HEALTH INFORMATION EXCHANGE ORGANIZATION PARTICIPATION AGREEMENT
BY AND BETWEEN
NORTH COAST HEALTH IMPROVEMENT AND INFORMATION NETWORK
AND
THE COUNTY OF HUMBOLDT

HEALTH INFORMATION ORGANIZATION	**PARTICIPANT**
Rosemary Den Ouden Chief Executive Officer North Coast Health Improvement and Information Network 2315 Dean Street Eureka, California 95501 Phone: (707) 443-4563 Email: rdenouden@nchiin.org	Humboldt County Department of Health and Human Services – Administration 507 F Street Eureka, California 95501 Phone: (707) 441-5400 Email: mstephens@co.humboldt.ca.us

INTRODUCTORY AND GENERAL PROVISIONS

This Health Information Exchange Organization Participation Agreement, by and between the North Coast Health Improvement and Information Network, a California nonprofit public benefit corporation, hereinafter referred to as "HIO," and the County of Humboldt, a political subdivision of the State of California, by and through its Department of Health and Human Services ("DHHS"), hereinafter referred to as "Participant," is made upon the following considerations:

Effective Date. The Effective Date of this Health Information Exchange Organization Participation Agreement ("Agreement") is April 1, 2022.

Term. This Agreement shall take effect on April 1, 2022 and shall remain in full force and effect until June 30, 2029, unless extended by a valid amendment hereto or sooner terminated as set forth in Section 2.1 (Termination of Participation Agreements) of the Terms and Conditions attached hereto. Each Project Addendum related hereto shall have the same end date as this Agreement regardless of its date of execution.

Nature of Organization. HIO is a California nonprofit public benefit corporation, organized to facilitate health information sharing and aggregation for treatment, payment, operations, public health and other lawful purposes in a manner that complies with all applicable laws and regulations, including, without limitation, those protecting the privacy and security of health information.

Exchanging Patient Data. From time to time, HIO may provide or arrange for the provision of data transmission and related services to allow Participants to search for and exchange Patient Data from a computer system that facilitates the sharing of Patient Data among disparate participants. HIO's services include establishing and applying standards for exchanging Patient Data.

Data Recipients and Providers. Participants in the Exchange include Data Recipients, who may be Health Care Providers, that will access Data through the Exchange and Data Providers that will provide Data through the Exchange. For purposes of this Agreement, Participant is both a Data Recipient and a Data Provider.

Description of Services. HIO provides, or arranges for the provision of, data transmission and related services to Participants to enable a Participant to send Patient Data to another Participant. HIO's services include establishing and applying standards for such exchange of Patient Data. HIO has access to and/or is responsible to maintain some or all of such Patient Data in the performance of HIO's services.

Maximum Amount Payable. The maximum amount payable by Participant for any and all costs and expenses incurred pursuant to the terms and conditions of any Project Addenda issued under this Agreement is Three Hundred Thousand Dollars ($300,000.00). HIO agrees to provide, or arrange for the provision of, any and all services required by any Project Addenda issued under this Agreement for an amount not to exceed such maximum dollar amount. However, if local, state or federal funding or allowance rates are reduced or eliminated, Participant may, by amendment, reduce the maximum amount payable hereunder or terminate this Agreement as provided in Section 2.1 (Termination of Participation Agreements) of the Terms and Conditions attached hereto.

Rate of Compensation. The specific rates and costs applicable to the services provided by HIO will be set forth in each Project Addendum issued under this Agreement.

Additional Services. Any Additional Services not otherwise set forth in any Project Addenda issued under this Agreement shall not be provided by HIO, or compensated by Participant, without Participant's prior written authorization. Any and all unauthorized costs and expenses incurred above the maximum payable amount set forth herein shall be the responsibility of HIO. HIO shall notify Participant, in writing, at least six (6) weeks prior to the date upon which HIO estimates that the maximum payable amount will be reached.

Payment. HIO shall submit to Participant semi-annual invoices itemizing any and all services provided, and costs and expenses incurred, pursuant to the terms and conditions of any Project Addenda issued under this Agreement. Invoices shall be in a format approved, and include any and all appropriate backup documentation as specified, by the DHHS Director and the Humboldt County Auditor-Controller. Payment for any and all costs and expenses incurred pursuant to the terms and conditions of any Project Addenda issued under this Agreement shall be made within thirty (30) days after the receipt of approved invoices. Any and all invoices submitted pursuant to the terms and conditions of this Agreement shall be sent to Participant at the following address:

COUNTY: Humboldt County DHHS – Administration
Attention: Financial Services
507 F Street
Eureka, California 95501

Complete Agreement. This Agreement includes, and incorporates by reference, all of the following terms, conditions and exhibits as well as any and all fully executed project addenda attached hereto:

Section 1 Development and Administration of Participation Agreements
Section 2 Termination of Participation Agreements
Section 3 Authorized Users
Section 4 General Obligations of Participants
Section 5 Data Recipient's Use of System and Services
Section 6 Data Provider's Use of System and Services
Section 7 Associated Hardware and Software to be Provided by HIO
Section 8 Privacy and Security of Patient Data
Section 9 Humboldt County Business Associate Agreement
Section 10 HIO's Operations and Responsibilities
Section 11 Governance
Section 12 Proprietary and Confidential Information
Section 13 Disclaimers, Exclusions of Warranties, Limitations of Liability
Section 14 Insurance and Indemnification
Section 15 Transparency, Oversight, Enforcement and Accountability
Section 16 Fees and Charges

Counterpart Execution. This Agreement, and any amendments hereto, may be executed in one (1) or more counterparts, each of which shall be deemed to be an original and all of which, when taken together, shall be deemed to be one (1) and the same agreement. This Agreement, and any amendments hereto, may be signed by manual or electronic signatures in accordance with any and all applicable local, state and federal laws, regulations and standards, and such signatures shall constitute original signatures for all purposes. A signed copy of this Agreement, and any amendments hereto, transmitted by email or by other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original executed copy of this Agreement and any amendments hereto.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates hereinafter indicated.

NORTH COAST HEALTH IMPROVEMENT AND INFORMATION NETWORK:

By: _____ Date: July 27, 2023

Name: Rosemary Den Ouden

Title: Chief Executive Officer

By: _____ Date: July 27, 2023

Name: Jessica Osborne-Stafsnes

Title: Chief Operating Officer

COUNTY OF HUMBOLDT:

By: Connie Beck _____ Date: 10-27-2023

Connie Beck, DHHS Director

(*Pursuant to the authority granted by the Humboldt County Board of Supervisors on October 24, 2023 [Item D-17]*)

INSURANCE AND INDEMNIFICATION REQUIREMENTS APPROVED:

By: Krista Freeman _____ Date: 9-21-2023

Risk Management

HEALTH INFORMATION EXCHANGE ORGANIZATION PARTICIPATION AGREEMENT TERMS AND CONDITIONS

SECTION 1
DEVELOPMENT AND ADMINISTRATION OF PARTICIPATION AGREEMENTS

1.1 Definitions. For the purposes of the Participation Agreement, the following terms shall have the meanings set forth below.

1.1.1 Additional Services. As used herein, the term "Additional Services" means data types, products and/or services not expressly described in this Agreement or any applicable Participation Agreement Addendums.

1.1.2 Associated Hardware. As used herein, the term "Associated Hardware" shall have the meaning described in Section 7.1 (Description of Associated Hardware and Associated Software) and if any, listed in Exhibit C (Associated Hardware and Associated Software).

1.1.3 Associated Software. As used herein, the term "Associated Software" shall have the meaning described in Section 7.1 (Description of Associated Hardware and Associated Software) and if any, listed in Exhibit C (Associated Hardware and Associated Software).

1.1.4 Authorized User. As used herein, the term "Authorized User" means an individual Participant or an individual designated to use the Services on behalf of the Participant, including, without limitation, an employee of the Participant and/or a credentialed member of the Participant's medical staff.

1.1.5 Breach of Privacy or Security. As used herein, the term "Breach of Privacy or Security" is a use or disclosure of Patient Data other than in compliance with these Terms and Conditions that either, (a) pursuant to applicable laws or regulations, must be reported to affected individuals and/or government officials, including, without limitation, federal or state data breach notification rules, or (b) adversely affects the viability of HIO, the trust among Participants or the legal liability of HIO or any Participant.

1.1.6 CMIA. As used herein, the abbreviation "CMIA" refers to the California Confidentiality of Medical Information Act, as codified at California Civil Code Sections 56, *et seq.*

1.1.7 Data Provider. As used herein, the term "Data Provider" means a Participant that is registered to provide information to HIO for use through the Services.

1.1.8 Data Recipient. As used herein, the term "Data Recipient" means a Participant that uses the Services to obtain health information.

1.1.9 Effective Date. As used herein, the term "Effective Date" means the Effective Date of these Terms and Conditions set forth in the Introductory and General Provisions of the Participation Agreement.

1.1.10 HIO. As used herein, the abbreviation "HIO" refers to North Coast Health Improvement and Information Exchange Network.

1.1.11 HIPAA. As used herein, the abbreviation "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996 and any and all regulations promulgated thereunder at Title 45 of the Code of Federal Regulations ("C.F.R.") Parts 160 and 164.

1.1.12 HITECH. As used herein, the abbreviation "HITECH" refers to the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009.

1.1.13 Medical Information. As used herein, the term "Medical Information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding an individual's medical history, mental or physical condition, or treatment, as defined by California Civil Code Section 56.05.

1.1.14 Other HIO. As used herein, the term "Other HIO" means a person or entity similarly situated to the HIO with which HIO has entered into a legally binding agreement pursuant to which HIO and that person or entity have agreed to arrange for their respective participants to share data through HIO's and the person's or entity's respective systems and services.

1.1.15 Participant. As used herein, the term "Participant" means a party that entered into a Participation Agreement with HIO to act as a Data Provider and/or as a Data Recipient.

1.1.16 Participant Type. As used herein, the term "Participant Type" means the category of Participant to which a particular Participant is assigned by HIO based upon that Participant's role in the health care system, as more specifically described in Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations).

1.1.17 Patient Data. As used herein, the term "Patient Data" means project specific information listed in any addenda to the Participation Agreement, including, without limitation, Protected Health Information, Personal Information, Personally Identifiable Information and Medical Information, that is provided, or made available for exchange, by a Data Provider through HIO's System and Services pursuant to Section 6.2 (Provision of Data).

1.1.18 Participation Agreement. As used herein, the term "Participation Agreement" means a legally binding agreement between HIO and a party pursuant to which that party acts as a Participant in accordance with, and agrees to comply with, these Terms and Conditions.

1.1.19 Personal Information. As used herein, the term "Personal Information" shall include, without limitation, any information that identifies or describes an individual, including, but not limited to, his or her physical description, home address, home telephone number, education, financial matters, medical or employment history and statements made by, or attributed, to the individual.

1.1.20 Personally Identifiable Information. As used herein, the term "Personally Identifiable Information" shall include, without limitation, any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, driver license number, identification card number, symbol or particular assigned to the individual, including, but not limited to, fingerprints, voice prints and photographs.

1.1.21 Policies, Procedures and Standards. As used herein, the term "Policies, Procedures and Standards" means, collectively, the policies, procedures and standards adopted by HIO pursuant to HIO's approved processes for the operation and use of the System and the Services, including, without limitation, the policies, procedures, standards and data security requirements set forth in Exhibit E (North Coast Health Improvement and Information Network Policy and Standards Manual) and Exhibit D (Data Security Requirements).

1.1.22 Protected Health Information. As used herein, the term "Protected Health Information" shall include, without limitation, individually identifiable health information that is transmitted by electronic media, maintained in electronic media or is transmitted or maintained in any other form or medium, as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information the Federal Security Standards contained in 45 C.F.R. Parts 160 and 164, all as may be amended from time to time.

1.1.23 Services. As used herein, the term "Services" means the health information exchange and related services for which the Participant registers pursuant to Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations) as described in Section 1.5.1 (Participation Agreement Required).

1.1.24 System. As used herein, the term "System" means the technology provided by HIO incident to HIO's performance of the Services.

1.1.25 Terms and Conditions. As used herein, the term "Terms and Conditions" means the terms and conditions set forth in this document that apply to a Participant and the HIO, respectively as amended, repealed, and/or replaced from time to time as described herein.

1.1.26 Unsecured Protected Health Information. As used herein, the term "Unsecured Protected Health Information" means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the United States Department of Health & Human Services through guidance issued pursuant to HITECH.

1.1.27 Unsuccessful Security Incident. As used herein, the term "Unsuccessful Security Incident" means a security incident (as defined under HIPAA) that does not result in: (1) the unauthorized access, use, disclosure, modification or destruction of information; or (2) material interference with system operations in a party's information system, including, without limitation, activity such as ping and other broadcast attacks on that party's firewall, port scans, unsuccessful log-on attempts, denial of service and/or any combination of the foregoing, so long as no such incident results in unauthorized access, use or disclosure of electronic protected health information.

1.2 Development and Dissemination of Terms and Conditions and Policies, Procedures and Standards. HIO is solely responsible for the development of these Terms and Conditions and the Policies, Procedures and Standards, and may amend, or repeal and replace, these Terms and Conditions and/or the Policies, Procedures and Standards as described in Section 1.4 (Changes to Terms and Conditions and/or Policies, Procedures and Standards).

1.3 Relationships Between Terms and Conditions and Policies, Procedures and Standards.

1.3.1 Incorporation of Policies, Procedures and Standards. The Policies, Procedures and Standards, in effect from time to time, are incorporated into these Terms and Conditions, and HIO and each Participant shall be required to comply with the applicable provisions of the Policies, Procedures and Standards as described in Section 1.5.5 (Effect of Terms and Conditions Upon Participation Agreements).

1.3.2 Other HIOs. HIO may exchange data with such Other HIOs that shall be identified in Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations), provided that such Other HIOs have agreed in their legally binding agreements with the HIO to:

(a) Comply with all laws applicable to the Other HIO, including, without limitation, the CMIA, HIPAA and HITECH, and to maintain and enforce appropriate Policies, Procedures and Standards in compliance therewith;

(b) Appropriately authenticate, in accordance with applicable industry standards, the identities and authorization of all the Other HIO's participants capable of exchanging data with or through or otherwise electronically interacting with the Other HIO's electronic systems;

(c) Promptly revoke or reduce, as appropriate, the access privileges of the Other HIO's participants who no longer have a need to electronically interact with the Other HIO's electronic systems in the manner or scope permitted by the privileges; and

(d) Comply with an appropriate indemnification provision regarding the Other HIO's act or omission related to the foregoing or receipt by an HIO of an inappropriate data request from or through Other HIO's systems.

1.4 Changes to Terms and Conditions and Policies, Procedures and Standards. Subject to Section 2.1 (Participant's Termination of Participation Agreement Based on Objection to Change) and Section 11 (Governance), HIO may amend, repeal and replace these Terms and Conditions and/or the Policies, Procedures and Standards at any time, and shall give Participants written notice of such changes not less than sixty (60) days prior to the implementation of those changes. However, if the change is required in order for HIO and/or Participants to comply with applicable laws or regulations, HIO may implement the change within a shorter period of time as HIO determines is appropriate under the circumstances. Any such change to these Terms and Conditions and/or Policies, Procedures and Standards shall automatically be incorporated by reference into each Participation Agreement, and be legally binding upon HIO and the Participant, as of the effective date of the change.

1.5 Development and Administration of Participation Agreements.

1.5.1 Participation Agreement Required. Only persons who enter into Participation Agreements with HIO shall be permitted to access the System and use the Services. A Participant may act as a Data Provider or as a Data Recipient, or as both, as described in Section 1.5 (Development and Administration of Participation Agreements). A Participant may use some or all of the Services, as specified in Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations) to that Participant's Participation Agreement after agreeing to the specific permitted uses, applicable standards and safeguards, and related terms.

1.5.2 Execution of Participation Agreements. A person may become a Participant by entering into a written Participation Agreement with HIO. Each such Participation Agreement shall describe:

(a) The Participant's Participant Type, as described in Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations);

(b) Whether the Participant is a Data Provider or a Data Recipient, or both;

(c) Which of the Services, Data Types and Projects the Participant may use; and

(d) Such other terms and conditions as HIO and the Participant shall agree.

/ / / /

1.5.3 Participant Type. Each Participation Agreement shall specify the Participant Type of the Participant, in accordance with the list of Participant Types set forth in Exhibit B (Participant Types, Data Types and Projects and Other Health Information Organizations).

1.5.4 Approval and Disapproval of Applications for Participation Agreements. Any party may apply to HIO to enter into a Participation Agreement, subject to the applicable terms of the Policies, Procedures and Standards. HIO shall review each application and shall approve or disapprove each in accordance with the Policies, Procedures and Standards and as HIO determines in its sole discretion is appropriate. HIO shall not be required to approve any application to be a Participant.

1.5.5 Effect of Terms and Conditions and Policies, Procedures and Standards Upon Participation Agreements. Each Participation Agreement shall incorporate by reference, and require that the Participant agree to comply with, these Terms and Conditions and the Policies, Procedures and Standards. HIO may make exceptions to this Section 1.5.5 (Effect of Terms and Conditions Upon Participation Agreements), provided that such exceptions, either individually or in the aggregate, do not materially reduce the obligations of the Participant to HIO or other Participants, or provide that the Participant is not subject to those provisions of these Terms and Conditions and the Policies, Procedures and Standards regarding the privacy and security of Patient Data.

1.5.6 Change or Termination of Services. HIO may cease to participate in any Other HIO, or may or may reduce the functionality, or make any other change to, the System and/or the Services, or may cease providing the Services, at any time upon the approval of the Management Committee and upon not less than ninety (90) days prior written notice to Participants.

SECTION 2
TERMINATION OF PARTICIPATION AGREEMENTS

2.1. Participant's Termination Based on Objection to Change. Notwithstanding Section 1.4 (Changes to Terms and Conditions and Policies, Procedures and Standards), the HIO shall not make any change to these Terms and Conditions and/or the Policies, Procedures and Standards that either (a) materially reduces the rights or increases the obligations of a Participant, (b) materially reduces the obligations of the HIO, or (c) substantially changes the provisions of the specific Terms and Conditions or Policies, Procedures and Standards regarding the privacy or security of Patient Data, without providing to the Participant the right to terminate its Participation Agreement by giving HIO written notice thereof not more than [thirty (30)] days following HIO's notice of the change. Such termination of a Participation Agreement shall be effective as of the effective date of the change to which the Participant objects; provided, however, that any change to these Terms and Conditions or the Policies, Procedures and Standards that HIO determines is required to comply with any federal, state, or local law or regulation shall take effect as of the effective date HIO determines is required, and the termination of any Participant's Participation Agreement based on the Participant's objection to the change shall be effective as of HIO's receipt of the Participant's notice of termination.

2.2 Participant's Termination Without Cause. A Participant may terminate its Participation Agreement at any time without cause by giving not less than ninety (90) days prior written notice to HIO.

2.3 Participant's Termination Upon Uncured Breach. Without limiting the obligations of HIO pursuant to Section 10.1 (HIO's Performance of Obligations, Generally), a Participant may terminate its Participation Agreement upon HIO's failure to perform a material responsibility

arising out of the Participant's Participation Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given HIO written notice of that failure and requested that HIO cure that failure.

2.4 Participant's Termination Upon Breach of Privacy or Security. A Participant may immediately terminate its Participation Agreement upon a Breach of Privacy or Security, as described in Section 8.3 (Reporting of Breaches and Security Incidents), when such Breach of Privacy or Security continues uncured for a period of sixty (60) days after the Participant has given HIO notice of that failure and requested that HIO cure that breach.

2.5 Participant's Termination Upon Breach of Business Associate Agreement. A Participant may immediately terminate its Participation Agreement based upon HIO's breach of Participant's Business Associate Agreement.

2.6 HIO's Termination Without Cause. Except as provided otherwise in the applicable Participation Agreement, HIO may terminate any Participant's Participation Agreement at any time without cause by giving not less than thirty (30) days prior **written** notice to the Participant provided, however, that HIO shall not terminate the Participation Agreement of any Participant without cause except incident to HIO's termination of the Participation Agreements of all Participants of the same Participant Type described in Exhibit B (Participant Types and Projects and Other Health Information Organizations).

2.7 HIO's Termination of Upon Uncured Breach. Without limiting the obligations of the Participant pursuant to Section 4.1 (Participant's Performance of Obligations, Generally), HIO may terminate any Participant's Participation Agreement upon the Participant's failure to perform a material responsibility arising out of the Participant's Participation Agreement, and that failure continues uncured for a period of sixty (60) days after HIO has given the Participant written notice of that failure and requested that the Participant cure that failure.

2.8 Effect of Termination. Upon any termination of a Participant's Participation Agreement, that party shall cease to be a Participant and thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services.

2.9 Survival of Provisions. The following provisions of these Terms and Conditions shall survive expiration or termination of a Participant's Participation Agreement: Section 3.5 (Responsibility for Conduct of Participant and Authorized Users), Section 8 (Privacy and Security of Patient Data), Section 9 (Humboldt County Business Associate Agreement), Section 12 (Proprietary and Confidential Information), Section 13.8 (Limitation on Liability) and Section 14.2 (Indemnification).

SECTION 3
AUTHORIZED USERS

3.1 Identification of Authorized Users. Each Participant shall adopt and implement a protocol for the selection and identification of that Participant's Authorized Users, and for those Authorized Users' use of the System and the Services, according to this Section 3.1 (Identification of Authorized Users) and Exhibit D (Data Security Requirements) a copy of which protocol shall be provided to HIO upon request. Such protocol shall comply with the requirements set forth in the Policies, Procedures and Standards, and shall describe, without limitation, the process by which the Participant shall uniquely identify each individual as an Authorized User prior to allowing that individual to use the System and the Services, the process by which the Participant shall verify the credentials of each Authorized User prior to enabling that Authorized User to use the System and the Services and the process by which

the Participant shall notify HIO of the removal of users from the Authorized User list. Each Participant shall comply with such protocol in all material respects.

3.2 Requirements of Authorized Users. At the time that a Participant identifies an Authorized User, the Participant shall require that the Authorized User:

(a) Has completed a training program conducted by Participant in accordance with Section 4.6 (Training);

(b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with HIO pursuant to Exhibit B (Participant Types and Projects and Other Health Information Organizations);

(c) Has agreed in writing not to disclose to any other person any passwords and/or other security measures issued to the Authorized User pursuant to Section 3.3 (Passwords and Other Security Mechanisms); and

(d) Has acknowledged in writing that his or her failure to comply with these Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant.

3.3 Passwords and Other Security Mechanisms. Based on the information provided by the Participant pursuant to Section 3.1 (Identification of Authorized Users) and Exhibit D (Data Security Requirements), HIO shall issue a user name and password or other security measure to each Authorized User that shall permit the Authorized User to access the System and use the Services. HIO shall provide each such user name and password or other security measure to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs HIO of the change, pursuant to Section 3.1 (Identification of Authorized Users), HIO shall cancel the user name and password or other security measure of such individual with respect to the Participant, and cancel and de-activate the user name and password or other security measure of such individual, if that individual is, as a result of the change, no longer an Authorized User.

3.4 No Use by Anyone Other than Authorized Users. The Participant shall restrict access to the System and, if applicable, use of the Services, only to the Authorized Users the Participant has identified to HIO in accordance with Section 3.1 (Identification of Authorized Users).

3.5 Responsibility for Conduct of Participant and Authorized Users. The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant's Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant's Authorized Users, with respect to the System, the Services and/or any confidential and/or other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant.

3.6 Termination of Authorized Users. The Participant shall require that all of its Authorized Users use the System and the Services only in accordance with these Terms and Conditions, including, without limitation, those governing the privacy and security of protected health information. The Participant shall appropriately discipline any Authorized User who fails to act in accordance with these Terms and Conditions in accordance with the Participant's disciplinary policies, procedures and standards.

SECTION 4
GENERAL OBLIGATIONS OF PARTICIPANTS

4.1 Participant's Performance of Obligations, Generally. The Participant shall, in accordance with the terms of its Participation Agreement, diligently perform all of its obligations arising under these Terms and Conditions and the Policies, Procedures and Standards and shall, promptly following written notice of any material breach thereof by HIO, cure such breach.

4.2 Compliance with Laws and Regulations. Without limiting any other provision of these Terms and Conditions relating to the parties' compliance with applicable laws and regulations, the Participant shall perform in all respects as contemplated by these Terms and Conditions in compliance with applicable federal, state, and local laws, ordinances and regulations.

4.3 System Security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Policies, Procedures and Standards, which is incorporated herein by reference.

4.4 Software and Hardware Provided by Participant. Except as provided in Section 7 (Associated Hardware and Software to be Provided by HIO), if applicable, each Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the Services, and provide to HIO all information required to be provided by the Participant ("Participant's Required Hardware and Software"). The Participant's Required Hardware and Software shall conform to HIO's then-current specifications, as set forth in the Policies, Procedures and Standards. As part of the Participant's obligation to provide Participant's Required Hardware and Software, the Participant shall be responsible for ensuring that all the Participant's computers to be used to interface with the System are properly configured, including, but not limited to, the operating system, web browser and Internet connectivity.

4.5 Malicious Software, Viruses, and Other Threats. The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including, without limitation, the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine or data, including, without limitation, malicious software or malware, viruses, worms, and Trojan Horses, which will disrupt the proper operation of the System or any part thereof or any hardware or software used by HIO in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by HIO or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

4.6 Training. The Participant shall provide appropriate and adequate training to all of the Participant's personnel, including, without limitation, Authorized Users, in the requirements of applicable laws and regulations governing the privacy and security of protected health information, including, without limitation, the requirements imposed under the CMIA, HIPAA and HITECH.

SECTION 5
DATA RECIPIENT'S USE OF SYSTEM AND SERVICES

If, pursuant to the applicable Participation Agreement, the Participant is a Data Recipient, the terms of this Section 5 (Data Recipient's Use of System and Services) shall apply to that Participant.

/ / / /

5.1 Grant of Rights to Use System and Services.

5.1.1 Grant by HIO. HIO grants to each Data Recipient, and each Data Recipient shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to, and use of, the System and the Services to be provided to that Data Recipient pursuant to the applicable Participation Agreement, subject to the Data Recipient's full compliance with these Terms and Conditions and the Data Recipient's Participation Agreement. HIO retains all other rights to the System and all the components thereof. No Data Recipient shall obtain any rights to the System except for the limited rights to use the System expressly granted by these Terms and Conditions.

5.1.2 Applicable Policies, Procedures and Standards. All issues concerning the ownership and rights in the System and the Services, and data and information obtained therefrom, shall be as set forth in the Policies, Procedures and Standards, which are incorporated herein by reference.

5.2 Permitted Purposes for Use of System and Services. A Data Recipient may use the System and the Services only to receive, locate or retrieve Patent Data for the purposes specified in its Participation Agreement. In no event shall a Data Recipient use the System and Services in any manner that is prohibited by any applicable local, state or federal laws, regulations, policies or standards.

5.3 Permitted Degree of Access to Patient Data. A Data Recipient shall use the System and the Services to request or seek access to only that amount of Patient Data that the Data Recipient is permitted to request pursuant to applicable laws and regulations.

5.4 Compliance with Applicable Laws. Without limiting the generality of Section 5.2 (Permitted Purposes for Use of System and Services), the Data Recipient shall in its use of the System and the Services comply with all applicable laws and regulations, including, without limitation, HIPAA and the CMIA.

5.5 Prohibited Uses of System and Services. A Data Recipient shall not use or permit the use of the System or the Services for any prohibited use described in the Policies, Procedures and Standards, which are incorporated herein by reference. Without limiting the generality of the foregoing, a Data Recipient shall not use or permit the use of the Services for any use or purpose described below:

5.5.1 No Services Prohibited by Law. The Data Recipient shall not use the System or the Services for which the Participant has registered for any purpose or in any manner that is prohibited by the laws of the State of California.

5.5.2 No Use for Comparative Studies. A Data Recipient shall not use the System or the Services to aggregate data to compare the performance of Participants and/or Authorized Users.

5.6 Permitted and Prohibited Uses and Disclosures of Patient Data. A Data Recipient may use and disclose Patient Data acquired through the use of the System and the Services as and to the extent permitted by law; provided, that the Participant shall not use or disclose Patient Data in any manner prohibited pursuant to Section 6.5 (Limitations on Use and Disclosure of Patient Data).

5.7 Effect of Expiration or Termination on Data Recipient. Upon any expiration or termination of a Data Recipient's Participation Agreement, the Data Recipient shall cease to be a Participant and thereafter shall have no right to, and shall not be permitted to, acquire Patient Data through the use of the System and the Services.

/ / / /

SECTION 6
DATA PROVIDER'S USE OF SYSTEM AND SERVICES

If, pursuant to the applicable Participation Agreement, the Participant is a Data Provider, the terms of this Section 6 (Data Providers' Use of System and Services) shall apply to that Participant.

6.1 Grant of Rights by HIO.

6.1.1 Grant by HIO. HIO grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to, and use of, the System for the purposes of complying with the obligations described in this Section 6 (Data Provider's Use of System and Services), subject to the Data Provider's full compliance with these Terms and Conditions and the Data Provider's Participation Agreement. HIO retains all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by these Terms and Conditions.

6.1.2 Applicable Policies, Procedures and Standards. All issues concerning the ownership and rights in HIO's System shall be as set forth in the Policies, Procedures and Standards, which are incorporated herein by reference.

6.2 Provision of Data. The Data Provider shall participate in and maintain its connection to the System's service-based network and provide through the System the Patient Data described in any and all addenda to the Participation Agreement as required for the Data Provider's Participant Type and data type Addendum of the Participant pursuant to Exhibit B (Participant Types and Projects and Other Health Information Organizations).

6.3 Measures to Assure Accuracy of Data. Each Data provider shall use reasonable care with respect to the accuracy and completeness of the Patient Data it provides through the System.

6.4 Grant of License to Use Patient Data. Subject to Section 6.5 (Limitations on Use and Disclosure of Patient Data), the Data Provider grants to HIO a perpetual, fully-paid, non-exclusive, royalty-free right and license to:

(a) License and/or otherwise permit others to access through the System and use all Patient Data provided by the Data Provider in accordance with the Policies, Procedures and Standards and these Terms and Conditions;

(b) Use such Patient Data to perform the Other Activities HIO performs pursuant to Section 10.9 (Other Activities); and

(c) Use such Patient Data to carry out HIO's duties under these Terms and Conditions, including, without limitation, system administration, testing, problem identification and resolution, management of the System, data aggregation activities as permitted by applicable state and federal laws and regulations, and otherwise as HIO determines is necessary and appropriate.

6.5 Limitations on Use and Disclosure of Patient Data. Notwithstanding Section 6.4 (Grant of License to Use Patient Data), Patient Data provided by a Data Provider shall not be used or disclosed for any purpose that is prohibited by the Policies, Procedures and Standards or any applicable laws or regulations.

/ / / /

6.6 Limitations on Data Provider's Provision of Patient Data. The Data Provider shall provide Patient Data only to the extent permitted by, and in accordance with the applicable requirements of, the Policies, Procedures and Standards, only to the extent permitted by applicable law and is the minimum necessary.

6.7 Effect of Expiration or Termination upon Data Provider. Upon any expiration or termination of a Data Provider's Participation Agreement, that Data Provider shall cease to be a Participant and thereupon and thereafter shall have no obligation to provide Patient Data through the System and the Services. Without limiting Section 9 (County of Humboldt HIPAA Business Associate Agreement), if and to the extent that HIO maintains any Patient Data on the Data Provider's behalf, HIO shall not, from and after the effective date of the expiration or termination of the Data Provider's Participation Agreement, provide or make that information available to Data Recipients, and thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services.

SECTION 7
ASSOCIATED HARDWARE AND SOFTWARE TO BE PROVIDED BY HIO

If, pursuant to the applicable Participation Agreement, the Participant has agreed to receive Associated Hardware and/or Associated Software from the HIO, the terms of this Section 7 (Associated Hardware and Software to be Provided by HIO) shall apply to that Participant.

7.1 Description of Associated Hardware and Associated Software. From time to time, HIO shall provide to the Participant the software and/or hardware required to access the System and use the Services the Participant has expressly agreed to receive in its Participation Agreement, as more particularly described in Exhibit C (Associated Hardware and Associated Software) when applicable. The Associated Software and Associated Hardware shall be provided in compliance with the specifications and/or service standards described on Exhibit C (Associated Hardware and Associated Software) when applicable.

7.2 Grant of License. HIO grants to the Participant a non-exclusive, personal, nontransferable, limited license to use the Associated Software and the Associated Hardware for access to, or use of, the System and, if the Participant is a Data Recipient, for the purpose of obtaining the Services.

7.3 Copying. The Participant may make one (1) copy of the whole or any part of the Associated Software in executable form for back-up or archival purposes; provided, that such copy must reproduce and include the copyright notice of HIO.

7.4 Modifications; Derivative Works. The Participant shall not modify, reverse engineer, decompile, disassemble, re-engineer or otherwise create or permit or assist others to create the Associated Software or the System otherwise, or to create any derivative works from the Associated Software or the System. The Participant shall not modify the Associated Software or combine the Associated Software with any other software or services not provided or approved by HIO.

7.5 Third-Party Software, Hardware, and/or Services.

7.5.1 Licenses, Subscription, and/or Other Agreements. The Associated Software includes certain third-party software, hardware, and services, which may be subject to separate licenses or subscription or other agreements or may require that a Participant enter into such agreements with third-party vendors. The Participant shall execute such agreements as may be required for the use of such software, hardware or services, and to comply with the terms of any applicable license or other agreement relating to third-party products included in Associated Software.

7.5.2 Standards and Warranties. The specifications, service standards and/or warranties to be provided by the vendor or vendors of the Associated Software and/or the Associated Hardware shall be described in the applicable agreements for those third-party products in the Addendum associated with the third-party product.

SECTION 8
PRIVACY AND SECURITY OF PATIENT DATA

8.1 Confidential Information.

8.1.1 Compliance with Applicable Laws and Regulations. HIO and each Participant agree to protect the confidentiality of all Patient Data transmitted pursuant to these Terms and Conditions in conformance with any and all applicable local, state and federal laws and regulations, including, but not limited to: California Welfare and Institutions Code Sections 827, 5328, 10850 and 14100.2; California Health & Safety Code Sections 1280.15 and 1280.18; the California Information Practices Act of 1977; the CMIA; HITECH; HIPAA; and any current and future implementing regulations promulgated thereunder, all as may be amended from time to time.

8.1.2 Continuing Compliance with Confidentiality Laws. HIO and each Participant acknowledge that local, state and federal laws, regulations, standards and contractual requirements pertaining to confidentiality, electronic data security and privacy are rapidly evolving and that amendment of these Terms and Conditions may be required to ensure compliance with such developments. HIO and each Participant agree to promptly enter into negotiations concerning an amendment to the Participation Agreement embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the CMIA and any other applicable local, state and federal laws, regulations, standards or contractual requirements.

8.2 Disclosure and Security Requirements.

8.2.1 Compliance with Applicable Laws and Regulations. HIO and each Participant shall comply with any and all local, state and federal privacy, security and confidentiality requirements applicable to the transmission of Patient Data pursuant to these Terms and Conditions, including, but not limited to, the Federal Privacy Regulations contained in 45 C.F.R. Parts 160 and 164, the Federal Security Standards contained in 45 C.F.R. Parts 160, 162 and 164 and the Federal Standards for Electronic Transactions contained in 45 C.F.R. Parts 160 and 162; 42 C.F.R. Sections 431.300, et seq.; and 45 C.F.R. Section 205.50, all as may be amended from time to time.

8.2.2 Compliance with Policies, Procedures and Standards. HIO and each Participant shall comply with any and all privacy, security and confidentiality requirements applicable to the transmission of Patient Data pursuant to these Terms and Conditions, including, without limitation, Protected Health Information, Personal Information, Personally Identifiable Information and Medical Information, set forth in the Policies, Procedures and Standards.

8.2.3 Disclosure of Patient Data.

8.2.3.1 Use and Disclosure of Patient Data. HIO and each Participant shall not use, store, disclose or access Patient Data transmitted pursuant to these Terms and Conditions in any manner that would constitute a breach of the Participation Agreement or a violation of any applicable local, state or federal laws, regulations, rules or standards.

8.2.3.2 Unauthorized Disclosures of Patient Data. Except as otherwise specifically permitted by these Terms and Conditions, HIO and each Participant shall not disclose Patient Data transmitted pursuant to these Terms and Conditions to any third-party, unless such disclosure is required by local, state or federal law.

8.2.3.3 Use of Patient Data. HIO and each Participant shall not use Patient Data transmitted pursuant to these Terms and Conditions for any purpose other than carrying out the duties and obligations set forth in the Participation Agreement.

8.2.3.4 Minimum Use and Disclosure of Patient Data. HIO and each Participant shall use or disclose only the minimum amount of Patient Data necessary to accomplish the intended purpose of the Participation Agreement.

8.2.3.5 Notification of Requests for Patient Data. HIO and each Participant shall promptly notify all interested parties of any and all requests for disclosure of Patient Data transmitted pursuant to these Terms and Conditions not emanating from a client, patient or person whose name or identifying information becomes available to HIO or the Participant pursuant to these Terms and Conditions.

8.2.3.6 Downloading Patient Data to Personal Devices. HIO and each Participant shall not download Patient Data to any personal device, including, but not limited to, flash drives, cell phones, iPads or tablets.

8.2.3.7 Maintenance and Preservation of Disclosure Records. HIO and each Participant shall timely prepare accurate and complete performance records relating to the use and disclosure of Patient Data transmitted pursuant to these Terms and Conditions, and to maintain and preserve said records for at least six (6) years from the date of expiration or termination of the Participation Agreement, except that if any litigation, claim, negotiation, audit or other action is pending, the records shall be retained until completion and resolution of all issues arising there from.

8.2.3.8 Availability of Disclosure Records. HIO and each Participant expressly agree to make its internal practices, books and records relating to the use and disclosure of Patient Data transmitted pursuant to these Terms and Conditions, available to any duly authorized public agency to the extent required for determining its compliance with any and all applicable local, state and federal laws and regulations. HIO and each Participant shall, within five (5) business day, provide to the other party copies of any such documentation.

8.2.3.9 Accounting Requirements. HIO and each Participant shall comply with the accounting requirements set forth in 45 C.F.R. Section 164.528 and any associated regulations or guidance issued by the United States Department of Health and Human Services – Office of Civil Rights, all as may be amended from time to time.

8.3 Breaches of Privacy and Security Incidents.

8.3.1 Identification and Mitigation of Security Incidents and Breaches of Patient Data. If HIO or a Participant has reason to believe that Patient Data may have been accessed, disclosed or acquired in breach of these Terms and Conditions, HIO or the Participant shall immediately take all actions necessary to preserve forensic evidence and to identify, mitigate and remediate the cause of the suspected breach or other security incident.

8.3.2 Reporting Breaches of Patient Data to Non-Breaching Parties. The breaching party shall notify all non-breaching parties, by telephone call and e-mail or fax, immediately after discovering a breach of Patient Data in electronic media or in any other media, if the Patient Data was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

8.3.3 Reporting Suspected Security Incidents to Non-Breaching Parties. The breaching party shall notify all non-breaching parties, by telephone call and e-mail or fax, within twenty-four (24) hours after discovering any other suspected security incident, intrusion, loss or unauthorized use or disclosure of Patient Data in violation of these Terms and Conditions, the Policies, Procedures and Standards or any applicable local, state or federal laws or regulations.

8.3.3.1 Discovery of Breaches and Security Incidents. For purposes of these Terms and Conditions, a breach of, or security incident involving, Patient Data shall be treated as discovered by the breaching party as of the first day on which such breach is known, or by exercising reasonable diligence would have been known, to the breaching party or any person, other than the person committing the suspected breach, who is an employee, officer or other agent of the breaching party.

8.3.4 Reporting Suspected Breaches and Security Incidents to Affected Individuals. To the extent deemed warranted, the breaching party shall provide notice to any and all individuals affected by a suspected breach of, or security incident involving, Patient Data. The breaching party shall be responsible for paying the full costs associated with notifying the affected individuals, which may include, but are not limited to, the costs to retain an outside consulting firm to undertake the notification effort. In addition, the breaching party shall consult with the non-breaching party regarding the steps required to notify the affected individuals and any other persons, media outlets or governmental agencies, and must supply the non-breaching party with the following information:

8.3.4.1 Description of Suspected Breach or Security Incident. A brief description of the circumstances surrounding the suspected breach of, or security incident involving, Patient Data, including, without limitation, the date of occurrence and discovery thereof, if known.

8.3.4.2 Description of the Information Involved. A description of the types of Patient Data that were involved in the suspected breach or security incident, including, but not limited to, the full name, date of birth and client identification number of all affected third parties.

8.3.4.3 Description of Remedial Actions. A brief description of the actions being taken by the breaching party to remediate the breach of, or security incident involving, Patient Data, mitigate losses and protect against any further breaches or security incidents.

8.3.5 Investigation of Suspected Breaches and Security Incidents. The breaching party shall immediately investigate any and all suspected breaches of, or security incidents involving, Patient Data. Within seventy-two (72) hours of the discovery of such suspected breach or security incident, the breaching party shall submit an updated "Privacy Incident Report" containing the applicable information to the extent known at that time.

8.3.6 Remediation of Breaches and Security Incidents. Upon discovery of a breach of, or security incident involving, Patient Data, the breaching party shall:

/ / / /

8.3.6.1 Corrective Action. Take prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment.

8.3.6.2 Legal Compliance. Take any action pertaining to such breach or security incident required by any and all applicable local, state and federal laws and regulations.

8.3.7 Cooperation with Remediation Efforts. Upon discovery of a breach of, or security incident involving, Patient Data, the breaching party shall give highest priority to immediately mitigating and remediating the breach or security incident, and shall devote such resources as may be required to accomplish that goal. In addition, the breaching party shall cooperate with the mitigation and remediation efforts of the non-breaching parties, including, without limitation, providing any and all information necessary to enable the non-breaching parties to fully understand the nature and scope of the breach or security incident, including, but not limited to, identification of each affected individual. In the event that the breaching party's assistance is required to reinstall software, such assistance shall be provided at no cost to the non-breaching parties in accordance with the non-breaching parties' policies and standards.

8.3.8 Remediation Report. The breaching party shall provide to the non-breaching parties a written report of the investigation of a breach of, or security incident involving, Patient Data within ten (10) business days of the discovery of such breach or security incident. The report shall include, without limitation, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to remediate and/or contain the breach or security incident.

8.3.9 Reporting Unsuccessful Security Incidents. The Participant shall provide, as required by the Policies, Procedures and Standards, an annual report to HIO which summarizes the nature and extent of any and all Unsuccessful Security Incidents involving Patient Data or the Participant's access or use of the System or the Services that occurred during the period covered by such report.

8.3.10 Reports to Participants. HIO shall provide monthly reports to all Participants which describes any and all breaches of, and security incidents involving, Patient Data which HIO becomes aware of during the prior month. HIO shall provide annual reports to all Participants summarizing any and all Unsuccessful Security Incidents reported by Participants to HIO pursuant to Section 8.3.9 (Reporting Unsuccessful Security Incidents) during the period covered by such report.

8.4 Safeguarding Patient Data. HIO and each Participant shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of all Patient Data transmitted pursuant to these Terms and Conditions. HIO and each Participant shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the nature, size and complexity of the relevant operations and activities, including, at a minimum, the safeguards set forth in Exhibit D (Data Security Requirements).

SECTION 9
HUMBOLDT COUNTY BUSINESS ASSOCIATE AGREEMENT

HIO shall execute and adhere to the terms and conditions set forth in the "County of Humboldt HIPAA Business Associate Agreement" which is attached hereto as Exhibit A (County of Humboldt HIPAA Business Associate Agreement) and incorporated herein by reference.

SECTION 10
HIO'S OPERATIONS AND RESPONSIBILITIES

10.1 Performance of Obligations, Generally. HIO shall, in accordance with the terms of the Participation Agreement, diligently perform all of its obligations arising under these Terms and Conditions and the Policies, Procedures and Standards and shall, promptly following notice from any Participant of a material breach thereof, cure that breach. Without limiting the generality of the foregoing, HIO shall perform all of its obligations arising under these Terms and Conditions and the Policies, Procedures and Standards in a manner that complies with all applicable laws and regulations.

10.2 Participation Agreements. HIO shall require that all Participants enter into a Participation Agreement or another legally binding agreement to comply with these Terms and Conditions in accordance with Section 1.5.5 (Effect of Terms and Conditions and Policies, Procedures and Standards Upon Participation Agreements). Without limiting Section 1.5.4 (Approval and Disapproval of Applications for Participation Agreements), HIO shall enter into Participation Agreements only with those parties that satisfy the requirements for participation set forth in the Policies, Procedures and Standards.

10.3 Monitoring of Participants. HIO shall regularly monitor Participant's compliance with the requirements for participation set forth in the Policies, Procedures and Standards.

10.4 Maintenance of System. HIO shall maintain the functionality of the System and the Services in accordance with the Policies, Procedures and Standards, and shall provide such service, security, and other updates as HIO determines are appropriate from time to time.

10.5 Training. HIO shall provide training to each Participant regarding the Participant's rights and obligations under its Participation Agreement and these Terms and Conditions, and the access and use of the System and Services, including such user manuals and other resources HIO determines appropriate to support the System and Services.

10.6 Telephone and/or E-Mail Support. HIO shall provide, by telephone and/or e-mail, during normal business hours, support and assistance in resolving difficulties in accessing and using the System and the Services.

10.7 Audits and Reports. HIO shall provide Participation Reports, Usage Reports, Public Agency Reports and Audit Trail Reports to each Participant as set forth in the Policies, Procedures and Standards.

10.8 Access to Patient Data. HIO shall permit access to Patient Data maintained by HIO only by Participants and other parties authorized by the Data Provider that provided such information, in a manner that complies with the Policies, Procedures and Standards.

10.9 Other Data Types and Projects. HIO shall add other data types, services, and/or projects from time to time by formally adding addendums specific to the services and data types.

SECTION 11
GOVERNANCE

11.1 Management Committee Composition. HIO shall create and maintain a Management Committee composed of HIO's Chief Executive Officer, HIO's Information Technology Manager and three (3) additional members selected by HIO's Board of Directors.

11.2 Meetings and Responsibilities of Management Committee. The Management Committee shall meet quarterly to consider and make recommendations to HIO's Board of Directors on various issues

pertaining to the use of the System and the Services by Participants, including, but not limited to, technical issues, privacy, information stored and accessed by Participants, use of information, and other issues including disputes related to the network or the parties' participation therein.

11.3 Management Committee Bylaws. The Management Committee shall adopt bylaws for the conduct of its meetings and other proceedings. Without limiting the generality of the foregoing, the Management Committee's bylaws shall provide procedures and rules concerning how the Management Committee shall call and conduct its meetings and take action.

11.4 Board of Directors Acting as the Management Committee. HIO's Board of Directors may assume the activities and responsibilities of the Management Committee.

SECTION 12
PROPRIETARY AND CONFIDENTIAL INFORMATION

12.1 Scope of Proprietary and Confidential Information. In the performance of their respective responsibilities pursuant to these Terms and Conditions, HIO and Participants may come into possession of certain Proprietary and Confidential Information of the other. For the purposes hereof, "Proprietary and Confidential Information" means all trade secrets, business plans, marketing plans, know-how, data, contracts, documents, scientific and medical concepts, member and customer lists, costs, financial information, profits and billings, and referral sources, existing or future services, products, operations, management, pricing, financial status, goals, strategies, objectives, and agreements of HIO or the Participant, as the case may be, whether written or verbal, that are confidential in nature; provided, however, that Proprietary and Confidential Information shall not include Patient Data or any other information that:

(a) Is in the public domain not as a result of a breach of these Terms and conditions, or any other confidentiality or nondisclosure agreement by any other party;

(b) Is already known or obtained by any other party other than in the course of the other party's performance pursuant to these Terms and Conditions, and without breach of any confidentiality, nondisclosure or other agreement by such other party;

(c) Is independently developed by any other party without causing a breach of these Terms and conditions or any other confidentiality or nondisclosure agreement by such other party; and/or

(d) Becomes known from an independent source having the right to disclose such information and without similar restrictions as to disclosure and use and without breach of these Terms and Conditions, or any other confidentiality or nondisclosure agreement by such other party.

12.2 Nondisclosure of Proprietary and Confidential Information. In the performance of their respective responsibilities pursuant to these Terms and Conditions, HIO and the Participant each shall:

(a) Keep and maintain in strict confidence all Proprietary and Confidential Information received from the other, or from any of the other's employees, accountants, attorneys, consultants, or other agents and representatives, in connection with the performance of their respective obligations under these Terms and Conditions;

(b) Not use, reproduce, distribute or disclose any such Proprietary and Confidential Information except as permitted by these Terms and Conditions; and

(c) Prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure.

12.3 Equitable Remedies. All Proprietary and Confidential Information represents a unique intellectual product of the party disclosing such Proprietary and Confidential Information (the "Disclosing Party"). The unauthorized disclosure of said Proprietary and Confidential Information would have a detrimental impact on the Disclosing Party. The damages resulting from said detrimental impact would be difficult to ascertain but would result in irreparable loss. It would require a multiplicity of actions at law and in equity in order to seek redress against the receiving party in the event of such an unauthorized disclosure. The Disclosing Party shall be entitled to equitable relief in preventing a breach of this Section 12 (Proprietary and Confidential Information) and such equitable relief is in addition to any other rights or remedies available to the Disclosing Party.

12.4 Notice of Disclosure. Notwithstanding any other provision hereof, nothing in this Section 12 (Proprietary and Confidential Information) shall prohibit or be deemed to prohibit a party hereto from disclosing any Proprietary and Confidential Information (or any other information the disclosure of which is otherwise prohibited hereunder) to the extent that such party becomes legally compelled to make such disclosure by reason of a subpoena, order of a court, administrative agency or other governmental body of competent jurisdiction or any applicable law or regulation, including, but limited to, the California Public Records Act and California Government Code Section 8546.7, and such disclosures are expressly permitted hereunder; provided, however, that a party that has been requested or becomes legally compelled to make a disclosure otherwise prohibited hereunder by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction shall provide the other party with notice thereof within five (5) calendar days, or, if sooner, at least three (3) business days before such disclosure will be made so that the other party may seek a protective order or other appropriate remedy. In no event shall a party be deemed to be liable hereunder for compliance with any such subpoena, order of any court, administrative agency or other governmental body of competent jurisdiction or applicable law or regulation.

SECTION 13
DISCLAIMERS, EXCLUSIONS OF WARRANTIES, LIMITATIONS OF LIABILITY

13.1 Carrier Lines. By using the System and the Services, each Participant shall acknowledge that access to the System 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 HIO's control. HIO 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 user's risk and is subject to all applicable local, state, national, and international laws.

13.2 No Warranties. Except as described in Exhibit C (Associated Hardware and Associated Software), or in an applicable third-party agreement described in Section 8.5.2 (Licenses, Subscriptions and/or Other Agreements), access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event

shall HIO be liable for any special, indirect, consequential, or exemplary damages, including, but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if HIO has been apprised of the possibility or likelihood of such damages occurring. HIO disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by third-party telecommunication service providers or the System.

13.3 Other Participants. By using the System and the Services, the Participant shall acknowledge that other Participants have access to the System and Services, and that other parties have access to the information contained in the System through their participation in an Other HIO. Such other Participants have agreed to comply with the Policies, Procedures and Standards, applicable data type addendum, concerning use of the information; however, the actions of such other parties are beyond the control of HIO. Accordingly, HIO 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 System resulting from any Participant's actions or failures to act.

13.4 Participant's Actions. The Participant shall be solely responsible for any damage to a computer system, loss of data, and any damage to the System caused by that Participant or any person using a user ID assigned to the Participant or a member of the Participant's workforce.

13.5 Unauthorized Access; Lost or Corrupt Data. HIO is not responsible for unauthorized access to the Participant's transmission facilities or equipment by individuals or entities using the System or for unauthorized access to, or alteration, theft, or destruction of the Participant's data files, programs, procedures, or information through the System, whether by accident, fraudulent means or devices, or any other method. The Participant is solely responsible for validating the accuracy of all output and reports and protecting the Participant's data and programs from loss by implementing appropriate security measures, including routine backup procedures. The Participant waives any damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, or the use of third-party software. HIO is not responsible for the content of any information transmitted or received through HIO's provision of the Services.

13.6 Inaccurate Data. All data to which access is made through the System and/or the Services originates from Data Providers and other parties making data available through one (1) or more Other Health Information Sharing Programs, and not from HIO. All such data is subject to change arising from numerous factors, including, without limitation, changes to patient health information made at the request of the patient, changes in the patient's health condition, the passage of time and other factors. HIO neither initiates the transmission of any data nor monitors the specific content of data being transmitted. Without limiting any other provision of these Terms and Conditions, HIO shall have no responsibility for or liability related to the accuracy, content, currency, completeness, content, or delivery of any data either provided by a Data Provider, or used by a Data Recipient, pursuant to these Terms and Conditions.

13.7 Patient Care. Without limiting any other provision of these Terms and Conditions, the Participant and the Participant's Authorized Users shall be solely responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients and clients resulting from, or in any way related to, the use of the System or the Services or the data made available thereby. No Participant or Authorized User shall have any recourse against, and through the Participation Agreements that apply thereto, each shall waive, any claim against HIO for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of the System and/or the Services or the data made available.

13.8 Limitation of Liability. Notwithstanding anything in these Terms and Conditions to the contrary, to the maximum extent permitted by applicable laws, the aggregate liability of HIO, and HIO's officers, directors, employees, and other agents, to any Participant with respect to the subject of these Terms and Conditions, regardless of theory of liability, shall be limited to the aggregate fees actually paid by the Participant in accordance with these Terms and Conditions for the six (6) month period preceding the event first giving rise to the claim.

SECTION 14
INSURANCE AND INDEMNIFICATION

14.1 Insurance. Without limiting the parties' indemnification obligations provided for herein, HIO and each Participant shall obtain and maintain insurance coverage in accordance with the Policies, Procedures and Standards. Without limiting the generality of the foregoing, HIO and each Participant shall comply with the insurance requirements representing the community standard for coverage.

14.2 Indemnification.

14.2.1 Indemnification, Generally. Nothing in these Terms and Conditions or any Participation Agreement shall limit HIO's or a Participant's respective legal and equitable obligations to each other and to other Participants arising out of the doctrines of equitable indemnity, comparative negligence, contribution or other common law bases of liability.

14.2.2 Specific Indemnities. Notwithstanding Section 14.2.1 (Indemnification, Generally), HIO and each Participant (each, an "Indemnifying Party") shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of any Breach of Privacy or Security arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees.

14.2.3 Rules for Indemnification. Any indemnification made pursuant to these Terms and Conditions shall include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys' fees and any settlement by or judgment against the party to be indemnified. In the event that a lawsuit is brought against the party to be indemnified, the party responsible to indemnify that party shall, at its sole cost and expense, defend the party to be indemnified, if the party to be indemnified demands indemnification by written notice given to the Indemnifying Party within a period of time wherein the Indemnifying Party is not prejudiced by lack of notice. Upon receipt of such notice, the Indemnifying Party shall have control of such litigation but may not settle such litigation without the express consent of the party to be indemnified, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third-parties, be a waiver of any defense or immunity otherwise available, and the Indemnifying Party, in indemnifying the Indemnified Party, shall be entitled to assert in any action every defense or immunity that the indemnified party could assert on its own behalf.

SECTION 15
TRANSPARENCY, OVERSIGHT, ENFORCEMENT AND ACCOUNTABILITY

15.1 Transparency. HIO shall develop, implement and conduct measures to provide Participants information concerning the ongoing operations of the System and the Services, including, without limitation, the efficiency, effectiveness, and security thereof, and the uses and disclosures of Patient Data made by and among Participants pursuant to their use thereof, as described in the Policies,

Procedures and Standards. Such measures shall include HIO's provision to Participants of the reports described in Section 8.3.10 (Reports to Participants).

15.2 Oversight. The Management Committee shall review and prepare periodic reports to HIO and Participants concerning the ongoing operations of, and other information regarding the System and the Services. Such reports shall include, without limitation, information regarding the efficiency, effectiveness, and security of the System and the Services, and the accesses to and uses and disclosures of Patient Data made by and among Participants pursuant to their use thereof, including, without limitation, Participants' adherence to the specific Terms and Conditions and/or Policies, Procedures and Standards regarding the privacy and security of Patient Data.

15.3 Enforcement and Accountability. The Management Committee may, either independently or upon the request of a Participant, review the uses and disclosures of Patient Data by any Participant, including, without limitation, the Participant's adherence to these Terms and Conditions and/or the Policies, Procedures and Standards, and make recommendations regarding action to be taken by HIO with respect thereto. Such activities of the Management Committee and HIO shall be conducted as described in the Policies, Procedures and Standards. Any action taken by HIO shall be taken only in accordance with these Terms and Conditions and the Policies, Procedures and Standards, and HIO shall provide the Participant an opportunity to provide information regarding the matter(s) involved in any such action to the HIO before any action is taken.

SECTION 16
FEES AND CHARGES

16.1 Agreed-Upon Fees. If the Participant's Participation Agreement describes the fees and charges to be paid by the Participant, the terms and conditions of that Participation Agreement with respect to the payment of fees and charges shall apply. If the Participant's Participation Agreement does not describe such fees and charges, any and all other applicable provisions of this Section 16 (Fees and Charges) shall apply.

16.2 Service Fees. Unless the Participant's Participation Agreement provides otherwise, each Participant shall pay Service Fees to HIO, in accordance with HIO's then-current Fee Schedule. The fee schedule is available at: www.nchiin.org/health-information-exchange/.

16.3 Changes to Fee Schedule. HIO may change its Fee Schedule at any time upon thirty (30) days prior written notice to Participants.

16.4 Miscellaneous Charges. Unless the Participant's Participation Agreement provides otherwise, the Participant also shall pay HIO's charges for all goods or services that HIO provides at the Participant's request that are not specified in HIO's then-current Fee Schedule ("Miscellaneous Charges").

16.5 Payment. The Participant shall pay all Service Fees and any Miscellaneous Charges within thirty (30) days following the date of invoice by HIO sent to the Participant's address as shown in HIO's records or e-mailed in accordance with the Participant's Participation Agreement.

16.6 Late Charges. Service Fees and Miscellaneous Charges not paid to HIO within thirty (30) business days following the due date therefor are subject to a late charge of five percent (5%) of the amount owing and interest thereafter at the rate of one and one-half percent (1.5%) per month on the outstanding balance, or the highest amount permitted by law, whichever is lower.

16.7 Suspension of Service. Failure to pay Service Fees and Miscellaneous Charges within sixty (60) days following the due date therefor may result in termination of the Participant's access to the System

and/or use of the Services on ten (10) days prior notice. A reconnection fee shall be assessed to re-establish connection after termination due to non-payment.

16.8 Taxes. All Service Fees and Miscellaneous Charges shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future, and the Participant shall pay any tax (excluding taxes on HIO's net income) that HIO may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services provided pursuant to the Terms and Conditions.

16.9 Other Charges and Services. The Participant shall be solely responsible for any other charges or expenses the Participant may incur to access the System and use the Services, including without limitation, telephone and equipment charges, and fees charged by third-party vendors of products and services.

SECTION 17
MISCELLANEOUS PROVISIONS

17.1 Applicable Law. The interpretation of these Terms and Conditions and the resolution of any disputes arising under these Terms and Conditions and Participants' Participation Agreements shall be governed by the laws of the State of California. If any action or other proceeding is brought on or in connection with these Terms and Conditions or a Participation Agreement, the venue of such action shall be exclusively in Humboldt County, in the State of California.

17.2 Non-Assignability. Neither HIO nor any Participant shall assign or transfer its rights or obligations under any Participation Agreement, either voluntarily or by operation of law, without the prior written consent of the other party. Any assignment in violation of this Section 17.2 (Non-Assignability) shall be void, and shall be cause for immediate termination of the Participation Agreement. This Section 17.2 (Non-Assignability) shall not be applicable to service agreements or other arrangements usually or customarily entered into by HIO or a Participant to obtain supplies, technical support or professional services.

17.3 Third-Party Beneficiaries. There shall be no third-party beneficiaries of any Participation Agreement.

17.4 Supervening Circumstances. Neither the Participant nor HIO shall be deemed in violation of any provision of a Participation Agreement if it is prevented from performing any of its obligations by reason of severe weather and storms, earthquakes or other natural occurrences, strikes or other labor unrest, power failures, nuclear or other civil or military emergencies, acts of legislative, judicial, executive, or administrative authorities or any other circumstances that are not within its reasonable control. This Section 17.4 (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.

17.5 Severability. Any provision of these Terms and Conditions or any Participant Participation Agreement that shall prove to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provision of these Terms and Conditions or such Participation Agreement, and such other provisions shall remain in full force and effect.

17.6 Notices. Any and all notices required or permitted under these Terms and Conditions shall be in writing and either served personally or sent by certified mail, to the respective addresses set forth below. Notice shall be effective upon actual receipt or refusal as shown on the receipt obtained pursuant to the foregoing.

HIO: North Coast Health Improvement and Information Network

Attention: Rosemary DenOuden, Chief Executive Officer
2315 Dean Street
Eureka, California 95501

Participant: Humboldt County Department of Health and Human Services
Attention: Connie Beck, Director
507 F Street
Eureka, California 95501

17.7 Waiver. No provision of these Terms and Conditions or any Participant Participation Agreement shall be deemed waived, and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether expressed or implied, shall not constitute consent to, waiver of, or excuse for any such breach in the future, or of the breach of any other requirement of these Terms and Conditions or any Participation Agreement.

17.8 Independent Contractors. In the performance of their respective responsibilities under any Participation Agreement, HIO and the Participant are and shall be at all times acting as the independent contractor of the other, and not by virtue of that Participation Agreement or otherwise under these Terms and Conditions acting as an employee, agent, or partner of, or joint venture with, the other.

17.9 Amendment. No addition to, or modification of, these Terms and Conditions or any Participation Agreement shall be valid unless made in writing and signed by the parties hereto.

17.10 Nuclear Free Humboldt County Ordinance Compliance. HIO certifies by its execution of the Participation Agreement that it is not a Nuclear Weapons Contractor, in that HIO is not knowingly or intentionally engaged in the research, development, production, or testing of nuclear warheads, nuclear weapons systems, or nuclear weapons components as defined by the Nuclear Free Humboldt County Ordinance. HIO agrees to notify Participant immediately if it becomes a Nuclear Weapons Contractor as defined above. Participant may immediately terminate its Participation Agreement if it determines that the foregoing certification is false or if HIO becomes a Nuclear Weapons Contractor.

17.11 Interpretation. These Terms and Conditions and Participant's Participation Agreement shall be deemed to have been prepared equally by both HIO and Participant, and shall not be construed or interpreted more favorably for one party on the basis that the other party prepared it.

17.12 Independent Construction. The titles of the sections, subsections, and paragraphs set forth in these Terms and Conditions, Participant's Participation Agreement and the Policies, Procedures and Standards are inserted for convenience of reference only, and shall be disregarded in construing or interpreting any of the provisions thereof.

17.13 Complete Understanding. The Participation Agreement, including all attachments thereto, these Terms and Conditions and the Policies, Procedures and Standards, constitutes the entire agreement between HIO and a Participant, and no other agreements, oral or otherwise, regarding the subject matter contained therein shall be deemed to exist or to bind either HIO or the Participant. In addition, the Participation Agreement, including all attachments thereto, these Terms and Conditions and the Policies, Procedures and Standards, shall supersede, in its entirety, any and all oral and written agreements between the parties.

HEALTH INFORMATION EXCHANGE ORGANIZATION PARTICIPATION AGREEMENT

EXHIBIT A
COUNTY OF HUMBOLDT HIPAA BUSINESS ASSOCIATE AGREEMENT

RECITALS:

WHEREAS, COUNTY, as a "Covered Entity" wishes to disclose certain information to CONTRACTOR, hereinafter referred to as the "BUSINESS ASSOCIATE," pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI").

WHEREAS, COUNTY and BUSINESS ASSOCIATE intend to protect the privacy and provide for the security of PHI disclosed to BUSINESS ASSOCIATE pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information and Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws.

WHEREAS, pursuant to HIPAA Regulations, the Privacy Rule and Security Rule (defined below) COUNTY is required to enter into an Agreement containing specific requirements with BUSINESS ASSOCIATE prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Agreement.

NOW THEREFORE, the parties hereto mutually agree as follows:

1. DEFINITIONS:

A. Breach. As used herein, the term "Breach" shall have the meaning given to such term under the HITECH Act and HIPAA Regulations [42 U.S.C. Section 17921 and 45 C.F.R. Section 164.402].

B. Breach Notification Rule. As used herein, the term "Breach of Notification Rule" shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and D.

C. Business Associate. As used herein, the term "Business Associate" shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including, but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.

D. Covered Entity. As used herein, the term "Covered Entity" shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

E. Designated Record Set. As used herein, the term "Designated Record Set" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

F. Electronic Protected Health Information. As used herein, the term "Electronic Protected Health Information" means Protected Health Information that is maintained in or transmitted by electronic media.

G. Electronic Health Record. As used herein, the term "Electronic Health Record" shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

H. **Health Care Operations.** As used herein, the term "Health Care Operations" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

I. **Privacy Rule.** As used herein, the term "Privacy Rule" shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

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

K. **Protected Information.** As used herein, the term "Protected Information" shall mean PHI provided by COUNTY to BUSINESS ASSOCIATE or created, maintained, received, or transmitted by BUSINESS ASSOCIATE on COUNTY's behalf.

L. **Security Incident.** As used herein, the term "Security Incident" shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. Section 164.304.

M. **Security Rule.** As used herein, the term "Security Rule" shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

N. **Unsecured PHI.** As used herein, the term "Unsecured PHI" shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h) and 45 C.F.R. Section 164.402.

2. OBLIGATIONS OF BUSINESS ASSOCIATE:

A. **Permitted Uses.** BUSINESS ASSOCIATE shall use Protected Information only for the purpose of performing BUSINESS ASSOCIATE's obligations under the Agreement and as permitted or required under the Agreement, or as required by law. Further, BUSINESS ASSOCIATE shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by COUNTY. However, BUSINESS ASSOCIATE may use Protected Information as necessary (i) for the proper management and administration of BUSINESS ASSOCIATE; (ii) to carry out the legal responsibilities of BUSINESS ASSOCIATE; or (iii) as required by law. [45 C.F.R. Sections 164.504(e)(2), 164.504(e)(4)(i)].

B. **Permitted Disclosures.** BUSINESS ASSOCIATE shall disclose Protected Information only for the purpose of performing BUSINESS ASSOCIATE's obligations under the Agreement and as permitted or required under the Agreement, or as required by law. BUSINESS ASSOCIATE shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by COUNTY. However, BUSINESS ASSOCIATE may disclose Protected Information as necessary (i) for the proper management and administration of BUSINESS ASSOCIATE; (ii) to carry out the legal responsibilities of BUSINESS ASSOCIATE; or (iii) as required by law. If BUSINESS ASSOCIATE discloses Protected Information to a third-party, BUSINESS ASSOCIATE must obtain, prior to making

any such disclosure, (i) reasonable *written* assurances from such third-party that such Protected Information will be held confidential as provided pursuant to this Agreement and used or disclosed only as required by law or for the purposes for which it was disclosed to such third-party, and (ii) a written agreement from such third-party to immediately notify BUSINESS ASSOCIATE of any breaches, suspected breaches, security incidents, or unauthorized uses or disclosures of the Protected Information in accordance with paragraph 2.l. of the Agreement, to the extent it has obtained knowledge of such occurrences [42 U.S.C. Section 17932; 45 C.F.R. Section 164.504(e)].

C. **Prohibited Uses and Disclosures.** BUSINESS ASSOCIATE shall not use or disclose PHI other than as permitted or required by the Agreement, or as required by law. BUSINESS ASSOCIATE shall not use or disclose Protected Information for fundraising or marketing purposes. BUSINESS ASSOCIATE shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which PHI solely relates [42 U.S.C. Section 17935(a) and 45 C.F.R. Section 164.522(a)(vi)]. BUSINESS ASSOCIATE shall not directly or indirectly receive remuneration in exchange for Protected Information, except with prior written consent of COUNTY and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2), and the HIPAA regulations, 45 C.F.R. Section 164.502(a)(5)(ii); however this prohibition shall not affect payment by COUNTY to BUSINESS ASSOCIATE for services provided pursuant to the Agreement.

D. Appropriate Safeguards. BUSINESS ASSOCIATE shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Agreement, including, but not limited to, administrative, physical and technical safeguards in accordance with the Security Rule, including but not limited to, 45 C.F.R. Sections 164.308, 164.310, and 164.312. [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. BUSINESS ASSOCIATE shall comply with the policies, procedures and documentation requirements of the Security Rule, including, but not limited to, 45 C.F.R. Section 164.316. [42 U.S.C. Section 17931].

E. Business Associate's Subcontractors and Agents. BUSINESS ASSOCIATE shall ensure that any agents and subcontractors that create, receive, maintain or transmit Protected Information on behalf of COUNTY, agree in writing to the same restrictions and conditions that apply to COUNTY with respect to such Protected Information and implement the safeguards required by paragraph 2(D) above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. BUSINESS ASSOCIATE shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e)(1)).

F. Access to Protected Information. If BUSINESS ASSOCIATE maintains a designated record set on behalf of COUNTY, BUSINESS ASSOCIATE shall make Protected Information maintained by BUSINESS ASSOCIATE or its agents or subcontractors in Designated Record Sets available to COUNTY for inspection and copying within five (5) days of a request by COUNTY to enable COUNTY to fulfill its obligations under California Health and Safety Code Section 123110 and the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 C.F.R. Section 164.504(e)(2)(ii)(e)]. If BUSINESS ASSOCIATE maintains Protected Information in electronic format, BUSINESS ASSOCIATE shall provide such information in electronic format as necessary to enable COUNTY to fulfill its obligations under the HITECH Act and HIPAA Regulations, including, but not limited to, 42 U.S.C. Section 17935(e) and 45 C.F.R. Section 164.524.

G. **Amendment of PHI.** If BUSINESS ASSOCIATE maintains a designated record set on behalf of COUNTY, within ten (10) days of a request by COUNTY for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, BUSINESS ASSOCIATE and its agents and subcontractors shall make such Protected Information available to COUNTY for amendment and incorporate any such amendment or other documentation to enable COUNTY to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526. If an individual requests an amendment of Protected Information directly from BUSINESS ASSOCIATE or its agents or subcontractors, BUSINESS ASSOCIATE must notify COUNTY in writing within five (5) days of the request and of any approval or denial of amendment of Protected Information maintained by BA or its agents or subcontractors [45 C.F.R. Section 164.504(e)(2)(ii)(F)].

H. **Accounting of Disclosures.** Within ten (10) days of a request by COUNTY for an accounting of disclosures of Protected Information, BUSINESS ASSOCIATE and its agents and subcontractors shall make available to COUNTY the information required to provide an accounting of disclosures to enable COUNTY to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c), as determined by COUNTY. BUSINESS ASSOCIATE agrees to implement a process that allows for an accounting to be collected and maintained by BUSINESS ASSOCIATE and its agents and subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BUSINESS ASSOCIATE maintains an Electronic Health Record. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. If a patient submits a request for an accounting directly to BUSINESS ASSOCIATE or its agents or subcontractors, BUSINESS ASSOCIATE shall within five (5) days of the request forward it to COUNTY in writing.

I. **Governmental Access to Records.** BUSINESS ASSOCIATE shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to COUNTY and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining BUSINESS ASSOCIATE's compliance with HIPAA [45 C.F.R. Section 164.504(e)(2)(ii)(I)]. BUSINESS ASSOCIATE shall provide COUNTY a copy of any Protected Information and other records that BUSINESS ASSOCIATE provides to the Secretary concurrently with providing such Protected Information to the Secretary.

J. **Minimum Necessary.** BUSINESS ASSOCIATES and its agents and subcontractors shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure. [42 U.S.C. Section 17935(b); 45 C.F.R. Section 164.514(d)]. BUSINESS ASOCIATE understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

K. **Data Ownership.** BUSINESS ASSOCIATE understands that BUSINESS ASSOCIATE has no ownership rights with respect to the Protected Information.

L. **Notification of Possible Breach.** BUSINESS ASSOCIATE shall notify COUNTY within twenty-four (24) hours of any suspected or actual breach of Protected Information; any use or

disclosure of Protected Information not permitted by the Agreement; any security incident (i.e., any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system) related to Protected Information, and any actual or suspected use or disclosure of data in violation of any applicable federal or state laws by BUSINESS ASSOCIATE or its agents or subcontractors. The notification shall include, to the extent possible, the identification of each individual whose unsecured Protected Information has been, or is reasonably believed by the BUSINESS ASSOCIATE to have been accessed, acquired, used, or disclosed, as well as any other available information that COUNTY is required to include in notification to the individual, the media, the Secretary, and any other entity under the Breach Notification Rule and any other applicable state or federal laws, including, but not limited, to 45 C.F.R. Section 164.404 through 45 C.F.R. Section 164.l408, at the time of the notification required by this paragraph or promptly thereafter as information becomes available. BUSINESS ASSOCIATE shall take (i) prompt corrective action to cure any deficiencies and (ii) any action pertaining to unauthorized uses or disclosures required by applicable federal and state laws. [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)]. Any and all notices required pursuant to the terms and conditions of this provision shall be submitted to COUNTY at the following address:

COUNTY: Humboldt County DHHS Compliance and Quality Assurance Office
Attention: Compliance and Quality Assurance Administrator & Privacy Officer
507 F Street
Eureka, California 95501
(707) 441-5410

M. **Breach Pattern or Practice by Business Associate's Subcontractors and Agents.** Pursuant to 42 U.S.C. Section 17934(b) and 45 C.F.R. Section 164.504(e)(1)(ii), if BUSINESS ASSOCIATE knows of a pattern or activity or practice of a subcontractor or agent that constitutes a material breach or violation of the subcontractor or agent's obligations under the Agreement or other arrangement, BUSINESS ASSOCIATE must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, BUSINESS ASSOCIATE must terminate the Agreement or other arrangement if feasible. BUSINESS ASSOCIATE shall provide written notice to COUNTY of any pattern of activity or practice of a subcontractor or agent that BUSINESS ASSOCIATE believes constitutes a material breach or violation of the subcontractor or agent's obligations under the Agreement or other arrangement within five (5) days of discovery and shall meet with COUNTY to discuss and attempt to resolve the problem as one (1) of the reasonable steps to cure the breach or end the violation.

N. **Audits, Inspection and Enforcement.** Within ten (10) days of a request by COUNTY, BUSINESS ASSOCIATE and its agents and subcontractors shall allow COUNTY or its agents or subcontractors to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Agreement for the purpose of determining whether BUSINESS ASSOCIATE has complied with this Agreement or maintains adequate security safeguards. BUSINESS ASSOCIATE shall notify COUNTY within five (5) days of learning that BUSINESS ASSOCIATE has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights or other state or federal government entity.

3. TERMINATION:

A. **Material Breach.** A breach by BUSINESS ASSOCIATE of any provision of this Agreement, as determined by COUNTY, shall constitute a material breach of the Agreement and shall

provide grounds for *immediate* termination of the Agreement, any provision in the Agreement to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii)].

B. **Effect of Termination.** Upon termination of the Agreement for any reason, BUSINESS ASSOCIATE shall, at the option of COUNTY, return or destroy all Protected Information that BUSINESS ASSOCIATE or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by COUNTY, BUSINESS ASSOCIATE shall continue to extend the protections of Section 2 of this Agreement to such information, and limit further use and disclosure of such PHI to those purposes that make the return or destruction of the information infeasible [45 C.F.R. Section 164.504(e)(ii)(2)(J)]. If COUNTY elects destruction of the PHI, BUSINESS ASSOCIATE shall certify in writing to COUNTY that such PHI has been destroyed in accordance with the Secretary's guidance regarding proper destruction of PHI.

4. **INTERPRETATION:**

Any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, and the HIPAA regulations.

EXHIBIT B
PARTICIPANT TYPES, DATA TYPES AND PROJECTS, AND OTHER HEALTH INFORMATION ORGANIZATIONS

Participant Types

Ambulatory Care Medical Practice or Clinic
County Public Health
Health Plan or Administrative Services Organization
Hospital
Licensed Clinical Laboratory
Mental Health Provider or Clinic
Rehabilitation Center
Skilled Nursing Facility
Surgery Center

Additional Services and Data Types

Project/Addendum Type	Data Type
ADT Information	Admission, Discharge, Transfer results delivery and query
CAIR	Immunization Data Sent to the California Immunization Registry
CalREDIE	Data sent to the California Reportable Disease Information Exchange
Community Information Exchange	Cross-sector data exchange shared to support care coordination
Care Coordination and Health Plan Support	Protected Health Information Exchange to support Care Coordination and Quality Improvement
Documents	Documents results delivery
Facility Alerts	Notification to providers of A/D.T
Lab Results	Lab Orders/results delivery

Other HIOs

Providence St. Joseph Health Clinical Informatics, Health Information Exchange and Interoperability

HEALTH INFORMATION EXCHANGE ORGANIZATION PARTICIPATION AGREEMENT

EXHIBIT C
ASSOCIATED SOFTWARE AND ASSOCIATED HARDWARE

Data Exchange Projects

Project:

Item	Amount
Development of	$
Annual software support and maintenance fees	$

HEALTH INFORMATION EXCHANGE ORGANIZATION PARTICIPATION AGREEMENT

EXHIBIT D
DATA SECURITY REQUIREMENTS

1. Personnel Controls.

1.1 Employee Training. All workforce members who assist in the performance of functions or activities on behalf of North Coast Health Improvement and Information Exchange Network, hereinafter referred to as "HIO," or access or disclose Patient Data, including, without limitation, Protected Health Information, Personal Information, Personally Identifiable Information and Medical Information, must complete information privacy and security training, at least annually, at their own expense. Each workforce member who receives information privacy and security training must sign a certification indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following expiration or termination of the Participation Agreement.

1.2 Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with any of the privacy, security and confidentiality requirements contained herein, including termination of employment where appropriate.

1.3 Confidentiality Statement. All persons that will be working with Patient Data must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use and Enforcement Policies. The statement must be signed by the workforce member prior to gaining access to Patient Data. The statement must be renewed annually. HIO shall retain each person's written confidentiality statement for inspection for a period of six (6) years following expiration or termination of the Participation Agreement.

1.4 Background Check. Before a member of the workforce may access Patient Data, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. HIO shall retain each workforce member's background check documentation for a period of three (3) years following expiration or termination of the Participation Agreement.

2. Technical Security Controls.

2.1 Workstation and Laptop Encryption. All workstations and laptops that store Patient Data either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard ("AES").

2.2 Server Security. Servers containing unencrypted Patient Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

2.3 Minimum Necessary. Only the minimum necessary amount of Patient Data required to perform necessary business functions may be copied, downloaded or exported.

2.4 Removable Media Devices. All electronic files that contain Patient Data must be encrypted when stored on any removable media or portable device, including, without limitation, USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes, etc. Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.

2.5 Antivirus Software. All workstations, laptops and other systems that process and/or store Patient Data must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

2.6 Patch Management. All workstations, laptops and other systems that process and/or store Patient Data must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release. Applications and systems that cannot be patched within the required time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

2.7 Data Destruction. When no longer needed, all Patient Data must be wiped using the Gutmann or United States Department of Defense ("DOD") 5220.22-M (7 Pass) standard or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

2.8 User Identification and Password Controls. All users must be issued a unique user name for accessing Patient Data. Usernames must be promptly disabled, deleted or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours. Passwords are not to be shared. Passwords must be at least eight (8) characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every ninety (90) days, preferably every sixty (60) days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z);
- Lower case letters (a-z);
- Arabic numerals (0-9);
- Non-alphanumeric characters (punctuation symbols).

2.9 System Timeout. The system providing access to Patient Data must provide an automatic timeout, requiring re-authentication after no more than twenty (20) minutes of inactivity.

2.10 Warning Banners. All systems providing access to Patient Data must display a warning banner stating that data is confidential, systems are logged and system use is for business purposes only by authorized users. Users must be directed to log off the system if they do not agree with these requirements.

2.11 System Logging. The system must maintain an automated audit trail which can identify the user or system process which alters Patient Data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only and must be restricted to authorized users. If Patient Data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence.

2.12 Access Controls. The system providing access to Patient Data must use role based access controls for all user authentications, enforcing the principle of least privilege.

2.13 Transmission Encryption. All data transmissions of Patient Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Patient Data can be encrypted. This requirement pertains to any type of Patient Data in motion such as website access, file transfer and E-Mail.

2.14 Intrusion Detection. All systems involved in accessing, holding, transporting and protecting Patient Data that are accessible via the internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls.

3.1 System Security Review. HIO must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Patient Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

3.2 Log Reviews. All systems processing and/or storing Patient Data must have a routine procedure in place to review system logs for unauthorized access.

3.3 Change Control. All systems processing and/or storing Patient Data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity and Disaster Recovery Controls.

4.1 Emergency Mode Operation Plan. HIO must establish a documented plan to enable continuation of critical business processes and protection of the security of Patient Data held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under the Participation Agreement for more than twenty-four (24) hours.

4.2 Data Backup Plan. HIO must have established documented procedures to backup Patient Data to maintain retrievable exact copies of Patient Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media and an estimate of the amount of time needed to restore Patient Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of data.

5. Paper Document Controls.

5.1 Supervision of Data. Patient Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Patient Data in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

5.2 Escorting Visitors. Visitors to areas where Patient Data is contained shall be escorted, and Patient Data shall be kept out of sight while visitors are in the area.

5.3 Confidential Destruction. Patient Data must be disposed of through confidential means, such as cross-cut shredding and pulverizing.

5.4 Removal of Data. Only the minimum necessary amount of Patient Data may be removed from the premises of HIO except with express written permission from the County of Humboldt. Patient Data shall not be considered "removed from the premises," if it is only being transported from one of HIO's locations to another of HIO's locations.

5.5 Faxing. Faxes containing Patient Data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

5.6 Mailings. Mailings containing Patient Data shall be sealed and secured from damage or inappropriate viewing of such Patient Data to the extent possible. Mailings which include five hundred (500) or more individually identifiable records of PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission to use another method is obtained.

EXHIBIT E
PROJECT ADDENDUM

Project Name	
Data Submitted for Exchange	
Data Provider(s)	
Data Recipient(s)	
Exchange Conditions	
Permitted Uses	
Authorized Users	
Specific Safeguards and Privacy Requirements	All Participants shall adhere to the HIE Policies, Procedures and Standards 1.1 available at http://nchiin.org.
Licensed Software	
Certification Requirements	N.A.
Definitions for Project Addendum	
Fees	
Organization	
Program	
Contact for Organization	Name: Title: Address: Telephone: Email:

[Signatures on Following Page]

IN WITNESS WHEREOF, the parties hereto have executed this Project Addendum on the dates hereinafter indicated.

NORTH COAST HEALTH IMPROVEMENT AND INFORMATION NETWORK:

By: _____ Date: _____

Name: _____

Title: _____

By: _____ Date: _____

Name: _____

Title: _____

COUNTY OF HUMBOLDT:

By: _____ Date: _____

Connie Beck, DHHS Director
(Pursuant to the authority granted by the Humboldt County Board of Supervisors on _____ __, 20[__] [Item _-_])