INDIAN HEALTH SERVICE

MASTER PATIENT INDEX, HEALTH INFORMATION EXCHANGE, PERSONAL HEALTH RECORD, AND RPMS DIRECT

MULTI-PURPOSE AGREEMENT

INTRODUCTION

The Multi-Purpose Agreement (MPA) is entered into by health programs operated by Indian tribes, tribal organizations and urban Indian organizations that are Covered Entities, (see, 45 CFR § 160.102), that desire to engage in electronic health information exchange as part of the Meaningful Use Incentive Program and eHealth Exchange using the Indian Health Service Health Information Exchange (IHS HIE). The MPA helps participants meet Privacy and Security laws and regulations requirements, as well as mutual responsibilities and expectations of all Members under this MPA. This MPA incorporates the requirements of the Inter-Connection Security Agreement, Business Associate Agreement, End User Agreement and the Data Use and Reciprocal Agreement (DURSA) for the Network.

ARTICLE I
Definitions

Section 1.01 Agreement. The term “Agreement” shall mean this document, the Multi-Purpose Agreement.

Section 1.02 Associated Software and Associated Hardware. The terms "Associated Software and Associated Hardware" mean the software and/or hardware required to access the IHS HIE, eHealth Exchange (Exchange), Personal Health Record (PHR), Master Patient Index (MPI), and Resource and Patient Management System DIRECT (RPMS DIRECT).

Section 1.03 Authorized User. The term "Authorized User" shall mean a person designated by Members to access the IHS HIE, eHealth Exchange, PHR, MPI, and RPMS DIRECT on behalf of that Member, including, but not limited to, an employee or a credentialed medical staff.

Section 1.04 Business Associate. The term "Business Associate" shall mean IHS when it performs or assists in the performance of the use or disclosure of PHI for the permitted purposes pursuant to this Agreement and on behalf of Members.

Section 1.05 Consolidated Clinical Document Architecture (CCDA). The term CCDA shall mean standard that provides a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents.

Section 1.06 Consumer Preferences. The term “Consumer Preferences” shall mean an application that provides Indian Health System users with a mechanism to update individual patient preferences, specifying “opt-in” or “opt-out” of having their data shared across the Exchange.

Section 1.07 Continuity of Care Document (CCD). The term “CCD” shall mean a document form that contains the clinical content using the HL7 ANSI standard format for the transmission and exchange of clinical content. CCD and successor formats are based on the Consolidated Clinical Document Architecture (CCDA).

Section 1.08 Designated Record Set. The term "Designated Record Set" shall mean a group of records maintained by Business Associate for a Covered Entity that is: (a) the medical records about Individuals maintained by or for a covered health care provider, or (b) used in whole or in part, by or for a Covered Entity to make decisions about Individuals. For these purposes, the term "record" means any item, collection, or grouping of information that includes Protected Health Information (PHI) and is maintained, collected, used, or disseminated by or for a Covered Entity.

Section 1.09 DHHS. The term "DHHS" shall mean the United States Department of Health and Human Services.

Section 1.10 eHealth Exchange (Exchange). The term "Exchange" shall mean a set of standards, services, and policies that enables secure health information exchange over the Internet. The IHS HIE will provide a foundation for the exchange of health information between participating Indian Health programs. The Exchange will broaden access across diverse entities across the country, helping to achieve the goals of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Section 1.11 Electronic Protected Health Information ("EPHI"). The term "Electronic Protected Health Information" and abbreviation EPHI shall mean PHI that is transmitted, stored, and/or exchanged by "electronic media" (as that term is defined at 45 CFR § 160.103) or that is maintained in any form of electronic media.

Section 1.12 Health Insurance Portability and Accountability Act ("HIPAA"). The acronym "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, all as amended.

Section 1.13 Indian Health Service Active Directory. The term "IHS Active Directory" shall mean the federal D1 domain of IHS.

Section 1.14 Indian Health Service Health Information Exchange ("IHS HIE"). The term "IHS HIE" shall mean an application that collects and stores patient health summary information in the form of a CCD or a successor format from the IHS Resource and Patient Management System (RPMS). The IHS HIE provides user access to summary medical record information from multiple Indian health facilities utilizing RPMS databases from across the country.

Section 1.15 Indian Health Service Personal Health Record ("IHS PHR"). The IHS PHR is a secure internet application that enables verified patients to view their clinical information and use this information to interact with their medical team.

Section 1.16 Indian Health System. The term "Indian Health System" shall mean the Indian Health Service and participating Tribal and Urban programs.

Section 1.17 Individual. The term "Individual" shall mean a person who is the subject of PHI as defined in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

Section 1.18 Master Patient Index (MPI). The term "MPI" shall mean an index that contains records for all the patients from all of the Indian Health System facilities participating in the MPI. Each facility record belongs to a Master Patient Index record, which is created by the MPI.

Section 1.19 Members. The term "Members" shall mean health programs operated by Indian tribes, tribal organizations and urban Indian organizations that are "Covered Entities" (as defined

at 45 CFR § 160.102) and use the Network to access and share PHI under the terms of this Agreement. Members include IHS to the extent it accesses and uses PHI in accordance with Article 4.

Section 1.20 Network. The term “Network” shall mean, collectively, the IHS HIE, eHealth Exchange, RPMS DIRECT, IHS MPI, and IHS PHR.

Section 1.21 Privacy and Security Rules. The term "Privacy and Security Rules" shall mean the Standards for Privacy and Security of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 CFR Parts 160 and 164, as amended.

Section 1.22 Protected Health Information ("PHI"). The term "Protected Health Information" and abbreviation "PHI" shall have the same meaning as the term "protected health information" at 45 CFR § 160.103, limited to the individually identifiable health information received by a Business Associate from or on behalf of a Covered Entity. This term shall include Electronic Protected Health Information. In this Agreement, PHI shall mean the written or electronic “Treatment” information stored by Members on the Network as more fully described in Section 3.01.

Section 1.23 Required by Law. The term "Required by Law" shall have the same meaning as the term "required by law" at 45 CFR § 164.103.

Section 1.24 RPMS DIRECT. The term “RPMS DIRECT” shall mean a secure, web-based messaging service, intended for the exchange of patients’ health information between healthcare providers and their patients and/or their personal representatives.

Section 1.25 Secretary. The term "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

Section 1.26 Security Incident. The term "Security Incident" shall have the same meaning as the term "security incident" at 45 CFR § 164.304 which means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Section 1.27 Treatment. The term "Treatment" shall have the same meaning as the term “treatment” at 45 CFR § 164.501 which means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an Individual; or the referral of an Individual for health care from one health care provider to another.

ARTICLE II
Recitals

Section 2.01 Purposes of Agreement.

(a) To establish binding standards for Members to participate in accessing and sharing data over the Network. The Network is organized to facilitate PHI access and sharing for Treatment in a manner that complies with all applicable laws and regulations, including without limitation, those protecting the privacy and security of PHI.

(b) Members recognize the benefits in improved quality of patient care to be gained from the sharing of Individuals' PHI. Through the sharing of PHI for Treatment of patients who are seen by more than one Member, the Network may reduce the costs of care inefficiencies such as unnecessary repeat testing and may increase the accuracy of medical diagnoses through common and rapid access to PHI through electronic means, and lead to improved outcomes for patients.

(c) Members desire to store patients' PHI on the Network, allowing other Members access to such patients PHI in order to provide better informed Treatment.

Section 2.02 Authority. This Agreement is authorized by the Transfer Act, 42 U.S.C. § 2001 et seq.; the Snyder Act, 25 U.S.C. § 13; the Indian Health Care Improvement Act, 25 U.S.C. § 1601 et seq., (including but not limited to 25 U.S.C. § 1662, Automated Management Information System); the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d-2 and 1320d-4, and 45 C.F.R. § 164.506(c)(2).

Section 2.03 Consideration. Members agree to share its patients' PHI, for Treatment purposes, in consideration of receiving access to the other Members' patient PHI, for Treatment purposes. Members acknowledge that this consideration renders the Agreement legally binding among Members.

ARTICLE III
Member Obligations and Storage of Patients' PHI

Section 3.01 Storage of Patients' PHI.

(a) IHS will create and maintain the Master Patient Index (MPI). The MPI contains records for all patients from all of the Indian Health System facilities participating in the MPI. Each facility record belongs to an MPI record. Two facility records that represent the same real-life person belong to the same MPI record. An MPI record contains its own set of patient demographics called the Single Best Record, which is calculated from the demographics data of its facility records. The MPI generates a unique patient identifier

(ID) for each MPI record. The MPI enables the IHS Health Information Exchange (IHS HIE).

(b) As soon as reasonably practicable after the execution of this Agreement, to the extent allowed by applicable law, Members shall submit their patients' data, MPI demographic data, and patient encounter data for incorporation into the Network.

Section 3.02 General Exchange Principles.

(a) Members shall have processes in place to provide accurate and complete patient data that it provides to the IHS HIE.

(b) Data submitted by each Member shall not be used for any of the following purposes:

(1) Any use or disclosure not permitted by this Agreement;

(2) Conducting comparisons of the performance of other Members; or

(3) Any use that is prohibited by Federal law.

Section 3.03 Members' Representation Regarding Legality of Access.

(a) Members represent and warrant that it is authorized to allow Members access to PHI; provided that such access is made as described in this Agreement pursuant to HIPAA Privacy and Security Rules, all other applicable Federal and state laws, and/or pursuant to a duly executed authorization from any Individual to whom the PHI applies.

(b) To the best of each Member's knowledge, storing the CCD on the IHS HIE does not violate any rights, including copyrights, of third parties.

(c) If applicable Federal or state law requires Members to obtain an Individual's authorization or consent prior to submitting the patient's PHI for storage, or prior to allowing the other Members to access the PHI on the Network, the Member shall obtain any such consents or authorizations before submitting PHI to the Network and such consents or authorizations shall be broad enough to allow the uses and disclosures allowed by this Agreement. The Member shall provide a copy of any such consents or authorizations to IHS or other Member upon request. For example, an Individual's authorization is required for the use or disclosure of psychotherapy notes pursuant to 45 C.F.R. § 164.508(a)(2). Likewise, drug and alcohol abuse records must have an Individual's written consent pursuant to 45 C.F.R. Part 2.

ARTICLE IV
Members Access to PHI

Section 4.01 License. IHS grants Members, and each Member shall be deemed to have accepted, a non-exclusive, nontransferable, limited right to have access to and to use the Network, subject to the Member's full compliance with this Agreement. IHS retains all other rights to the Network and all the components thereof. Members shall not obtain any rights to the Network except for the limited rights to use the Network expressly granted by this Agreement.

Section 4.02 Permissible Uses of the Network by Members.

(a) Members may use the Network only for the permitted purposes described in this Agreement.

(b) Members may use the IHS HIE to share PHI with other Members for Treatment purposes.

(c) Members may use the IHS HIE to receive PHI submitted by other Members for Treatment purposes.

(d) Members may use RPMS DIRECT to exchange PHI with the Indian Health System RPMS DIRECT participants, other trusted DIRECT partners, and patients and/or their personal representatives with registered accounts.

(e) Members may use the IHS PHR to provide patients with access to personal health records in accordance with policies governing access and use of the IHS PHR.

(f) Members may use the IHS HIE to access the Exchange portal to view and share patient data for patient that have opted in with other Exchange partners. For the purpose of engaging in transactions through the Exchange, members shall be considered Participant Users under the Data Use and Reciprocal Support Agreement (DURSA) and shall comply with the terms and conditions applicable to participant users found in the DURSA or its successor. Members acting as Participant Users under the DURSA may Transact Message Content for Permitted Purposes only, including but not limited to Treatment.

(g) Members shall not use the Network for any purpose or in any manner that is prohibited by Federal law.

(h) Members shall not use the Network to aggregate data to compare the performance of other Members and/or Authorized Users.

Section 4.03 PHI Not Acquired from the Network. This Agreement does not apply to the use or disclosure of PHI that is in the possession of Members that was not acquired from the Network.

Section 4.04 Access to PHI By Members' Authorized Users. Members shall determine the Authorized Users under its control who may access the applicable Network services to retrieve PHI for the uses permitted by this Agreement. For users at Tribal and Urban facilities not on the IHS D1 domain, access to the Network services (PHR, RPMS DIRECT, HIE, and MPI) is granted only after processing of a Help Desk ticket for each individual service.

Member's Responsibility for Authorized Users. Members shall be solely responsible for all acts and omissions of the Member and/or its Authorized Users, with respect to the Network and/or any confidential or other information accessed and all such acts and omissions shall be deemed to be the acts and omissions of the Member. Members attest:

(a) Authorized Users have received training regarding the confidentiality of PHI under the HIPAA Privacy and Security Rules and all other applicable Federal or state laws and agree to protect the PHI in compliance with the HIPAA Privacy and Security Rules, such laws and this Agreement;

(b) Authorized Users shall only access the Network as approved by its Member;

(c) Authorized Users have agreed to protect all passwords, or other means for accessing the Network, in a confidential and secure manner and to not release them to another person or entity;

(d) Authorized Users agree and understand that its failure to comply with the terms of this Agreement may result in the Authorized Users' exclusion from the Network and may constitute cause for disciplinary action by the Member;

(e) Members restrict access to the Network only to the Authorized Users that Members have identified pursuant to this Article.

Section 4.05 Treatment. Without limiting any other provision of this Agreement, Members and its Authorized Users shall be solely responsible for all decisions and actions taken or not taken involving Treatment for respective Individuals resulting from or in any way related to the use of the Network or the PHI made available thereby.

Section 4.06 Acknowledgements Related to Access and PHI.

(a) The IHS HIE uses available technology (MPI) to match Individual identities with their records in the IHS HIE to provide Members with an Individual's PHI. Because such

records are maintained in multiple places, it is possible that false matches or a failure to match may occur or that there may be errors or omissions in the PHI provided to Members. To that end, it is incumbent upon Members to verify the Individual's PHI with each Individual before the PHI is relied upon in treating or diagnosing the Individual. The IHS does not independently verify or review the PHI transmitted through the IHS HIE for accuracy or completeness.

(b) Members acknowledge and agree that the Associated Software is an information management tool only. Members further acknowledge and agree that IHS has not represented that its services have the ability to diagnose disease, prescribe Treatment, or perform any other tasks that constitute the practice of medicine or other health professions.

(c) IHS does not independently verify or review the PHI transmitted through the IHS HIE for accuracy or completeness.

Section 4.07 Inaccurate Data. All data to which access is made through the Network and/or the Services originating from Members, and not from IHS (except when IHS also acts as a Member) is subject to change arising from numerous factors, including without limitation, changes to PHI made at the request of the Individual, changes in the Individual's health condition, the passage of time and other factors.

Section 4.08 Compliance with IHS Policies and Procedures. Members agree to comply with certain Indian Health Service policies and procedures governing access and use of the Network. The policies and procedures are listed in Addendum A to this Agreement and may be found at the IHS website. Members acknowledge that these policies and procedures may be revised periodically and Addendum A may be revised unilaterally by IHS to reflect such changes. Members further acknowledge that IHS may create new policies and procedures applicable to the use and access of the Network and that Addendum A may be revised unilaterally by IHS to add such policies and statements. Notification of any revisions of current policies or the creation of new policies will be made no later than 30 days before their effective date of implementation. If Members object to such revisions or new policies and will not abide by their terms, it must so notify IHS and withdraw from this Agreement on or before the effective date of implementation. If Members fail to object within the required time, they are deemed to have waived any objection.

ARTICLE V
Confidentiality and Security

Section 5.01 Confidentiality. Members agree that any PHI obtained from the Network will be kept confidential pursuant to the HIPAA Privacy and Security Rules and all other applicable Federal or state laws, statutes and regulations, as well as Members' own rules and regulations

governing the confidentiality of an Individual's records and information. Any hard copy or electronic copy of PHI acquired from the Network for Treatment purposes by a Member will be placed in the Individual's medical record that is maintained by the Member. Notwithstanding the foregoing, PHI that is acquired from the Network for Treatment purposes shall become a part of Member's medical record for that Individual, and consequently, if such PHI is incorporated into such record, other Members shall no longer have the right to control further downstream uses or disclosures of such PHI.

Section 5.02 Privacy Act. Members acknowledge that records incorporated into and maintained by IHS as part of the MPI are Federal records subject to the Privacy Act of 1974. Otherwise, records maintained by Members may be subject to the provisions of the Indian Self-Determination and Education Assistance Act (ISDEAA), including 25 U.S.C. § 450j(o) and deemed Federal records.

Section 5.03 Confidentiality Enforcement by Members. In addition to complying with HIPAA, Members agree to report any breach of the confidentiality of the PHI it becomes aware to the other Members, as permitted by law. Members agree to enforce the confidentiality provisions of this Agreement by appropriately disciplining persons within Member organizations who violate the confidentiality of the PHI pursuant to each Member's respective confidentiality and disciplinary policies. Such discipline may include, but not be limited to: warnings; suspensions; termination; or revocation of medical staff privileges.

Section 5.04 Access to Members' Organizational Confidential and Proprietary Information (Non-PHI). IHS agrees that it will not provide Members' confidential and/or proprietary information to any other Member, person, or entity, and will not publish any such information. Members shall be responsible for identifying whether information provided to IHS is Confidential and/or Proprietary Information.

Section 5.05 Security. Members shall implement security measures with respect to PHI obtained from the Network. These security measures shall comply with the HIPAA Privacy and Security Rules.

Section 5.06 Malicious Software, Viruses and Other Threats. Members must provide "malware" (including without limitation malicious software or malware, viruses, worms and Trojan Horses) protection on its environment and shall ensure that the connection to and use of the Network will not introduce any program, routine, subroutine, or data. Members will not disrupt the proper operation of the Network or any part thereof or any hardware or software used by IHS.

ARTICLE VI
Coordination of the Network

Section 6.01 IHS Role.

(a) IHS shall maintain and administer the Network. Members acknowledge and agree that access to the PHI contained therein shall be granted to IHS for all of its functions and obligations under this Agreement for the sole purpose of assisting IHS in its responsibilities. If IHS determines that the services of one or more contractors is necessary to fulfill some or all of IHS's obligations to the Network, IHS may use contractor(s), subject to applicable Federal law.

(b) By using the Network, Members shall acknowledge that other Members have access to the Network. All Members have agreed to comply with this Agreement; however, the actions of each Member are beyond the control of IHS. Accordingly, unless required by law or this Agreement, IHS does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on the Network resulting from any Member's actions or failures to act.

Section 6.02 Provision of Equipment, Software, and Training.

(a) IHS shall identify and may provide the software and/or hardware required to access the Network, as well as training to use the Associated Software. Members shall cooperate with IHS to install, implement, and maintain the Associated Software and Associated Hardware at Member location(s).

(b) Members shall not modify, reverse engineer, decompile, disassemble, re-engineer or otherwise create or permit or assist others to create the Associated Software or the Network, or to create any derivative works from the Associated Software or the Network. Members shall not modify the Associated Software or combine the Associated Software with any other software or services not provided or approved by IHS.

Section 6.03 Disclaimer of Warranties. To the extent allowed by law, IHS and Members disclaim any warranties, whether expressed or implied, which may be claimed regarding any of the equipment acquired by or supplied to Members. IHS and Members specifically expressly disclaim any implied warranties of merchantability and fitness for a particular purpose. IHS and Members shall take all reasonable steps to assure that manufacturers' and sellers' warranties may be enforced by Members, and shall cooperate with other Members in exercising warranty rights.

Section 6.04 Carrier Lines. By using the Network, Members shall acknowledge that access to the Network is to be provided over various facilities and communications lines, and information

will be transmitted over local exchange and internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and internet service providers, all of which are beyond IHS' control. IHS assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at Members' risk and is subject to all applicable local, state, and Federal laws.

Section 6.05 Use of Network Equipment. Members agree that any equipment associated with the Network, whether supplied by IHS or Members, shall not be used in any way that interferes with Network-based or security activity.

Section 6.06 Cooperation with IHS. Members agree to provide assistance to and cooperate with IHS with regard to the installation and maintenance of the software or equipment necessary to store PHI on and access the Network. Members agree to exercise reasonable care in the use of the equipment provided by IHS, and further agree to immediately notify IHS or its designee upon the malfunction of any of said equipment. Members agree to work with IHS Security for any incidents or vulnerability found in its environment.

ARTICLE VII
Interconnection Security Requirements

Section 7.01 Description of Interconnection. The interconnection between the IHS and Members is a two-way path subject to Members' and IHS' firewall filtering. Data exchanged will include Individual PHI. Data involved in the interconnection will include data from IHS, Tribal, and Urban Indian health programs. The interconnection will be used to provide an exchange of data among Members and IHS in accordance with the terms of this Agreement. Other services offered include but are not limited to "demilitarized zone" configuration, patch management, route configuration and management, filtering of traffic based on access control lists, active monitoring of traffic, spam filtering, malicious code prevention, bandwidth consumption management, and network admission controls.

Section 7.02 Data Sensitivity. Data shared under this Agreement will include unclassified but Sensitive, up to and including "High" level of sensitivity as defined by National Institute of Standards and Technology (NIST) SP800-60 Volume 2, section D.14.4 "Health Care Delivery Services Information type".

Section 7.03 User Community.

Users of the interconnection between Members and IHS include a variety of staff and business associates in the IHS, Tribal, and Urban Indian health programs. Users who are authorized by

Members and IHS may use this interconnection. These users include health care professionals in the IHS, Tribal, and Urban Indian health programs who have various levels of training and background clearances.

Technical users support the interconnection of the IHS, Tribal, and Urban Indian health programs by: maintaining infrastructure, ensuring security, providing management support, supporting communications and similar activities.

Section 7.04 Information Exchange Security Technical Controls.

IHS uses an encrypted virtual private network (VPN) tunnel for remote connections and data transfer. IHS uses network-based, passive intrusion detection systems to inspect all inbound and outbound network activity and identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IHS uses firewalls to control the ports, protocols, IPs leaving the boundary of the network. Members must use an encrypted LAN-to-LAN (L2L) VPN tunnel for remote connections and data transfer. Members must use firewalls to control the ports, protocols, IPs leaving the boundary of the Network. Members must use a VPN concentrator to authenticate internal users against Member's Active Directory. VPN security is set at the highest level for the highest risk data.

Section 7.05 Physical security controls at each end of the connection.

IHS systems are protected in accordance with federal mandates and NIST guidance. Servers are located within controlled access facilities.

Members' systems must be protected in accordance with applicable federal mandates and NIST guidance. Servers must be located within controlled access facilities.

Section 7.06 Logical access to information.

Users with access to Members' systems must not have access to the data except through their systems' security software inherent to the operating system. Access must be provided by a written approval process. Access must be controlled by authentication and role-based methods to validate the users' access.

Section 7.07 Trusted Behavior Expectations.

Members shall ensure that their employees, contractors, and other authorized users with access to the Network have passed or will have passed a criminal background check and adhere to organizational policies and procedures (including but not limited to Standard Operating Procedures (SOP) and Rules of Behavior prior to having access to the systems described in this Agreement.

All remote access users and contractors, and other authorized users that specifically require individual accounts on the IHS network to access resources shall request access from IHS in accordance with IHS procedure through the Information Technology Access Control (ITAC) system. The ROB must be signed upon initial access and annually thereafter for the duration of this Multi-Purpose Agreement. The ITAC request must be approved before initial access, and the ITAC request must be reviewed annually thereafter for the duration of this interconnection agreement.

Section 7.08 Formal Security Policy.

Policy documents that govern the protection of the data are the Indian Health Manual, Part 8, and the HHS Information Security Program Policy (see Addendum A).

Section 7.09 Incident Reporting.

Members and IHS shall report incidents in accordance with their own incident response procedures and, as applicable, with the incident reporting policies and procedures as outlined in Indian Health Manual, Part 8, Chapters 9 and 12 and IHS SOP 07-02, Incident and Event Reporting.

Section 7.10 Audit Trail Responsibilities.

All parties are responsible for auditing application processes and user activities involving the interconnection. Activities that shall be recorded include: event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers.

Members must maintain traffic logs of all authorized network traffic between Members and the Network for a minimum of thirty (30) days.

Section 7.11 Security Parameters.

Interconnections will be used to transmit data between Members and the Network via secured data streams for the purposes specified in this Agreement. If an exchange not covered by this Agreement is detected without prior appropriate approval, it must be refused, and documented as a possible intrusion until the interconnected service is authorized. Also, additional security parameters may be required (e.g., personal accountability) to allow the respondent system to determine whether a requestor is authorized to receive the information and/or services requested and whether all details of the transaction fall within the scope of user services authorized in this Agreement.

Section 7.12 Training and Awareness.

All IHS information system users are required to take security awareness training as a condition of receiving access and annually thereafter. There is no new/additional security awareness or training requirements as a result of the interconnection of the systems.

Members must: (i) ensure that its authorized users are made aware of the security risks associated with their activities and of the applicable laws related to the security of organizational information systems; and (ii) ensure that such authorized users are adequately trained to carry out their assigned information security-related duties and responsibilities upon initial granting of access and annually thereafter. All Members shall ensure that their employees, contractors, and other authorized users with access to the IHS network complete all required training and security awareness in accordance with their organizational policies and procedures, and this agreement.

Section 7.13 Security Documentation.

All IHS systems have been certified and accredited and have appropriate supporting documents, including Risk Assessment Reports and System Security Plans. All non-sensitive IHS security documentation is available upon request. The IHS Office of Information Technology (OIT) Division of Information Security has the responsibility for the security program.

Members may purchase commercial off-the-shelf (COTS) software and/or rely on custom software development for programming purposes. In such cases, Members must rely upon security documentation, certification and accreditation, if any, of such commercial vendors, consultants, or internal staff. Members are responsible for following IHS methods and procedures to connect or upload to IHS data systems.

ARTICLE VIII
HIPAA Business Associate Provisions Applicable to IHS

Section 8.01 Limits on Use and Disclosure.

(a) IHS may use and disclose PHI to maintain the Network and make disclosures to Members for Treatment purposes. IHS agrees to not use or further disclose PHI other than as permitted or required by this Agreement or as required by law.

(b) IHS shall not use or disclose PHI for any fundraising or marketing purposes. Further, IHS will not make the following disclosures that are otherwise allowed to be made by Members under 45 C.F.R. § 164.512 unless compelled to do so by law or unless such a disclosure is specifically authorized or required by this Agreement:

(1) About victims of abuse, neglect, or domestic violence;

(2) For health oversight activities;

(3) For judicial and administrative proceedings;

(4) For law enforcement purposes;

(5) About decedents;

(6) For cadaveric organ, eye, or tissue donation purposes;

(7) To avert a serious threat to health or safety;

(8) For specialized government functions; or

(9) For workers' compensation purposes.

If IHS is requested to make a disclosure for one of the foregoing reasons, it shall forward such request to the Member so that it can coordinate and prepare a timely response. IHS shall make PHI available to the Member for the foregoing reasons if requested to do so in writing by the Member.

Section 8.02 Safeguards. IHS agrees to use reasonable and appropriate administrative, physical and technological safeguards to prevent use or disclosure of the PHI other than as provided in this Agreement. IHS further agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains or transmits on behalf of Members. IHS agrees to use appropriate safeguards, as set forth in Subpart C of 45 C.F.R. Part 164 with respect to EPHI, to prevent use or disclosure of electronic PHI other than as authorized by this Agreement or required by law.

Section 8.03 Contractors. IHS shall ensure that any contractors hired pursuant to Section 6.01(a) agree in writing to the same restrictions and conditions that apply through this Agreement to the IHS. IHS shall require the contractors to implement reasonable and appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI that the contractors create, receive, maintain or transmit on behalf of Members.

Section 8.04 Access to Records. IHS shall provide reasonable access to PHI in a Designated Record Set in the IHS's possession to Members in order for a Member to meet the requirements under 45 CFR § 164.524 with regard to providing an Individual with a right to access their PHI. Prior to making a request to IHS under this Section, a Member shall make a good faith effort to gather the requested PHI from its own data sources that populate the Network. IHS shall not respond directly to requests from Individuals for access to their PHI in a Designated Record Set.

IHS will refer Individuals to the relevant Members so that Member can coordinate and prepare a timely response to the Individual.

Section 8.05 Reporting Use or Disclosures Not Authorized By this Agreement or Required by Law. IHS agrees to report to Members any security incident or use/disclosure of PHI not authorized by this Agreement or required by law within thirty (30) calendar days of discovering the use or disclosure. In addition, IHS shall mitigate, to the extent practicable, any harmful effect that is known to IHS of the use, disclosure, or security incident.

Section 8.06 Notification of a Breach of Unsecured PHI. In addition to the above, IHS shall notify Members of a breach, as set forth in 45 C.F.R. § 164.410, of any unsecured PHI that is received from, or created or received, on behalf of Members within thirty (30) calendar days after the discovery of the breach by IHS, its employees, officers, and/or other agents, unless notification is specifically excepted by 45 C.F.R. § 164.412.

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 IHS 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 IHS's discovery of the breach; and the type of unsecured PHI involved in the breach. IHS agrees to provide any other available information that Members are required to include in notification to the Individual under 45 CFR §164.404(c). In the event notification is delayed, evidence demonstrating the necessity of the delay shall accompany the notification.

Section 8.07 Amendments to PHI.

(a) IHS shall provide reasonable access to PHI in a Designated Record Set in IHS's possession to Members so it can make any amendments pursuant to 45 CFR § 164.526 or to otherwise allow Members to comply with its obligations under 45 CFR § 164.526. Amendments to PHI in the IHS HIE shall be made by Members to the IHS HIE through routine submissions of PHI via an electronic interface from a system operated by Members.

(b) IHS shall not respond directly to requests from Individuals for amendments to their PHI in a Designated Record Set. IHS will refer Individuals to relevant Members so that Member can coordinate and prepare a timely response to the Individual.

Section 8.08 Documentation and Provision of Disclosures.

(a) IHS shall promptly report to applicable Members any knowledge of uses or disclosures of PHI that are not in accordance with this Agreement or applicable law. In addition, IHS shall mitigate, to the extent practicable, any harmful effect that is known to IHS of a use

or disclosure of PHI by IHS in violation of the requirements of the HIPAA Privacy and Security Rules. IHS further agrees to report to Members, or designees, in writing, any physical or technical Security Incidents of which it becomes aware.

(b) IHS shall provide to a requesting Member, within a reasonable time period after the Member's request, information collected to permit the Member to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. However, IHS shall not respond directly to requests from an Individual for an accounting of disclosures. IHS will refer Individuals to relevant Members so that Member can coordinate and prepare a timely response to the Individual.

Section 8.09 Availability of Internal Practices, Books, Manuals, and Records. IHS shall make its internal practices, books, manuals, and records relating to the use and disclosure of PHI received from, or created or received by IHS on behalf of, Members available to the Secretary, in a reasonable time and manner designated by the Secretary, for purposes of determining a Member's compliance with the HIPAA Privacy and Security Rules.

Section 8.10 Change or Revocation of Permission. Members shall provide IHS with written notice of any changes in, or revocation of, permission by an Individual to use or disclose PHI, or of any restriction to the use or disclosure of PHI that Members have agreed to in accordance with 45 CFR § 164.522, if such changes or restrictions affect IHS's permitted or required uses and disclosures. IHS shall not be responsible for any use or disclosure that fails to comply with any such change or revocation that occurs prior to being notified by Members pursuant to this Section. Members shall not agree to restrict individual’s information from being used for treatment purposes.

Section 8.11 Notice of Privacy Practices. Members shall provide IHS with the Notice of Privacy Practices that Members produces in accordance with 45 CFR § 164.520, as well as any changes to such Notice. Members shall ensure that its Notice of Privacy Practices includes provisions that adequately inform Individuals: (a) that their PHI may be used and disclosed and received from other health care providers for Treatment purposes; and (b) that their PHI may be used and disclosed by IHS to perform functions allowed in this Agreement.

Section 8.12 Withdrawal. Notwithstanding any other provision, Members may withdraw from this Agreement in accordance with 45 C.F.R. § 164.314 if it determines that IHS, acting as a Business Associate, has violated a material term of this Agreement.

ARTICLE IX
Liability and Indemnifications

Section 9.01 Data. Except to the extent required by Federal law, IHS is not responsible for the content of any information transmitted or received through the Network.

Section 9.02 No Indemnification. No indemnification for any loss, claim, damage or liability is intended or provided by any Member under this Agreement. Members shall be liable for any loss, claim, damage, or liability that Members incur as a result of its activities under this Agreement, except that the IHS, as an agency of the United States, assumes liability only to the extent provided under the Federal Tort Claims Act, 28 U.S.C.§ 2671 et seq. This Section shall survive the termination of this Agreement and the withdrawal of any Member.

ARTICLE X
Addition of Subsequent Members

Section 10.01 Addition of New Members. Members acknowledge that additional Members may be added to the Network upon execution of this Multi-Purpose Agreement.

ARTICLE XI
Term and Termination

Section 11.01 Term of the Agreement. The term of this Agreement shall begin on _____, 20_____ and shall last for a term of one (1) year. This Agreement shall automatically renew unless a Member has provided written notice of its intent to withdraw, with or without cause, at least thirty (30) days in advance of termination. The withdrawal of any Member shall not be considered a termination of the Agreement and the remaining Members shall continue to participate under the terms of the Agreement.

Section 11.02 Use and Disclosure of PHI After Termination. When this Agreement terminates, IHS, at the Member's option, shall return or destroy all PHI in its possession, and keep no copies of PHI except as requested by the Member or required by law. Members shall notify IHS whether IHS must return or destroy any PHI in its possession. Members acknowledge that any data or file(s) covered by this Agreement and held by IHS, including PHI, may be subject to certain record retention requirements, including 36 CFR § 1228.100, making return or destruction infeasible. If IHS destroys any PHI, as permitted by law, then IHS will provide Members with documentation evidencing such destruction. Any PHI maintained by IHS shall continue to be extended the same protections set forth in this Agreement for as long as it is maintained.

Section 11.03 Use and Disclosure of PHI After Withdrawal. Upon a Member's withdrawal, the PHI stored by such Member will continue to be available for treatment purposes and all confidentiality provisions contained in this Agreement shall remain in force.

ARTICLE XII
Miscellaneous Provisions

Section 12.01 Governing Law. The scope, performance, validity, enforcement, and all other aspects of this Agreement shall be governed by Federal law.

Section 12.02 Multiple Counterparts. This Agreement is a multiparty contract that may be executed in multiple counterparts, each of which will be deemed an original, but all of which together will constitute one and the same.

Section 12.03 Incorporation By Reference. All addenda attached to this Agreement are incorporated by reference and made a part of this Agreement as if those exhibits were set forth at length in the text of this Agreement.

Section 12.04 Headings. Any subject headings used this Agreement are included for purposes of convenience only, and shall not affect the construction or interpretation of any of its provisions.

Section 12.05 No Succession and Assignment. This Agreement will be binding on and will inure to the benefit of Members. Members may not assign or transfer any rights or obligations under this Agreement.

Section 12.06 No Third Party Rights. This Agreement does not and will not create in any natural person, corporation, partnership, governmental entity, or other organization any benefits or rights, and this Agreement will be effective only as to Members.

Section 12.07 Compliance with Laws. Members to this Agreement intend and in good faith believe that this Agreement complies with all applicable Federal and state laws. If any provision of this Agreement is declared void by a court or arbitrator, or rendered invalid by any law or regulation, that portion shall be severed from this Agreement, and the remaining provisions shall remain in effect, unless the effect of the severance would substantially alter this Agreement or obligations of Members, in which case, Members agree to attempt in good faith to renegotiate the Agreement to comply with such law(s) to the satisfaction of all Members. In the event Members are not able to mutually agree to a new Agreement within thirty (30) days before the renewal date, then any affected Member may withdraw.

Section 12.08 Independent Entities. It is mutually understood and agreed that in performing their respective duties and obligations hereunder, Members are at all times acting as independent

Covered Entities with respect to each other. Nothing in this Agreement shall constitute or be construed to create a partnership or joint venture between or among Members.

Section 12.09 Regulatory References. A reference in this Agreement to a section in a Federal or State statute, law, or regulation means the section as in effect or as amended.

Section 12.10 Waiver of Breach. No failure or delay by any Member in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any breach shall constitute a waiver of any prior, concurrent, or subsequent breach.

Section 12.11 Force Majeure. No Member nor IHS shall be deemed in violation of any provision of this Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control. This Section shall not apply to obligations imposed under applicable laws and regulations.

Section 12.12 Complete Understanding. This Agreement shall contain the entire understanding of Members and/or IHS, and there are no other written or oral understandings or promises between Members and/or IHS with respect to the subject matter of this Agreement.

IN WITNESS WHEREOF, Members and IHS have executed this Agreement as of the dates indicated below.

INDIAN HEALTH SERVICE

By: _____
Signature

_____
Printed

_____
Title

_____
Date

Addendum A - Applicable Indian Health Service Policies and Procedures (see 4.08).

- IHS Policy Draft Part 8, Chapter XX.
- Data Use and Reciprocal Support Agreement (DURSA).
- IHS Policies: The General User Security Handbook/SOP 06-11a, IHS Technical and Managerial Handbook/SOP 06-11b and IHS Manual Part 8, Chapter 12.http://www.ihs.gov/IHM/index.cfm?module=dsp_ihm_pc_p8c12.