Department of Health Care Services
Integrated Systems of Care Division

Electronic Service Authorization (eSAR) Trading Partner Agreement

---

6/14/2017

TABLE OF CONTENTS

A Trading Partner Agreement (TPA) is a document required to be agreed upon by any entity, known as a Trading Partner, that is itself or through a subcontractor transmitting or receiving Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant ASC X12N 278 (005010X217) Transactions, hereby known as the electronic Service Authorization Requests (eSAR) system with the Department of Health Care Services (DHCS), Integrated Systems of Care Division (ISCD).

Please contact the CMS Net help desk if you have questions about the TPA:

Toll-Free Phone Number: (866) 685-8449

Local Telephone Number: (916) 617-5401

FAX Number: (916) 440-5346

Hours of Operation: Monday through Friday: 7:00 a.m. – 5:00 p.m.

Email address: CMSHelp@dhcs.ca.gov

1 GENERAL

This Agreement is between the Department of Health Care Services (DHCS), Integrated Systems of Care Division (ISCD) and the Trading Partner submitting an application (together the Parties" and individually a "Party"). ISCD is responsible for oversight and administration of the California Children's Services (CCS) and the Genetically Handicapped Persons Program (GHPP) programs.

The following Attachments are hereby incorporated in this Agreement as though fully set forth:

1. Attachment A: Transaction Set
2. Attachment B: Protection of Personally Identifiable Data and Information Assets

2 PURPOSE

A. This Agreement outlines the requirements for the transfer of electronic health care information, between the Trading Partner and the eSAR system. The transfer of this information is necessary for the Parties to perform testing functions. The information shall be transferred to and from the eSAR system. The Trading Partner and/or its subcontractors and vendors are in the business of submitting said electronic transactions on behalf of itself or issuer(s).

B. The transfer and sharing of information is for the purpose of allowing issuers and ISCD to transfer electronic transactions as described below in Attachment A with respect to clients of the CCS and GHPP programs. This Agreement provides for the transfer and exchange of information necessary for the processing of such transactions. These transactions shall comply with the applicable requirements of the American National Standards Institute (ANSI) accredited standards, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), 45 CFR Parts 160, 162, 164 and the HITECH Act, and the Final Omnibus Rule and Standards for Electronic Transactions, published in the Federal Register August 17, 2000, as modified by the U.S. Secretary of Health and Human Services (HHS) and the Patient Protection and Affordability Care Act (ACA) and its implementing regulations.

C. The Trading Partner is prohibited from transferring electronic health care information received from the eSAR system for any purpose not expressly permitted pursuant to this Agreement, or as required by law.

3 TERM

This Agreement shall continue in effect until terminated by either Party immediately upon written notice to the other Party or upon termination under Section VII, below. applicable), and Attachment B to this Agreement, contain the survival terms with the Parties that shall continue in effect after termination of this Agreement

4 DEFINITIONS

A. CCS-The California Children's Services program, a public health program which pays for the health care of children with specific medically eligible conditions.

B. DHCS– The Department of Health Care Services, doing business as a government entity in the State of California.

C. Health Insurance Portability and Accountability Act of 1996 (HIPAA)- The Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs; reduces health care fraud and abuse; mandates industry-wide standards for health care information on electronic billing and other processes; and requires the protection and confidential handling of protected health information.

D. eSAR– The electronic Service Authorization system, a service offering by DHCS/ISCD to accept electronic ASC X12N 278 (005010X217) transactions.

E. GHPP-The Genetically Handicapped Persons program, a public health program which pays for the health are of adults with specific genetic conditions.

F. ISCD – The Integrated Systems of Care Division (ISCD), the government entity which administers the CCS and GHPP programs in California.

G. Personally Identifiable Information (PII) – Any information that identifies or describes an individual, including, but not limited to, his or her name, social security number, home address, home telephone number, education, financial matters, medical or employment history, and statements made by, or attributed to, the individual. It also includes any identifiable information collected from or about an individual for purposes of determining eligibility and authorization of services for the CCS or GHPP programs.

H. Privacy Rule – "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

I. Protected Health Information (PHI) – Protected health information, including electronic protected health information, as defined in HIPAA that relates to an applicant or enrollee. Protected Health Information also includes medical

information as defined by the California Confidentiality of Medical Information Act (CMIA) at California Civil Code section 56, et seq.

J. Trading Partner Agreement (TPA) - A document required to be agreed upon by the Trading Partner, that is itself or through a subcontractor transmits or receives ASC X12N 278 (005010X217) Transactions.

K. Transactions and Code Set Regulations – mean those regulations governing the transmission of certain data transactions as published by the Department of Health and Human Services under

5 PROVISIONS OF THE AGREEMENT

A. All transactions must be formatted in accordance with the DHCS, CMS eSAR Companion Guide ASC X12N 278 (005010X217) Health Care Services Request for Review and Response 278, as applicable. ISCD shall provide the companion guide for the transactions, to specify certain situational data elements necessary for the eSAR system. HIPAA transactions to be transferred and shared between Trading Partner and eSAR system are identified in Attachment A, Transaction Sets of this Agreement.

B. The Trading Partner shall complete testing for each of the transactions it is required to implement and shall not transfer and share data with the eSAR system in production mode until testing is satisfactorily completed, as determined by ISCD.

1. Successful testing means the ability to successfully pass HIPAA compliance transaction tests, to submit requests for authorization of services transmitted by Trading Partner to the eSAR system and process the responses transmitted from the eSAR system back to the Trading Partner.

C. ISCD and the Trading Partner shall protect the client's information contained in the transfer of information by means of both physical and electronic security measures as required by Attachment B, included in this Agreement. Security measures shall include, at a minimum, the following requirements:

1. Each Party shall control access to its physical locations and devices so that only authorized personnel have access to the information transmitted in the transfer of information.

2. Each Party shall utilize passwords in accordance with established procedures so that only authorized personnel have knowledge of those passwords. Upon departure of personnel from employment, the Trading Partner shall promptly notify ISCD so that a new password can be established. ISCD shall establish a similar system for departure of its own employees;

3. Each Party shall report to the other any violation of security or the release of protected information that is not in accordance with this Agreement.

D. The following technical rules shall be used for the transfer of electronic client's information between the Parties:

1. The recommended delimiters for the inbound X12 transaction sets shall be:
    a. "*" Asterisk for data element separation;
    b. "^" Caret for sub-element separation;
    c. ":" Colon Component element separation; and d. "~" Tilde for segment terminator.

2. The delimiters for the outbound X12 transaction sets shall be:
    a. "*" Asterisk for data element separation;
    b. "^" Caret for sub-element separation;
    c. ":" Colon Component element separation; and d. "~" Tilde for segment terminator.

E. The production sign-on procedures once connected to the eSAR system shall be followed according to instructions issued by ISCD. All such instructions shall be provided in advance to Trading Partner with time for review and comment prior to implementation.

F. Use of Subcontractors. Trading Partner shall require any subcontractor, vendor or assignee to agree to be bound by all applicable provisions of this Agreement; provided however that nothing in this Section shall limit Trading Partner's ability to hold subcontractor liable for performance under the contract between Trading Partner and subcontractor. The obligation of Trading Partner to comply with responsibilities under this Agreement and applicable laws, rules and regulations shall remain and shall not be waived or released if Trading Partner subcontracts or otherwise delegates any obligations required to be performed by Trading Partner under this Agreement or by laws, rules or regulations or any other obligations under this Agreement. Trading Partner shall be solely responsible for (i) exercising appropriate diligence in connection with its selection of its subcontractors, and (ii) monitoring and auditing the services provided by such subcontractor to assure that the services provided by such subcontractors are provided in accordance with the terms set forth in this Agreement or imposed by applicable laws, rules and regulations regarding arrangements by and between Trading Partner and subcontractors.

6 AMENDMENT AND MODIFICATION

A. Except as otherwise provided herein, this Agreement may be modified or amended only by ISCD. The failure of either Party to insist upon strict performance of any provision of this Agreement shall not constitute a waiver of any subsequent default of the same or similar nature.

B. Modifications to transaction set formats used for client's information between the Trading Partner and ISCD shall require a mutually agreed upon update to Attachment A, and not an amendment to the Agreement.

7 TERMINATION

A. Either Party may terminate this Agreement without cause by providing the other Party with written notice.

B. The Agreement may be terminated immediately upon written notice if:

1. A Party fails to adhere to the prescribed and agreed upon formats;

2. It is determined that either Party is using information for purposes outside the scope of this Agreement.

8 CONFIDENTIALITY FOR PROPRIETARY INFORMATION

A. During the term of this Agreement and for a period of seven (7) years thereafter, each Party shall use the same means it uses to protect its own confidential proprietary information, but in any event not less than commercially reasonable means, to prevent the disclosure and to protect the confidentiality of both Parties' confidential proprietary information when:

1. Written information received from the other Party is marked or identified as confidential; or

2. Oral or visual information identified as confidential at the time of disclosure, which is summarized in writing and provided to the other Party in such written form promptly after such oral or visual disclosure ("Confidential Information").

B. The foregoing shall not prevent either Party from disclosing Confidential Information that belongs to such Party, is not prohibited from disclosure by a duty of confidentiality other than as set forth in this Agreement and is:

1. Already known by the recipient;

2. Publicly known or becomes publicly known through no unauthorized act of the Recipient Party;

3. Rightfully received from a third Party;

4. Independently developed by the recipient Party without use of the other Party's Confidential Information;

5. Disclosed without similar restrictions to a third Party by the Party owning Confidential Information;

6. Approved by the other Party for disclosure; or

7. Required to be disclosed pursuant to a requirement of a governmental agency or law so long as the disclosing Party provides the other Party with notice of such requirement prior to any such disclosure. Each Party represents and warrants that it has the right to disclose information that it has made and shall make available to the other hereunder.

9 MISCELLANEOUS

A. Administration of Agreement. ISCD may adopt policies, procedures, rules and interpretations that are consistent with applicable laws, rules and regulations and deemed advisable by CMS Net to promote orderly and efficient administration of this Agreement.

B. Days: Wherever in this Agreement a set number of days is stated or allowed for a particular event to occur, the days are understood to include all calendar days, including weekends and holidays, unless otherwise specified.

C. Force Majeure: Except as prohibited by applicable laws, rules and regulations, neither Party to this Agreement shall be in default of its obligations hereunder for delay or failure in performing that arises out of causes beyond the control and without the fault or negligence of either Party and arising from a catastrophic occurrence or natural disaster, such as Acts of God or of the public enemy, acts of the State in its sovereign capacity, acts of the State Controller's Office or other State agency having an impact on its ability to pay its obligations, acts of the State legislature, fires, floods, power failure, disabling strikes, epidemics, quarantine restrictions, and freight embargoes. However, each Party shall utilize its best good faith efforts to perform under this Agreement in the event of any such occurrence.

D. Binding Effect and Entire Agreement. This Agreement contains the entire understanding of the Parties, and there are no representations, warranties, covenants, or undertakings other than those set forth herein. Except as otherwise set forth herein, all the provisions of this Agreement shall be binding upon the respective successors in interest to the parties.

E. Governing Law: This Agreement shall be construed in accordance with and be governed by Federal and California State laws, rules, and regulations, regardless of the forum where it arises.

10 ATTACHMENT A – TRANSACTIONS SETS

The following transaction set is made part of this Trading Partner Agreement for eSAR transactions. All transactions are to be implemented in accordance with the HIPAA implementation guides. ISCD/CMS shall provide companion documents for each of the transactions that the Trading Partner will need. As additional transaction sets or operating rules are required to be implemented pursuant to HIPAA implementation guides, the Parties shall complete a new Attachment A indicating the transaction sets that are to be part of this Agreement.

- ASCX12N 278 (005010X217) Health Care Services Request for Review and Response

11 ATTACHMENT B – PROTECTION OF PERSONALLY IDENTIFIABLE DATA AND INFORMATION ASSETS

A. Privacy and Security Requirements for Personally Identifiable Data.

1. HIPAA Requirements. Trading Partner agrees to comply with applicable provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Administrative Simplification Provisions of HIPAA, as codified at 42 U.S.C. § 1320d et seq., the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), and any current and future regulations promulgated under HITECH or HIPAA, all as amended from time to time and collectively referred to herein as the "HIPAA Requirements". Trading Partner agrees not to use or further disclose any Protected Health Information (PHI), other than as permitted or required by the HIPAA Requirements and the terms of this Agreement. For purposes of this Agreement, ISCD represents that ISCD is a "health oversight entity", as that term is defined in HIPAA at 45 C.F.R. § 164.501 and, as such, Trading Partner, is permitted to disclose PHI to ISCD in its role as a health oversight entity.

2. California Requirements. With respect to all provisions of information under this Agreement, Trading Partner agrees to comply with all applicable California state health information privacy and security laws applicable to Personally Identifiable Information, including but not limited to the Confidentiality of Medical Information Act, the California Insurance Information and Privacy Protection Act, and the Information Practices Act, all collectively referred to as "California Requirements".

3. Interpretation. Notwithstanding any other provisions in this section, to the extent a conflict arises between the permissibility of a use or disclosure of Protected Health Information or Personally Identifiable Information under the HIPAA Requirements, ISCD Requirements, or California Requirements with respect to Trading Partner Exchange Functions, the applicable requirements imposing the more stringent privacy and security standards to such uses and disclosures shall apply. In addition, any ambiguity in this Agreement regarding the privacy and security of Protected Health

Information and/or Personally Identifiable Information shall be resolved to permit ISCD and Trading Partner to comply with the most stringent of the applicable privacy and security laws or regulations.

4. Trading Partner Exchange Function Obligations. The following obligations apply to Trading Partner Exchange Functions (and information related thereto):

    a. Uses and Disclosures. Pursuant to the terms of this Agreement, Trading Partner may receive from ISCD Protected Health Information and/or Personally Identifiable Information in connection with Trading Partner Exchange Functions that is protected under applicable Federal and State laws and regulations. Trading Partner shall not use or disclose such Protected Health Information or Personally Identifiable Information obtained in connection with Trading Partner Exchange Functions other than as is expressly permitted under ISCD Requirements and only to the extent necessary in performing functions under this Agreement to assist applicants with securing health insurance coverage.

    b. Fair Information Practices. Trading Partner shall implement reasonable and appropriate fair information practices to support the operations of ISCD that are consistent with ISCD Requirements and address, at a minimum:

        i. Individual Access. Trading Partner shall provide access to, and permit inspection and copying of Protected Health Information and Personally Identifiable Information in either an electronic or hard copy format as specified by the individual and as required by law, within thirty (30) calendar days of such request from the individual. If the Trading Partner is unable to provide access within the time required by this subsection, Trading Partner may have no more than thirty (30) additional calendar days to provide the requested access. If the Trading

Partner denies access, in whole or in part, the Trading Partner must provide a written denial within the time limits for providing access, which includes the basis for the denial and a statement of the individual's review rights, if applicable. In the event any individual requests access to Protected Health Information or Personally Identifiable Information maintained by ISCD directly from Trading Partner, Trading Partner shall within five (5) calendar days forward such request to ISCD and the relevant health plan as needed.

ii. Amendment. Trading Partner shall provide an individual with the right to request an amendment of inaccurate Protected Health Information and Personally Identifiable Information. Trading Partner shall respond to such individual within sixty (60) calendar days of such a request either by making the correction and informing the individual of such correction or notifying the individual in writing that the request was denied, which notice shall provide an explanation for the denial and explain that the individual may submit a statement of disagreement with the denial.

iii. Openness and Transparency. Trading Partner shall make available to individual's applicable policies, procedures, and technologies that directly affect such individuals and/or their Protected Health Information and Personally Identifiable Information.

iv. Choice. Trading Partner shall provide individuals with a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their Protected Health Information and Personally Identifiable Information.

v. Limitations. Trading Partner represents and warrants that all Protected Health Information and Personally Identifiable Information shall be collected, used, and/or disclosed under this Agreement only to the extent necessary to accomplish a specified purpose under the terms of this Agreement or as permitted by ISCD Requirements and never to discriminate inappropriately.

vi. Data Integrity. Trading Partner shall implement policies and procedures reasonably intended to ensure that Protected Health Information and Personally Identifiable Information in its possession is complete, accurate, and current, to the extent necessary for the Trading Partner's intended purposes, and has not been altered or destroyed in an unauthorized manner.

vii. Safeguards. Trading Partner shall have in place administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information and Personally Identifiable Information that it creates, receives, maintains or transmits pursuant to the Agreement and to prevent the use or disclosure of Protected Health Information and/or Personally Identifiable Information other than as provided for in this Agreement, or as required by law. In furtherance of compliance with such requirements, Trading Partner shall:

a. encrypt all Protected Health Information and/or Personally Identifiable Information that is in motion or at rest, including but not limited to data on portable media devices, using commercially reasonable means, consistent with applicable Federal and State laws, regulations and agency guidance, including but not limited to the U.S. Department of Health

and Human Services Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as Protected Health Information and/or Personally Identifiable Information. Data centers shall be encrypted or shall otherwise comply with industry data security best practices.

b. implement a contingency plan for responding to emergencies and/or disruptions to business that in any way affect the use, access, disclosure or other handling of Protected Health Information and/or Personally Identifiable Information;

c. maintain and exercise a plan to respond to internal and external security threats and violations;

d. maintain an incident response plan;

e. maintain technology policies and procedures that provide reasonable safeguards for the protection of Protected Health Information and Personally Identifiable Information stored, maintained or accessed on hardware and software utilized by Trading Partner and its subcontractors and agents;

f. mitigate to the extent practicable, any harmful effect that is known to Trading Partner of any Security Incident related to Protected Health Information and/or Personally Identifiable Information or of any use or disclosure of Protected Health Information and/or Personally Identifiable Information by Trading Partner or its subcontractors or agents in violation of the requirements of this Agreement or applicable privacy and security laws and regulations and agency guidance;

g. destroy Protected Health Information and Personally Identifiable Information in a manner consistent with applicable Federal and State laws, regulations, and agency guidance on the destruction of Protected Health Information and Personally Identifiable Information; and

h. comply with all applicable Exchange Protection of Information policies as specified in accordance with the terms and conditions set forth in this Agreement and in this Attachment B, including, but not limited to, executing non- disclosure agreements and other documents required by such policies. Trading Partner shall also require any subcontractors and agents to comply with all such Exchange Protection of Information policies.

viii. Breach Notification. (a) Trading Partner shall report to ISCD: (i) any use or disclosure of Protected Health Information and/or Personally Identifiable Information not permitted by this Agreement; (ii) any Security Incident involving Protected Health Information and/or Personally Identifiable Information created or received in connection with Trading Partner Exchange Functions; and/or (iii) any breach as defined in the HIPAA Requirements or California Requirements in connection with Protected Health Information and/or Personally Identifiable Information created or received in connection with Trading Partner Exchange Functions (each of which shall be referred to herein as a “Breach”). (b) Trading Partner shall, without unreasonable delay, but no later than within three (3) calendar days after Trading Partner’s discovery of a Breach, report such Breach to ISCD. In addition, Trading Partner shall, without unreasonable delay, but no later than within five (5) calendar days after Trading Partner's discovery of a successful Security Incident not involving Protected Health Information and/or Personally Identifiable Information, report such successful Security Incident not involving Protected Health Information and/or Personally Identifiable Information to ISCD. (c) Any such report will be made on a form made available to Trading Partner, or by such other reasonable means of reporting as may be communicated to Trading Partner by ISCD. (d) Trading Partner shall cooperate with ISCD in investigating the

Breach and/or successful Security Incident not involving Protected Health Information and/or Personally Identifiable Information and in meeting ISCD's obligations, if any, under applicable Federal and State security breach notification laws, regulatory obligations or agency requirements. If the cause of the Breach or the successful Security Incident not involving Protected Health Information and/or Personally Identifiable Information is attributable to Trading Partner or its agents or subcontractors, Trading Partner shall be responsible for Breach notifications and reporting as required under applicable Federal and State laws, regulations and agency guidance. Such notification(s) and required reporting shall be done in cooperation with ISCD. (e) To the extent possible, Trading Partner's initial report shall include: (i) the names of the individual(s) whose Protected Health Information and/or Personally Identifiable Information has been, or is reasonably believed by Trading Partner to have been accessed, acquired, used or disclosed or in the event of a successful Security Incident not involving Protected Health Information and/or Personally Identifiable Information, provide such information regarding the nature of the information system intrusion and any systems potentially compromised; (ii) a brief description of what happened including the date of the incident and the date of the discovery of the incident, if known; (iii) a description of the types of Protected Health Information and/or Personally Identifiable Information that were involved in the incident, as applicable; (iv) a brief description of what Trading Partner is doing or will be doing to investigate, to mitigate harm to the individual(s) and to its information systems, and to protect against recurrences; and (v) any other information that ISCD determines it needs to include in notifications to the individual(s) or relevant regulatory authorities under applicable privacy and security requirements. (f) After conducting its investigation, and within fifteen (15) calendar days, unless an extension is granted by ISCD, Trading Partner shall file a complete report with the information listed above, if available. Trading Partner shall make all reasonable efforts to obtain the information listed above and shall provide an explanation if any information cannot be obtained. Trading Partner and ISCD will cooperate in developing content for any public statements. (g) Trading Partner also shall, on at least a quarterly basis, report to ISCD the occurrence and nature of attempted but Unsuccessful Security Incidents (as defined herein).

"Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Trading Partner's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Protected Health Information and/or Personally Identifiable Information.

5. Other Obligations. The following additional obligations apply to Trading Partner:

a. Trading Partner's Subcontractors and Agents. Trading Partner shall enter into an agreement with any agent or subcontractor that will have access to Protected Health Information and/or Personally Identifiable Information that is received from, or created or received by, Trading Partner on behalf of ISCD or in connection with this Agreement, or any of its contracting Plans, pursuant to which such agent or subcontractor agrees to be bound by the same or more stringent restrictions, terms and conditions as those that apply to Trading Partner pursuant to this Agreement with respect to such Protected Health Information and Personally Identifiable Information.

b. Records and Audit. Trading Partner agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information and/or Personally Identifiable Information received from ISCD, or created or received by Trading Partner on behalf of ISCD or in connection with this Agreement available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining the Trading Partner's and/or ISCD's compliance with HIPAA Requirements. In addition, Trading Partner shall provide ISCD with information concerning its safeguards described throughout this Section and/or other information security practices as they pertain to the protection of Protected Health Information and Personally Identifiable Information, as the Exchange may from time to time request. Failure of Trading Partner to complete or to respond to ISCD's request for information within the reasonable timeframe specified by ISCD shall constitute a material breach of this Agreement. In the event of a Breach or Security Incident related to Protected Health Information and/or Personally Identifiable Information or any use or disclosure of Protected Health Information and/or Personally Identifiable Information by Trading Partner in violation of the requirements of this Agreement, ISCD will be permitted access to Trading Partner's

facilities in order to review policies, procedures and controls relating solely to compliance with the terms of this Agreement.

c. Electronic Transactions Rule. In conducting any electronic transaction that is subject to the Electronic Transactions Rule, Trading Partner agrees to comply with all applicable requirements of the Electronic Transactions Rule set forth in 45 C.F.R. § 162. Trading Partner agrees to require that any agent, including a subcontractor of Trading Partner that conducts standard transactions with Protected Health Information and/or Personally Identifiable Information of the Plan, comply with all applicable requirements of the Electronic Transactions Rule.

d. Minimum Necessary. Trading Partner agrees to request and use only the minimum necessary type and amount of Protected Health Information required to perform its services and will comply with any regulations promulgated under the HIPAA Requirements and agency guidance concerning the minimum necessary standard pertaining to Protected Health Information. Trading Partner will collect, use and disclose Personally Identifiable Information only to the extent necessary to accomplish a specified purpose under this Agreement.

e. Indemnification.

i. Trading Partner shall indemnify, hold harmless, and defend ISCD from and against any and all costs (including mailing, labor, administrative costs, vendor charges, and any other costs ISCD determines to be reasonable), losses, penalties, fines, and liabilities arising from or due to a Breach or other non-permitted use or disclosure of Protected Health Information and/or Personally Identifiable Information by Trading Partner or its subcontractors or agents, including without limitation, (1) damages resulting from any action under applicable (a) HIPAA Requirements, (b) ISCD Requirements or (c) California Requirements, and (2) the costs of ISCD actions taken to: (i) notify the affected individual(s) and other entities of and to respond to the Breach; (ii) mitigate harm to the affected individual(s); and (iii) respond to questions or requests for information about the Breach or other impermissible use or disclosure of Protected Health Information and/or Personally Identifiable Information.

ii. The obligation to provide indemnification under this Agreement shall be contingent upon ISCD:

a. providing Trading Partner with prompt reasonable written notice of any claim for which indemnification is sought,

b. allowing Trading Partner to control the defense and settlement of such claim; provided, however, that the Trading Partner consults with ISCD regarding the defense of the claim and any possible settlements and agrees not to enter into any settlement or compromise of any claim or action in a manner that admits fault or imposes any restrictions or obligations on ISCD without ISCD's prior written consent, which will not be unreasonably withheld; and,

c. cooperating fully with the Trading Partner in connection with such defense and settlement. Indemnification under this section is limited as described herein.

6. Notice of Privacy Practices. ISCD shall notify Trading Partner of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, other provisions within the HIPAA Requirements, or any other applicable Federal and State laws, regulations or agency guidance, to the extent that such limitation may affect Trading Partner's use or disclosure of Protected Health Information and/or Personally Identifiable Information.

7. Reporting Violations of Law. Trading Partner may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(2), other provisions within the HIPAA Requirements, or any other applicable state or federal laws or regulations.

8. Survival. Notwithstanding anything to the contrary in the Agreement, the provisions of this Attachment B on the Protection of Personally Identifiable Data and Information Assets shall survive termination of the Agreement with respect to information that relates to Trading Partner Exchange Functions until such time as all Personally Identifiable Information and Protected Health Information is destroyed by assuring that hard copy Personally Identifiable Information and Protected Health Information will

be shredded and electronic media will be cleared, purged, or destroyed consistent with National Institute of Standards and Technology Guidelines for Media Sanitization, or is returned to ISCD, in a manner that is reasonably acceptable to ISCD.

9. Contract Breach. Without limiting the rights of the parties pursuant to this Agreement, if Trading Partner breaches its obligations under this Agreement, ISCD may, at its option: (a) exercise any of its rights of access and inspection under this Agreement; (b) require Trading Partner to submit to a plan of monitoring and reporting, as ISCD may determine necessary to maintain compliance with this Agreement and such plan shall be made part of this Agreement; or (c) notwithstanding any other provisions of this Agreement, after giving Trading Partner opportunity to cure the breach, terminate this Agreement. If Trading Partner materially breaches its obligations under this Section, ISCD may terminate this Agreement, with or without opportunity to cure the breach. ISCD's remedies under this Section and any other part of this Agreement or provision of law shall be cumulative, and the exercise of any remedy shall not preclude the exercise of any other.

B. Protection of Information Assets

1. The following terms shall be given the meaning shown:

a. "Information Assets" means any information, including Confidential Information, necessary to the operation of either Party that is created, stored, transmitted, processed or managed on any hardware, software, network components, or any printed form or is communicated orally. "Information Assets" does not include information that has been transferred from the Disclosing Party to the Receiving Party under applicable laws, regulations and agency guidance, and that is being maintained and used by the Receiving Party solely for purposes that are not Trading Partner Exchange Functions.

b. "Confidential Information" includes, but is not limited, to any information (whether oral, written, visual or fixed in any tangible medium of expression), relating to either Party's services, operations, systems,

programs, inventions, techniques, suppliers, customers and prospective customers (excluding ISCD), cost and pricing data, trade secrets, know- how, processes, plans, reports, designs and any other information of or relating to the business or either Party, including Trading Partner's programs, but does not include information that (a) is described in the Evidence of Coverage booklets; (b) was known to the Receiving Party before it was disclosed to the Receiving Party by the Disclosing Party, (c) was or becomes available to the Receiving Party from a source other than the Disclosing Party, provided such fact is evidenced in writing and the source is not bound by a confidentiality obligation regarding such information to Disclosing Party, or (d) is developed by either Party independently of the other Party's Confidential Information, provided that such fact can be adequately documented.

c. "Disclosing Party" means the Party who sends Information Assets that it owns to the other Party for the purposes outlined in this Agreement.

d. "Receiving Party" means the Party who receives Information Assets owned by the other.

2. The Receiving Party shall hold all Information Assets of the Disclosing Party in confidence and will not use any of the Disclosing Party's Information Assets for any purpose, except as set forth in this Agreement, or as otherwise required by law, regulation or compulsory process.

3. The Receiving Party must take all reasonable and necessary steps to prevent the unauthorized disclosure, modification or destruction of the Disclosing Party's Information Assets. The Receiving Party must, at a minimum, use the same degree of care to protect the Disclosing Party's Information Assets that it uses to protect its own Information Assets.

4. The Receiving Party agrees not to disclose the Disclosing Party's Information Assets to anyone, except to employees or third parties who require access to the Information Assets pursuant to this Agreement, but only where such third parties have signed agreements regarding the Information Assets containing terms that are equivalent to, or stricter than, the terms of this Section, or as otherwise required by law.

5. In the event the Receiving Party is requested to disclose the Disclosing Party's Information Assets pursuant to a request under the California Public Records Act (PRA), a summons, subpoena or in connection with any litigation, or to comply with any law, regulation, ruling or government or public agency request, the Receiving Party shall, to the extent it may do so lawfully, give the Disclosing Party timely notice of such requested disclosure and afford the Disclosing Party the opportunity to review the request before Receiving Party discloses the Information Assets. The Disclosing Party shall, in accordance with applicable law, have the right to take such action as it reasonably believes may be necessary to protect the Information Assets, and such action shall not be restricted by the dispute resolution process of this Agreement. If such request is pursuant to the PRA, ISCD shall give Trading Partner sufficient notice to permit Trading Partner to consult with ISCD prior to disclosure of any Confidential Information. This subdivision shall not apply to restrict disclosure of any information to the State or in connection with a dispute between ISCD and Trading Partner or any audit or review conducted pursuant to this Agreement.

6. The Receiving Party shall notify the Disclosing Party in writing of any unauthorized disclosure, modification or destruction of the Disclosing Party's Information Assets by the Receiving Party, its officers, directors, employees, Trading Partners, agents or third parties. The Receiving Party shall make this notification promptly upon becoming aware of such disclosure, modification or destruction, but in any event, not later than four (4) calendar days after becoming aware of the unauthorized disclosure, modification or destruction. After such notification, the Receiving Party agrees to cooperate reasonably, at the Receiving Party's expense, with the Disclosing Party to remedy or limit the unauthorized disclosure, modification or destruction and/or its effects.

7. The Receiving Party understands and agrees the Disclosing Party may suffer immediate, irreparable harm in the event the Receiving Party fails to comply with any of its obligations under this Section, that monetary damages will be inadequate to compensate the Disclosing Party for such breach and that the Disclosing Party shall have the right to enforce this section by injunctive or other equitable remedies. The provisions of this Section shall survive the expiration or termination, for any reason, of this Agreement.

8. In the event of a conflict or inconsistency between the requirements of the various applicable sections of this Attachment B, Trading Partner shall comply with the provisions that provide the greatest protection against access, use or disclosure.

9. Survival. Notwithstanding anything to the contrary in the Agreement, the provisions of this Section II on Information Assets shall survive termination of the Agreement until such time as all Information Assets provided by ISCD to Trading Partner, or created, received or maintained by Trading Partner on behalf of ISCD, is destroyed by assuring that hard copy Information Assets will be shredded and electronic media will be cleared, purged, or destroyed consistent with National Institute of Standards and Technology Guidelines for Media Sanitization or is returned to ISCD, in a manner that is reasonably acceptable to ISCD.