirements of Notice. Such notice shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such breach; a brief description of the circumstances of the breach of security, including the date of the breach and the date of Business Associate's discovery of the breach; and the type of unsecured PHI involved in the breach. Business Associate agrees to provide any other available information that Covered Entity is required to include in notification to the individual under 45 §164.404(c). In the event notification is delayed, evidence demonstrating the necessity of the delay shall accompany the notification.

H. Individual Access to PHI: Business Associate shall maintain a designated record set for each individual for whom it maintains PHI. In accordance with an individual's right to access his or her PHI, Business Associate shall make available all PHI in the individual's designated record set to the individual to whom that information pertains, or, upon the request of the individual, to that individual's authorized representative, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524. Availability to access PHI shall be made within five (5) calendar days of receipt of a valid request.

I. Accounting of Disclosures: Business Associate shall maintain records of PHI received from, or created or received on behalf of, Covered Entity and shall document subsequent uses and disclosures of such information by Business Associate. Business Associate shall, within five (5) calendar days after receiving a request from Covered Entity, provide to Covered Entity such information as Covered Entity may require to fulfill its obligations to account for disclosures of PHI pursuant to 45 C.F.R. § 164.528.

J. Amendment of PHI: Business Associate shall, within five (5) calendar days of a request by Covered Entity, make PHI available to Covered Entity for Covered Entity to fulfill its obligations under 45 C.F.R. § 164.526 to amend PHI and shall, as directed by Covered Entity, within five (5) calendar days of receipt of such direction, incorporate any amendments into PHI held by Business Associate. In addition, Business Associate shall ensure incorporation of any such amendments into PHI held by its agents or subcontractors within ten (10) days of such direction, and shall notify Covered Entity within five (5) calendar days of when

those agents or subcontractors have completed the incorporation of the amendments. Business Associate shall forward to Covered Entity all requests to amend PHI that it receives directly from individuals within five (5) calendar days of its receipt of a request.

K. Carrying out Covered Entity's Obligations: To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s).

L. Disclosures for Verifying Compliance: Upon request, Business Associate shall permit access by the Secretary and Covered Entity during normal business hours to its facilities, books, records, accounts, and any other sources of information, including PHI and any agreements that it has with subcontractors, vendors, and/or other agents relating to the use and disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, for purposes of determining both Business Associate's and Covered Entity's compliance with the HIPAA Rules.

IV. Permitted Uses and Disclosures by Business Associate:

A. Business Associate shall not use or disclose PHI except to perform functions, activities, or services on behalf of Covered Entity as provided for in the Contract, this Agreement, the HIPAA Rules, or other applicable law.

B. Business Associate agrees that it may use or disclose PHI on behalf of Covered Entity only:

1. Upon obtaining the authorization of the individual to whom the PHI pertains;
2. For the purposes of treatment, payment or health care operations unless Covered Entity has agreed to a restriction pursuant to 45 C.F.R. § 164.520(b)(iv)(A) or 45 C.F.R. § 164.522; or
3. Without an authorization or consent, if in accordance with 45 C.F.R. § 164.510, 45 C.F.R. § 164.512, 45 C.F.R. § 164.514(e), 45 C.F.R. § 164.514(f), or 45 C.F.R. § 164.514(g).

C. Business Associate shall use and disclose PHI in compliance with each applicable requirement of 45 C.F.R. § 164.504(e), which section is fully incorporated herein.

D. Business Associate agrees to make uses, disclosures, and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures.

E. It is anticipated that Business Associate will have access to the MPI.

F. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.

1. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the 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 purposes 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.

V. Obligations of Covered Entity:

A. Covered Entity shall provide Business Associate with its Notice of Privacy Practices and any changes to the Notice.

B. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices under 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

C. Covered Entity shall notify Business Associate of any change in, or revocation of, the permission by an individual to use or disclose his or her PHI to the extent that such changes may affect Business Associate's use or disclosure of PHI.

D. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

E. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except as provided in Part IV, Subpart F, Section 1.

VI. Termination:

A. **Term:** The Term of this Agreement shall be effective as of the date Business Associate signs the underlying Contract and shall terminate when the Contract ends or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

B. **Termination for Cause:** Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate

has violated a material term of the Agreement and Business Associate has not ended the violation within the time specified by Covered Entity.

C. **Obligations of Business Associate Upon Termination:** Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to Covered Entity, or, if agreed to by Covered Entity, destroy, the remaining PHI that Business Associate does not need to continue its proper management and administration or to carry out its legal responsibilities;
3. Continue to use appropriate safeguards, in compliance with Subpart C of 45 C.F.R. Part 164, with respect to electronic PHI to prevent use or disclosure of electronic PHI, other than as provided for in this Part, for as long as Business Associate retains the PHI;
4. Not use or disclose PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out above, at Part IV, Subpart F, Section 1 of the Agreement which applied prior to termination;
5. Return to Covered Entity, or, if agreed to by Covered Entity, destroy, the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities; and
6. If Business Associate or its agent or subcontractor destroys any PHI, Business Associate will provide Covered Entity with documentation evidencing such destruction within thirty (30) days of completion of destruction.

D. **Survival:** The obligations of Business Associate under this Part shall survive the termination of this Agreement.

VII. <u>Indemnification:</u>

In the event Business Associate is investigated and/or becomes a party to a civil or criminal cause of action in any forum relating to its failure to comply with the HIPAA Rules, Business Associate shall reimburse Covered Entity all reasonable costs and expenses Covered Entity may incur relating to such investigation and/or cause of action, and will otherwise hold Covered Entity harmless for any and all reasonable costs and expenses relating to the foregoing.

VIII. <u>Miscellaneous:</u>

A. **Incorporation:** This Agreement is attached to and fully incorporated into the Contract.

B. **Notices:** All notices under this Agreement shall be provided by certified mailing, and shall require proof of date of receipt.

C. **Regulatory References:** A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

D. **Amendment:** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

E. **Interpretation:** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

F. **Successors and Assigns:** This Agreement shall be binding upon, inure to the benefit of and be enforceable by and against the Parties and their successors and assigns.

G. **Severability:** If a court of competent jurisdiction deems any provision of this Agreement unenforceable, such provision shall be severed from this Agreement and every other provision of the Agreement shall remain in full force and effect.