



INLAND EMPIRE HEALTH INFORMATION EXCHANGE

PARTICIPATION AGREEMENT

SEPTEMBER 1, 2016

v2.3

COUNTY OF FRESNO



TERMS AND CONDITIONS FOR
INLAND EMPRIE HEALTH INFORMATION EXCHANGE
PARTICIPANT'S AGREEMENT

Section 1
INTRODUCTORY AND GENERAL PROVISIONS

1.1 Introduction. These applicable provisions of these Terms and Conditions (the "Terms and Conditions") are incorporated by reference into each Health Information Exchange Participant's Agreement (each, a "Participation Agreement") entered into by and between Inland Empire E.H.R. Resource Center, a California 501(c)(3) nonprofit corporation, on behalf of the Inland Empire Health Information Exchange ("IEHIE"), and the County of Fresno, limited to Programs participating as part of its Health Care Component and Emergency Medical Services ("Participant").

1.2 Effective Date. The Effective Date of these Terms and Conditions is made and entered into as of the last date signed below (the "Effective Date").

1.3 Nature of Organization. IEHIE is California nonprofit organization, organized by the Inland Empire Health Information Exchange, 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.

1.3.1 Affiliation. Participant is affiliated with the Central Valley [formerly the Tulare-Kings-Fresno-Madera] Health Information Exchange ("CVHIE") and intends to participate in CVHIE through the Inland Empire Health Information Exchange.

1.4 Description of Services. IEHIE provides or arranges for the provision of data transmission and related services to allow Participants to conduct searches for Patient Data, and to exchange Patient Data identified from those searches, from a centralized computer system that facilitates the sharing of Patient Data among disparate Participants. IEHIE's services include establishing and applying standards for such exchange of Patient Data. IEHIE has access to and/or is responsible to maintain all of such Patient Data in the performance of IEHIE's services. IEHIE also aggregates and/or maintains a repository of Patient Data.

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

1.5.1 "Additional Services" means products and/or services not expressly described in these Terms and Conditions that the IEHIE offers to certain Participants from time to time, as described in the Policies and Procedures and/or the applicable Participation Agreement.

1.5.2 "Associated Hardware" and "Associated Software" shall have the meanings described in Section 8.1 (Description of Associated Hardware and/or Associated Software).

1.5.3 “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.

1.5.4 “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 (i) the viability of IEHIE; (ii) the trust among Participants; or (iii) the legal liability of IEHIE or any Participant.

1.5.5 “CMIA” means the California Confidentiality of Medical Information Act, California Civil Code Section 56 *et. seq.*

1.5.6 “Data Provider” means a Participant that is registered to provide information to IEHIE for use through the Services.

1.5.7 “Data Recipient” means a Participant that uses the Services to obtain health information.

1.5.8 “Effective Date” means the Effective Date of these Terms and Conditions specified pursuant to Section 1.2 (Effective Date).

1.5.9 “Fee Schedule” means that part of the Participation Agreement which sets forth the fees paid (“Fees”) in exchange for the Services provided by the IEHIE.

1.5.10 “HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder at 45 CFR Parts 160 and 164.

1.5.11 “HITECH” means 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 (commonly known as “ARRA”), Pub. L. No. 111-5 (February 17, 2009).

1.5.12 “Other HIO” means a person or entity similarly situated to the IEHIE with which IEHIE has entered into a legally binding agreement pursuant to which IEHIE and that person or entity have agreed to arrange for their respective participants to share data through IEHIE’s and the person’s or entity’s respective systems and services.

1.5.13 “Participant” means a party that entered into a Participation Agreement with IEHIE to act as a Data Provider and/or as a Data Recipient.

1.5.14 “Participant Type” means the category(ies) of Participant to which a particular Participant is assigned by IEHIE based upon that Participant’s role in the health care system, as more specifically described in Section 2.4.3 (Participant Type).

1.5.15 “Participation Agreement” means a legally binding agreement between IEHIE and a party pursuant to which that party acts as a Participant in accordance with, and agrees to comply with, these Terms and Conditions.

1.5.16 “Patient Data” means information provided, or made available for exchange, by a Data Provider through IEHIE’s System and Services pursuant to Section 7.2 (Provision of Data).

1.5.17 “Person(s)” means human beings, generally as individuals, but can also be interpreted as members of legal entities (such as firms, IPAs, partnerships, associations, corporations, legal representatives, etc.) who have the legal capacity of their organization to sign legally binding agreements.

1.5.18 “Policies and Procedures” means, collectively, the policies and procedures adopted by IEHIE’s using approved processes for the operation and use of the System and the Services, including without limitation any operations manual, privacy and/or security policies, and technical specifications for the System and/or the Services.

1.5.19 “Services” means the health information exchange and related services described in Section 1.3.1 (Description of Services) for which the Participant registers and pays Fees for, as described in Section 2.4.1 (Participation Agreement Required).

1.5.20 “System” means the technology provided by IEHIE incident to IEHIE’s performance of the Services, as described in the Policies and Procedures.

1.5.21 “Terms and Conditions” means the terms and conditions set forth in this document that apply to a Participant and the IEHIE, respectively as amended, repealed, and/or replaced from time to time as described herein.

1.5.22 “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 U.S. Department of Health & Human Services (“HHS”) through guidance issued pursuant to HITECH.

1.5.23 “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.

Section 2

DEVELOPMENT AND ADMINISTRATION OF PARTICIPATION AGREEMENTS

2.1 Development and Dissemination of Terms and Conditions and Policies and Procedures; Amendments. Subject to the Governing Council, IEHIE is solely responsible for the development of the Terms and Conditions and the Policies and Procedures, and may amend, or repeal and replace, the Terms and Conditions and/or the Policies and Procedures as described in Section 2.3 (Changes to Terms and Conditions and/or Policies and Procedures).

2.2 Relationships Between Terms and Conditions and Policies and Procedures.

(a) The Policies and Procedures are incorporated into these Terms and Conditions, and IEHIE and each Participant shall be required to comply with the applicable provisions of the Policies and Procedures as described in Section 2.4.5 (Effect of Terms and Conditions Upon Participation Agreements).

(b) IEHIE may exchange data with such Other HIOs that shall be identified in the Policies and Procedures, provided that such Other HIOs have agreed in their legally binding agreements with the IEHIE to (i) comply with all laws applicable to the Other HIO, including but not limited to HIPAA and HITECH, and to maintain and enforce appropriate policies and procedures in compliance therewith, (ii) appropriately and, in accordance with applicable industry standards, authenticate 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, (iii) 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 HIOs electronic systems in the manner or scope permitted by the privileges; and (iv) an appropriate indemnification provision regarding the Other HIOs act or omission related to the foregoing or receipt by an HIO of an inappropriate data request from or through Other HIOs' systems.

2.3 Changes to Terms and Conditions and Policies and Procedures. Subject to Section 3.2 (Participant's Termination of Participation Agreement Based on Objection to Change) and Section 12.2 (Meetings and Responsibilities of Governing Council), IEHIE may amend, repeal and replace these Terms and Conditions and/or the Policies and Procedures at any time, as required in order for IEHIE and/or Participants to comply with applicable laws and regulations. IEHIE shall endeavor to give Participants notice of such changes not less than thirty (30) days prior to the implementation of those changes. However, IEHIE may implement the change within a shorter period of time as IEHIE determines is appropriate under the circumstances. Any such change to the Terms and Conditions and/or Policies and Procedures shall automatically be incorporated by reference into each Participation Agreement, and be legally binding upon IEHIE and the Participant, as of the effective date of the change.

2.4 Development and Administration of Participation Agreements.

2.4.1 Participation Agreement Required. Only Persons who enter into Participation Agreements with IEHIE shall be permitted to access the System and use the Services. A Participant must act as a Data Provider and as a Data Recipient, as described in this Section 2.4

(Development and Administration of Participation Agreements). A Participant may use some or all of the Services, as specified in Section 1.4 of that Participant's Participation Agreement and in accordance with the Exhibit C (Fees and Payments).

2.4.2 Execution of Participation Agreements. A Person may become a Participant only by entering into a written Participation Agreement with IEHIE. Each Participation Agreement shall describe:

- (a) The Participant's Participant Type, as described in Section 2.4.3 (Participant Type);
- (b) Which of the Services the Participant may use; and
- (c) Such other terms and conditions as IEHIE and the Participant shall agree.
- (d) The Fees to be paid in exchange for the Services.

2.4.3 Participant Type. Each Participant will be both a Data Recipient and a Data Provider, and therefore subject to both provisions in Section 6 and Section 7.

2.4.4 Approval and Disapproval of Applications for Participation Agreements. Any party may apply to IEHIE to enter into a Participation Agreement, subject to the applicable terms of the Policies and Procedures. IEHIE shall not be required to approve any application to be a Participant. If a party is located in a service area served wholly or in part by another IEHIE-contracted HIO, IEHIE will consult with that IEHIE client with respect to the new application. In the event of a disagreement with respect to entertaining a new application, the client may appeal to the Governing Council or to dispute resolution.

2.4.5 Effect of Terms and Conditions and Policies and Procedures Upon Participation Agreements. Each Participation Agreement shall incorporate by reference, and require that the Participant agree to comply with, these Terms and Conditions, as well as all IEHIE Policies and Procedures. IEHIE may make exceptions to this Section 2.4.5 (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 IEHIE or other Participants, or provide that the Participant is not subject to those provisions of the Terms and Conditions and the Policies and Procedures regarding the privacy and security of Patient Data.

2.5 Change or Termination of Services. IEHIE may cease to participate in any Other HIO, 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 in its sole discretion upon not less than ninety (90) days prior notice to Participants.

Section 3

TERM AND TERMINATION OF PARTICIPATION AGREEMENTS

3.1 Term of Participation Agreements. Each Participation Agreement shall take effect on the Effective Date specified therein, and shall remain in force and effect for a period of five (5) years, or until terminated by either IEHIE or the Participant, as provided in these Terms and Conditions.

3.2 Participant's Termination of Participation Agreement Based on Objection to Change. Notwithstanding Section 2.3 (Changes to Terms and Conditions and Policies and Procedures), the IEHIE shall not make any change to the Terms and Conditions and/or the Policies and Procedures that either (a) materially reduces the rights or increases the obligations of a Participant, (b) materially reduces the obligations of the IEHIE, or (c) substantially changes the provisions of the Terms and Conditions or Policies and Procedures regarding the privacy or security of Patient Data, without providing to the Participant the right to terminate its Participation Agreement by giving IEHIE written notice thereof not more than thirty (30) days following IEHIE'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 the Terms and Conditions or Policies and Procedures that IEHIE determines is required to comply with any federal, state, or local law or regulation shall take effect as of the effective date IEHIE 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 IEHIE's receipt of the Participant's notice of termination.

3.3 Participant's Termination of Participation Agreement Without Cause. A Participant may terminate its Participation Agreement at any time without cause by giving not less than ninety (90) days prior notice to IEHIE. However, Participant may be subject to a termination fee, as outlined and attached hereto as Exhibit C (Fees and Payments).

3.4 Participant's Termination of Participation Agreement Upon Uncured Breach. Without limiting the obligations of IEHIE pursuant to Sections 3.5 or 11.1 (IEHIE's Performance of Obligations, Generally), a Participant may terminate its Participation Agreement upon IEHIE's failure to substantially conform to the performance of Services listed in the Participant's Participation Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given IEHIE notice of that failure and requested that IEHIE cure that failure.

3.5 Participant's Termination of Participation Agreement Upon Breach of Business Associate Agreement. Notwithstanding any other provision of Section 2.4 (Development and Administration of Participation Agreements) to the contrary, the Participant may terminate its Participation Agreement based upon IEHIE's breach of its Business Associate Agreement with the Participant if breach continues uncured for thirty (30) days after Participant has notified IEHIE in writing.

3.6 IEHIE's Termination of Participation Agreement Without Cause. Except as provided otherwise in the applicable Participation Agreement, IEHIE may terminate any Participant's Participation Agreement at any time without cause by giving not less than ninety (90) days prior notice to the Participant.

3.7 IEHIE's Termination of Participation Agreement Upon Uncured Breach. Without limiting the obligations of the Participant pursuant to Section 5.1 (Participant's Performance of Obligations, Generally), IEHIE may terminate any Participant's Participation Agreement upon the Participant's failure to substantially conform the Terms and Conditions arising out of and contained in the Participant's Participation Agreement, and that failure continues uncured for a period of sixty (60) days after IEHIE has given the Participant notice of that failure and requested that the Participant cure that failure.

3.8 Effect of Termination of Participation Agreement. 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.

3.9 Survival of Provisions. The following provisions of the Terms and Conditions shall survive any termination of a Participant's Participation Agreement: Section 4.5 (Responsibility for Conduct of Participant and Authorized Users), Section 9 (Privacy and Security of Patient Data), Section 10 (Business Associate Agreement), Section 14 (Proprietary and Confidential Information), Section 15.8 (Limitation on Liability) and Section 16.2 (Indemnification, Generally).

Section 4 AUTHORIZED USERS

4.1 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, a copy of which protocol shall be provided to IEHIE upon request. Such protocol shall comply with the requirements therefor set forth in the Policies and Procedures, 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 and to verify the credentials of each Authorized User prior to enabling that Authorized User to use the System and the Services. Each Participant shall comply with such protocol in all material respects.

4.2 Certification of Authorized Users. At the time that a Participant identifies an Authorized User to IEHIE pursuant to Section 4.1 (Identification of Authorized Users), the Participant shall certify to IEHIE that the Authorized User:

(a) Has completed a training program conducted by Participant in accordance with Section 5.7 (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 IEHIE pursuant to Section 2.4.3 (Participant Type);

(c) Has agreed not to disclose to any other person any passwords issued to the Authorized User pursuant to Section 4.3 (Passwords and Other Security Mechanisms);

(d) Has acknowledged in writing that his or her failure to comply with the 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. Documentation, including the signed Access Request Form, shall be retained by Participant for at least six (6) years and made available to IEHIE upon request.

4.3 Passwords and Other Security Mechanisms. Based on the information provided by the Participant pursuant to Section 4.1 (Identification of Authorized Users), IEHIE shall issue a user name and password to each Authorized User that shall permit the Authorized User to access the System and use the Services. IEHIE shall provide each such user name and password 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 IEHIE of the change, pursuant to Section 4.1 (Identification of Authorized Users), IEHIE shall cancel the user name and password of such individual with respect to the Participant, and cancel and de-activate the user name and password of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

4.4 No Use by 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 IEHIE in accordance with Section 4.1 (Identification of Authorized Users).

4.5 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.

4.6 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, by its own accord, or immediately, upon notice from IEHIE, discipline appropriately or terminate their Authorized User status, any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with the Participant's disciplinary policies and procedures. Failure to do so shall be considered a material breach of this Agreement by Participant.

Section 5

GENERAL OBLIGATIONS OF PARTICIPANTS

5.1 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 the Terms and Conditions and the Policies and Procedures and shall, promptly following notice of any material breach thereof by IEHIE, cure such breach.

5.2 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.

5.3 System Security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Policies and Procedures, which is incorporated herein by reference as well as all requirements under state and federal regulations and guidelines.

a. In the course of normal business operations, such as software updates, possible breach investigations, reconfiguration of connection routes, et cetera (examples are illustrative, not exhaustive) it may become necessary for Participant to temporarily stop the transmission of Patient Data. Upon advanced notice to IEHIE of the planned downtime, or as soon as possible in the event of an unplanned downtime, Participant shall be permitted to temporarily cease transmission to IEHIE. Participant will also include an estimated time period for the downtime event and include the expected recommencement of transmission, if applicable and/or known. Notices may be sent by United States mail, overnight delivery service, facsimile transmission, or electronic mail to the address described in Section 18.6 (Notices).

5.4 Software and Hardware Provided by Participant. Except as provided in Section 8 (Associated Hardware and Software to be Provided by IEHIE), 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 IEHIE all information required to be provided by the Participant ("Participant's Required Hardware and Software"). Each Participant's Required Hardware and Software shall conform to IEHIE's then-current specifications, as set forth in the Policies and Procedures. 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.

5.5 Pass-Through Obligations. The Participant acknowledges that the use of the System incident to the Services by the Participant, and by all individuals acting on the Participant's behalf, including without limitation, all employees and other staff, shall be subject to certain obligations of the agreements and other arrangements pursuant to which IEHIE shall procure rights to use the System, as specified in Exhibit B (Exchange Overview), and subject to the Terms and Conditions of the Agreement. The Participant shall comply, and assure the compliance of the Participant's employees and other staff, with these pass-through obligations.

5.6 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 IEHIE 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 IEHIE or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

5.7 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 requirements imposed under HIPAA.

Section 6

DATA RECIPIENT'S USE OF SYSTEM AND SERVICES

Pursuant to the applicable Participation Agreement, the Participant is a Data Recipient, the terms of this Section 6 (Data Recipient's Use of System and Services) shall apply to that Participant.

6.1 Grant of Rights to Use System and Services.

6.1.1 Grant by IEHIE. IEHIE 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 to use 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 the Terms and Conditions and the Data Recipient's Participation Agreement. IEHIE 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 the Terms and Conditions.

6.1.2 Applicable Policies and Procedures. 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 and Procedures, which are incorporated herein by reference.

6.1.3 Permitted Purposes for Use of System and Services. A Data Recipient may use the System and the Services only to locate and retrieve Patient Data for purposes of treatment, payment or health care operations, as those terms are defined in HIPAA.

6.2 Permitted Degree of Access to Patient Data. Except for requests for Patient Data for treatment purposes, the Data Recipient shall use the System and the Services to request or seek access to only that amount of Patient Data that is the minimum necessary to accomplish the Data Recipient's intended purpose in making the request or seeking access and, to the extent practicable, the Data Recipient shall limit its request for Patient Data to that Patient Data contained in a limited data set, as defined by HIPAA.

6.3 Compliance with Applicable Laws. Without limiting the generality of Section 6 (Permitted Uses 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.

6.4 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 and Procedures, which are incorporated herein by reference.

6.4.1 No Services to Third Parties. Except as expressly permitted by the applicable Participation Agreement, the Data Recipient shall use the System or the Services for which the Participant is to receive pursuant to its Participation Agreement and only for the Data Recipient's own account, and shall not use any part of the System or the Services to provide separate services or sublicenses to any third party, including without limitation providing any service bureau services or equivalent services to a third party.

6.4.2 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.

6.4.3 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, without the express written consent of IEHIE and each of the Participants and Authorized Users being compared.

6.5 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 7.5 (Limitations on Use of Patient Data).

6.6 Effect of Termination on Data Recipient. Upon any termination of a Data Recipient's Participation Agreement, the Data Recipient shall cease to be a Participant and thereupon 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 7

DATA PROVIDERS' USE OF SYSTEM AND SERVICES

Pursuant to the applicable Participation Agreement, the Participant is a Data Provider, the terms of this Section 7 (Data Providers' Use of System and Services) shall apply to that Participant.

7.1 Grant of Rights by IEHIE.

7.1.1 Grant by IEHIE. IEHIE 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 to use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider's Use of System and Services), subject to the Data Provider's full compliance with the Terms and Conditions and the Data Provider's Participation Agreement. IEHIE 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 the Terms and Conditions.

7.1.2 Applicable Policies and Procedures. All issues concerning the ownership and rights in IEHIE's System shall be as set forth in the Policies and Procedures, which are incorporated herein by reference. Nothing in the Policies and Procedures or the Agreement is intended to limit a Participant's use of its own data.

7.2 Provision of Data. The Data Provider shall participate in and maintain its connection to the System's record locator, service-based federated network and provide through the System the Patient Data the Data Provider has agreed to provide pursuant to the specific terms of its Participation Agreement.

7.3 Measures to Assure Accuracy of Data.

7.3.1 Applicable Policies and Procedures. Each Data Provider shall, in accordance with the Policies and Procedures, use reasonable and appropriate efforts to assure that all of the Patient Data it provides through the System is accurate, free from serious error, reasonably complete, and provided in a timely manner, as specified in the Policies and Procedures.

7.4 Grant of License to Use Patient Data. Subject to Section 7.5 (Limitations on Use of Patient Data), the Data Provider grants to IEHIE a perpetual, fully-paid, non-exclusive, royalty-free right and license (i) to 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 and Procedures and these Terms and Conditions, (ii) to use such Patient Data to perform the Other Activities IEHIE performs pursuant to Section 11.8 (Other Activities), and (iii) to use such Patient Data to carry out IEHIE's duties under the Policies and Procedures and 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 IEHIE determines is necessary and appropriate.

7.5 Limitations on Use and Disclosure of Patient Data. Notwithstanding Section 7.4 (Grant of License to Use Patient Data by Data Provider), Patient Data provided by a Data Provider shall not be used or disclosed for any of the following purposes:

7.5.1 Uses and Disclosures Prohibited by Policies and Procedures. Any use or disclosure that is prohibited by the Policies and Procedures.

7.5.2 Uses and Disclosure Prohibited by Law. Any use or disclosure use that is prohibited by applicable laws.

7.6 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 and Procedures. Without limiting the generality of the foregoing, except in connection with the provision of Patient Data for treatment purposes, as defined under HIPAA, the Data Provider shall, to the extent practicable, limit the Patient Data provided in response to a request received through the System for information or access to information to that information contained in a limited data set, as defined by HIPAA. The Data Provider shall in any event limit the Patient Data disclosed pursuant to a request received through the System for information or access to information to the Patient Data that is the minimum necessary to respond to the request.

7.7 Effect of Termination Upon Data Provider. Upon any 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 10 (Business Associate Agreement), if and to the extent that IEHIE maintains any Patient Data on the Data Provider's behalf, and it is feasible to do so, the IEHIE shall not, from and after the effective date of the termination of the Data Provider's Participation, provide or make that information available to Data Recipients. Thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services.

Section 8

ASSOCIATED HARDWARE AND SOFTWARE TO BE PROVIDED BY IEHIE

If, pursuant to the applicable Participation Agreement, the Participant has agreed to receive Associated Hardware and/or Associated Software from the IEHIE, the terms of this Section 8 (Associated Hardware and Software to be Provided by IEHIE) shall apply to that Participant.

8.1 Description of Associated Software and Associated Hardware. IEHIE shall arrange for the provision of the software and/or hardware required to access the System and use the Services the Participant has agreed to receive pursuant to its Participation Agreement, as more particularly described in Schedule 8 attached to the applicable Participation Agreement (the “Associated Software” and “Associated Hardware,” respectively). The vendor or vendors of the Associated Software and/or Associated Hardware shall be responsible for the provision of, and the performance of, the Associated Software and Associated Hardware provided in accordance with the applicable license or subscription or other agreements described in Section 8.5 (Third Party Software, Hardware and/or Services).

8.2 Grant of License. IEHIE 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 (the “Associated Software”). IEHIE shall make the Vendor Terms and Conditions of such licenses and other rights available to Participant upon request.

8.3 Copying. The Participant shall not, without IEHIE’s prior written consent, copy any of the Associated Software.

8.4 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 IEHIE.

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

8.5.1 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.

8.5.2 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.

Section 9
PRIVACY AND SECURITY OF PATIENT DATA

9.1 Compliance with Policies and Procedures. IEHIE and each Participant shall comply with the standards for the privacy and security of patient health information, including without limitation protected health information described in HIPAA and HITECH, and medical information described in the CMIA, the Policies and Procedures of the California Interoperability Committee, and the IEHIE Policies and Procedures and CTEN Policies, which are incorporated herein by reference. When in conflict, the requirements of the CTEN Policies shall have precedent.

9.2 Reporting of Breaches and Security Incidents.

9.2.1 Without limiting any Business Associate Agreement entered into pursuant to Section 10 (Business Associate Agreement), IEHIE and Participant shall report to the other any use or disclosure of Patient Data not provided for by these Terms and Conditions of which IEHIE or Participant becomes aware, any security incident (other than an Unsuccessful Security Incident) concerning electronic Patient Data and any Breach of Privacy or Security. This report shall be made without unreasonable delay and in no case later than two (2) days.

9.2.2 Reporting Unsuccessful Security Incidents. The Participant shall annually provide a report to IEHIE describing in summary form the nature and extent of Unsuccessful Security Incidents concerning Patient Data or the Participant's access or use of the System or the Services experienced by the Participant during the period covered by that report, as more specifically described in the Policies and Procedures.

Section 10
BUSINESS ASSOCIATE AGREEMENT

If, pursuant to the applicable Participation Agreement, the IEHIE is to act as the business associate (as defined by HIPAA) of the Participant, the IEHIE shall enter into a Business Associate Agreement with that Participant in the form attached hereto as Exhibit A (Business Associate Agreement).

Section 11

IEHIE'S OPERATIONS AND RESPONSIBILITIES

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

11.2 Participation Agreements. IEHIE shall require that all Participants enter into a Participation Agreement or another legally binding agreement to comply with the Terms and Conditions in accordance with Section 2.4.5 (Effect of Terms and Conditions and Policies and Procedures Upon Participation Agreements). Without limiting Section 2.4.4 (Approval or Disapproval of Applications for Participation Agreements), IEHIE shall enter into Participation Agreements only with those parties that satisfy the requirements for participation set forth in the Policies and Procedures.

11.3 Monitoring of Participants. IEHIE shall regularly monitor Participant's compliance with the requirements for participation set forth in the Policies and Procedures.

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

11.5 Training. IEHIE shall provide training to IEHIE staff in the requirements of applicable laws and regulations governing the privacy and security of protected health information, including without limitation requirements imposed under HIPAA and other Federal and California law. IEHIE shall provide administrative-level training to the Participant's Authorized User regarding access and use of the System and Services, including such user manuals and other resources IEHIE determines appropriate to support the System and Services, as outlined and attached hereto as Exhibit B (Exchange Overview).

11.6 Telephone and/or E-Mail Support. IEHIE shall provide, by telephone and/or e-mail, during normal business hours, support and assistance to the Participant's help desk or other facility that supports use of the System and the Services by Authorized Users.

11.7 Access to Patient Data. IEHIE shall permit access to Patient Data maintained by IEHIE only by Participants and other parties authorized by the Data Provider that provided that Patient Data, and only in compliance with the Policies and Procedures.

11.8 Other Activities. IEHIE shall perform the other activities, including without limitation any additional services or functions involving the System, the Services and/or Patient Data, whether performed for Participants and/or other parties, as and to the extent described in the Policies and Procedures.

Section 12 GOVERNANCE

12.1 IEHIE Governing Council Composition. IEHIE has established and maintains a Board of Directors (the “Governing Council”) composed of at least sixteen (16) members, including four hospital seats; four physician seats; one public health seat; two Board of Supervisors seats (one each for Riverside and San Bernardino counties); one seat for the Local Extension Center (Inland Empire EHR Resource Center) and a HIE Partner seat for each active HIE Partner. Governing Council members must have decision making authority within their organization and are elected to a term of service of three (3) years.

12.2 Meetings and Responsibilities of Governing Council. The Governing Council shall meet at least four (4) times per calendar year to consider and resolve various issues pertaining to the use of the System and the Services by Participants, including but not limited to, oversight of systems, data security, technology integration, and approving changes to Policies and Procedures.

12.3 Governing Council Bylaws. The Governing Council has adopted bylaws for the conduct of its meetings and other proceedings. Without limiting the generality of the foregoing, the Bylaws shall provide procedures and rules concerning how the Governing Council shall call and conduct its meetings and take action.

Section 13 FEES AND CHARGES

13.1 Agreed-Upon Fees. The Participant shall pay the fees and charges described in Exhibit C (Fees and Payments).

13.2 Service Fees. The Participant shall pay Service Fees to IEHIE, in accordance with Exhibit C, which is based on IEHIE's Fee Schedule, as of the date of negotiation of this Agreement.

13.3 Changes to Fee Schedule. IEHIE may change its Fee Schedule at any time upon thirty (30) days prior written notice to Participants. Such changes shall apply to services conducted thereafter.

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

13.5 Payment. The Participant shall pay all Service Fees and any Miscellaneous Charges within forty-five (45) days following the due date of the invoice by IEHIE sent to the Participant's address as shown in IEHIE's records or e-mailed in accordance with the Participant's Participation Agreement. Fees shall be paid annually.

13.6 Late Charges. Service Fees and Miscellaneous Charges not paid to IEHIE within sixty (60) 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 ½%) per month on the outstanding balance, or the highest amount permitted by law, whichever is lower.

13.7 Suspension of Service. Failure to pay Service Fees and Miscellaneous Charges within ninety (90) 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 thirty (30) days prior notice.

13.8 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 IEHIE's net income) that IEHIE 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.

13.9 Other Charges and Expenses. 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 14

PROPRIETARY AND CONFIDENTIAL INFORMATION

14.1 Scope of Proprietary and Confidential Information. In the performance of their respective responsibilities pursuant to the Terms and Conditions, IEHIE 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 IEHIE 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 any information that:

- (a) Is in the public domain;
- (b) Is already known or obtained by any other party other than in the course of the other party’s performance pursuant to the 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;
- (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 the Terms and Conditions, or any other confidentiality or nondisclosure agreement by such other party; and/or
- (e) Is Patient Data.

14.2 Nondisclosure of Proprietary and Confidential Information. IEHIE and the Participant each (i) shall 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 the Terms and Conditions; (ii) shall not use, reproduce, distribute or disclose any such Proprietary and Confidential Information except as permitted by the Terms and Conditions; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure.

14.3 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 could 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 seek equitable relief in to prevent a breach of this Section 14 (Proprietary and Confidential Information) and such equitable relief is in addition to any other rights or remedies available to the Disclosing Party.

14.4 Notice of Disclosure. Notwithstanding any other provision hereof, nothing in this Section 14 (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 or order of a court, administrative agency or other governmental body of competent jurisdiction, 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 or order of any court, administrative agency or other governmental body of competent jurisdiction.

Section 15

DISCLAIMERS, EXCLUSIONS OF WARRANTIES, LIMITATIONS OF LIABILITY, AND INDEMNIFICATION

15.1 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 IEHIE’s control. IEHIE 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.

15.2 No Warranties. Except as provided in this Agreement, 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 IEHIE 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 IEHIE has been apprised of the possibility or likelihood of such damages occurring. IEHIE disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

15.3 Other Participants. By using the System and the Services, each 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 and Procedures, concerning use of the information; however, the actions of such other parties are beyond the control of IEHIE. Accordingly, IEHIE 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.

15.4 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.

15.5 Unauthorized Access; Lost or Corrupt Data. IEHIE 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. IEHIE is not responsible for the content of any information transmitted or received through IEHIE's provision of the Services.

15.6 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 IEHIE. 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. IEHIE neither initiates the transmission of any data nor monitors the specific content of data being transmitted. Without limiting any other provision of the Terms and Conditions, IEHIE 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 the Terms and Conditions.

15.7 Patient Care. Without limiting any other provision of the 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 claims against IEHIE 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 thereby.

15.8 Limitation of Liability. Notwithstanding anything in the Terms and Conditions to the contrary, to the maximum extent permitted by applicable laws, the aggregate liability of IEHIE, and IEHIE'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 the Terms and Conditions for the six (6) month period preceding the event first giving rise to the claim.

Section 16
INSURANCE AND INDEMNIFICATION

16.1 Insurance. The Participant shall obtain and maintain insurance coverage in accordance with the Policies and Procedures, which is incorporated herein by reference. In addition, Participant requires IEHIE to maintain the insurance requirements identified in Exhibit D (Participant Insurance Requirements of IEHIE).

16.2 Indemnification, Generally. IEHIE and each Participant (each, an “Indemnifying Party”) each shall indemnify the other and 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 the act or omission of the Indemnifying Party or any of the Indemnifying Party’s Authorized Users, members, agents, staff, or employees, including the Indemnifying Party’s failure to comply with or perform its obligations under the applicable Participation Agreement.

16.3 Privacy and Security Breaches. Notwithstanding Section 16.2 (Indemnification, Generally), IEHIE and each Participant (each, an “Indemnifying Party”) each 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.

16.4 Rules for Indemnification. Any indemnification made pursuant to the 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 17

TRANSPARENCY, OVERSIGHT, ENFORCEMENT, AND ACCOUNTABILITY

17.1 Transparency. IEHIE 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 and Procedures.

17.2 Oversight. The Governing Council shall review and prepare periodic reports to IEHIE 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 Terms and Conditions and /or Policies and Procedures regarding the privacy and security of Patient Data.

17.3 Enforcement and Accountability. Any Participant may, based upon a finding of the Governing Council with respect to another Participant's failure to comply with the Terms and Conditions and/or the Policies and Procedures, temporarily or permanently suspend the sharing of Patient Data with that other Participant, upon giving notice to IEHIE and the other Participant, and an opportunity to the other Participant to cure the non-compliance or provide other information regarding same as described in the Policies and Procedures.

Section 18
MISCELLANEOUS PROVISIONS

18.1 Applicable Law. The interpretation of the Terms and Conditions and the resolution of any disputes arising under the 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 the Terms and Conditions or a Participation Agreement, the venue of such action shall be exclusively in Fresno County, in the State of California. Prior to bringing an action regarding a dispute under this Agreement, the Parties shall meet and confer in a good faith attempt to resolve the dispute.

18.2 Non-Assignability. No rights of the Participant under its Participation Agreement may be assigned or transferred by the Participant, either voluntarily or by operation of law, without the prior written consent of IEHIE, which it may withhold in its sole discretion.

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

18.4 Supervening Circumstances. Neither the Participant nor IEHIE 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: (a) severe weather and storms; (b) earthquakes or other natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control. This Section 18.4 (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.

18.5 Severability. Any provision of the 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 the Terms and Conditions or such Participation Agreement, and such other provisions shall remain in full force and effect.

18.6 Notices. Any and all notices required or permitted under the Terms and Conditions shall be sent by United States mail, overnight delivery service, or facsimile transmission to the address provided by the Participant to IEHIE or such different addresses as a party may designate in writing. If the Participant has supplied IEHIE with an electronic mail address, IEHIE may give notice by email message addressed to such address; provided that if IEHIE receives notice that the email message was not delivered, it shall give the notice by United States mail, overnight delivery service, or facsimile. Notices shall be mailed to the following addresses:

If to Participant:

County of Fresno
Attention: Contracts Section – 6th Floor
Department of Public Health
P.O. Box 11867
Fresno, California 93775

If to IEHIE:

Inland Empire Health Information Exchange
3993 Jurupa Ave.
Riverside, CA 92506

18.7 Waiver. No provision of the 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 a consent to, waiver of, or excuse for any other different or subsequent breach.

18.8 Independent Contractors. In the performance of their respective responsibilities under any Participation Agreement, IEHIE 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.

18.9 Complete Understanding. With respect to any Participant Participation Agreement made pursuant to the Terms and Conditions, that Agreement and the Terms and Conditions together contain the entire understanding of the parties, and there are no other written or oral understandings or promises between the parties with respect to the subject matter of any Participation Agreement other than those contained or referenced in that Participation Agreement. All modifications or amendments to any Participation Agreement shall be in writing and signed by all parties.

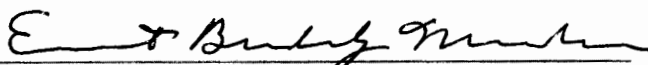
18.10 Addendums. Incorporated within the Terms and Conditions of this Agreement, and attached hereto, are Exhibit A (Business Associate Agreement), Exhibit B (Exchange Overview), and Exhibit C (Fees and Payments). Additional Terms and Conditions to this Agreement may be set forth as addendums, which will be agreed upon by both Parties, and attached hereto and incorporated by reference.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement
as of the day and year first hereinabove written.

CONTRACTOR

COUNTY OF FRESNO

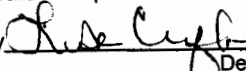

(Authorized Signature)


Ernest Buddy Mendes, Chairman,
Board of Supervisors


Dolores Green
EXECUTIVE DIRECTOR
3993 JURUPA AVENUE
RIVERSIDE, CA 92506
Mailing Address

ATTEST:

BERNICE E. SEIDEL, Clerk
Board of Supervisors

By  Deputy

DATE: September 1, 2016

DATE: October 11, 2016

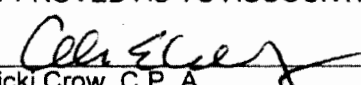
REVIEWED & RECOMMENDED FOR APPROVAL


David Pomaville, Director,
Department of Public Health

APPROVED AS TO LEGAL FORM


Daniel C. Cederborg,
County Counsel

APPROVED AS TO ACCOUNTING FORM


Vicki Crow, C.P. A.
Auditor-Controller/Treasurer-Tax Collector

FOR ACCOUNTING USE ONLY:

ORG No.: 56201621
Account No.: 7295
Requisition No.:

Exhibit A

BUSINESS ASSOCIATE AGREEMENT

Inland Empire E.H.R Resource Center, a California 501(c)(3) nonprofit corporation, on behalf of the Inland Empire Health Information Exchange (“Business Associate”), and the Participant identified on the Signature Page hereof (“Covered Entity”), hereby agree to the following terms and conditions of this Business Associate Agreement (the “Business Associate Agreement”).

Recitals

- A. Covered Entity is a “covered entity” (as defined in HIPAA).
- B. Covered Entity and Business Associate have entered into one (1) or more agreements (collectively, the “Participation Agreement”) pursuant to which Business Associate provides to Covered Entity certain services that now or in the future shall include, other than in the capacity of a member of the workforce of Covered Entity, the creation, receipt, maintenance and/or transmission of “protected health information” (as defined in HIPAA), on behalf of Covered Entity, for a function or activity regulated by HIPAA. Business Associate therefore shall act as a “business associate” (as defined in HIPAA) with respect to Covered Entity.
- C. Covered Entity and Business Associate accordingly have agreed to enter into the following terms and conditions.

Agreement

In consideration of the foregoing recitals and the promises set forth herein, the parties agree as follows:

1. Definitions. For the purposes of this Business Associate Agreement, the term “HIPAA” means the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. Parts 160, 162 and 164), as in effect from time to time. All terms used in this Business Associate Agreement not specifically defined otherwise shall have the same definitions as given to them under HIPAA; provided, however, that the term “PHI” shall refer only to protected health information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity.

2. Obligations of Business Associate.

(a) Compliance with Regulatory Obligations of Business Associate. Without limiting any other provision of this Business Associate Agreement, Business Associate shall perform and comply with all the applicable obligations and requirements imposed upon business associates pursuant to HIPAA [Reference: 45 C.F.R. § 164.314(a)(2)(i)(A)].

(b) Permitted Use and Disclosure of PHI. Business Associate shall use and disclose PHI only as necessary to perform Business Associate’s obligations, functions, activities and/or

services under the Participation Agreement, or as otherwise permitted or required by this Business Associate Agreement, or as otherwise permitted by HIPAA, including without limitation 45 C.F.R. § 164.502(b) with respect to the minimum necessary use and disclosure of PHI, or required by law. Except as expressly permitted by this Business Associate Agreement, Business Associate shall not use or disclose PHI in any manner that would violate the requirements of HIPAA if done by Covered Entity. [Reference: 45 C.F.R. §§ 164.502(a)(3) & 164.504(e)(2)(i) & 45 C.F.R. § 164.504(e)(2)(ii)(A)].

(c) Specified Permitted Uses of PHI. Without limiting the generality of Section 2(b) (Permitted Use and Disclosure of PHI), Business Associate may use PHI as follows, if necessary:

(i) For the proper management and administration of Business Associate [Reference: 45 C.F.R. § 164.504(e)(2)(i)(A) & 45 C.F.R. § 164.504(e)(4)(i)(A)].

(ii) To carry out the legal *responsibilities* of Business Associate [Reference: 45 C.F.R. § 164.504(e)(4)(i)(B)].

(iii) To provide data aggregation services relating to the health care operations of Covered Entity if and to the extent *provided* by the Participation Agreement [Reference: 45 C.F.R. § 164.504(e)(2)(i)(B)].

(d) Specified Permitted Disclosures of PHI. Without limiting the generality of Section 2(b) (Permitted Use and Disclosure of PHI), Business Associate may disclose PHI as follows:

(i) For the proper management and administration of Business Associate [Reference: 45 C.F.R. § 164.504(e)(2)(i)(A)] or to carry out the legal responsibilities of Business Associate [Reference: 45 C.F.R. § 164.504(e)(4)(i)(B)] if:

(A) If the disclosure is required by law [Reference: 45 C.F.R. § 164.504(e)(4)(ii)(A)]; or

(B) If Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person [Reference: 45 C.F.R. § 164.504(e)(4)(ii)(B)(1)], and if the person promptly notifies Business Associate of any instances in which it is aware in which the confidentiality of the information has been breached [Reference: 45 C.F.R. § 164.504(e)(4)(ii)(B)(ii)].

(e) Safeguards. Business Associate shall use appropriate safeguards and comply, where applicable, with 45 C.F.R. §§ 164.302 through 164.316 with respect to electronic PHI, to prevent use or disclosure of the information other than as provided for by this Business Associate Agreement [Reference: 45 C.F.R. §§ 45 C.F.R. § 164.314(a)(2)(i)(A) & 164.504(e)(2)(ii)(B)]. Without limiting the generality of the foregoing Business Associate shall appropriately safeguard electronic PHI by implementing administrative safeguards in accordance with 45 C.F.R. § 164.308 [Reference: 45 C.F.R. § 164.308(b)(1)].

(f) Reporting Unauthorized Uses and Disclosures. Business Associate shall report to Covered Entity, without unreasonable delay, and in no cases later than two (2) calendar days from discovery of the breach, any use or disclosure of PHI not permitted by this Business Associate Agreement of which Business Associate becomes aware, including without limitation any security incident involving electronic PHI and any breach of unsecured PHI as required by 45 C.F.R. § 164.410 [Reference: 45 C.F.R. §§ 164.314(a)(2)(C) & 164.504(e)(2)(ii)(C)]. Without limiting the generality of the foregoing:

(i) Notwithstanding anything to the contrary in this Section 2(f) (Reporting Unauthorized Uses and Disclosures), Business Associate shall report to Covered Entity on a regular and periodic basis the ongoing existence and occurrence of Unsuccessful Security Incidents (as defined below). The parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of unsuccessful Security Incidents, for which no additional notice shall be required. For purposes of this Business Associate Agreement, the term “Unsuccessful Security Incident” shall mean any security incident that does not result in any unauthorized access, use or disclosure of electronic PHI, including without limitation, activity such as pings and other broadcast attacks on a firewall, port scans, unsuccessful log-on attempts, denial of service and any combination of the above.

(ii) Except in the event of a law enforcement delay, Business Associate shall report the information described below to Covered Entity without unreasonable delay, and in no case more than two (2) calendar days following discovery of a breach of unsecured PHI. Such notice shall include, to the extent possible:

(A) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the breach;

(B) The date of the breach;

(C) The date of the discovery of the breach;

(D) A description of the types of unsecured PHI that were involved;
and

(E) Any other details necessary to complete an assessment of the risk that the PHI has been compromised.

[Reference: 45 C.F.R. §§ 164.410 & 164.404(c).]

(g) Arrangements with Subcontractors. Business Associate shall enter into a business associate agreement with any subcontractor of Business Associate that creates, receives, maintains, or transmits PHI on behalf of Business Associate, pursuant to which the subcontractor shall agree to comply with the applicable requirements of HIPAA and the same restrictions and conditions that apply to Business Associate with respect to that PHI pursuant to this Business Associate Agreement, and pursuant to which Business Associate shall obtain satisfactory

assurances that the subcontractor shall appropriately safeguard that PHI [References: 45 C.F.R. § 164.308(b)(2), 45 C.F.R. § 164.314(a)(2)(i)(B) & 45 C.F.R. § 164.504(e)(2)(ii)(D)].

(h) Individuals' Access to PHI. If and to the extent that Business Associate maintains PHI in a designated record set, Business Associate shall upon request by Covered Entity make that PHI available to Covered Entity within thirty (30) calendar days as and to the extent required for Covered Entity's compliance with its obligations to provide individuals with access to and copies of PHI pursuant to 45 C.F.R. § 164.524. If Business Associate receives an individual's request for access to PHI, Business Associate shall forward that request to Covered Entity within five (5) calendar days. Covered Entity shall be responsible for making all determinations regarding the granting or denial of an individual's request, and for notifying individuals thereof, and Business Associate shall not make any such determinations or notifications [*Reference: 45 C.F.R. §§ 164.502(a)(4)(ii) & 164.504(e)(2)(ii)(E)*].

(i) Amendments to PHI. If and to the extent that Business Associate maintains PHI in a designated record set, Business Associate shall upon request by Covered Entity make that PHI available to Covered Entity within thirty (30) calendar days for amendment, and shall promptly incorporate any amendments to PHI directed by Covered Entity, as and to the extent required for Covered Entity's compliance with 45 C.F.R. § 164.526. If Business Associate receives an individual's request for an amendment to PHI, Business Associate shall forward that request to Covered Entity within five (5) calendar days. Covered Entity shall be responsible for making all determinations regarding the granting or denial of an individual's request, and for notifying individuals thereof, and Business Associate shall not make any such determinations or make any such amendments except as directed by Covered Entity [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(F)*].

(j) Accountings of Disclosures. Business Associate shall document disclosures of PHI as required to provide Covered Entity with information sufficient to respond to any request by an individual for an accounting of disclosures in compliance with 45 C.F.R. § 164.528, and shall provide such information to Covered Entity upon request within thirty (30) calendar days. If Business Associate receives an individual's request for an accounting of disclosures, Business Associate shall forward that request to Covered Entity within thirty (30) calendar days. Covered Entity shall be responsible for providing all accountings of disclosures to individuals, and Business Associate shall not provide any such accountings to individuals directly [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(G)*].

(k) Other Obligations. To the extent that Business Associate is, pursuant to the Participation Agreement or this Business Associate Agreement, responsible to carry out an obligation of Covered Entity under HIPAA, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of that obligation [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(H)*].

(l) Books and Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the U.S. Secretary of Health & Human Services for purposes of determining Covered Entity's or Business Associate's compliance under HIPAA [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(I)*]. Without limiting the

generality of the foregoing, Business Associate shall disclose PHI when required by the U.S. Secretary of Health & Human Services under Subpart C of 45 C.F.R. Part 160 to investigate or determine Business Associate's compliance with HIPAA [*Reference: 45 C.F.R. § 164.502(a)(4)(i)*].

3. Covered Entity's Obligations.

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

(b) Notice of Change in Permissions. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Notice of Change in Use. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) Appropriate Requests. Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

4. Term and Termination.

(a) Term. Subject to the other provisions of this Section 4 (Term and Termination), the term of this Business Associate Agreement shall be coextensive with that of the Participation Agreement.

(b) Termination. If Covered Entity knows of a pattern of activity or practice by Business Associate that constitutes a material breach or violation of Business Associate's obligations under HIPAA or this Business Associate Agreement, and after taking reasonable steps to cure that breach have been unsuccessful, Covered Entity may terminate this Business Associate Agreement and the Participation Agreement, if feasible, subject to and in accordance with the terms and conditions of Section 3.5 of the Participation Agreement [*Reference: 45 C.F.R. §§ 164.504(e)(1)(ii) & 164.504(e)(2)(iii)*].

(c) Breach Pattern of Practice by Covered Entity. If Business Associate knows of a pattern of activity or practice by Covered Entity that constitutes a material breach or a violation of Covered Entity's obligations under HIPAA or this Business Associate Agreement, and after taking reasonable steps to cure that breach have been unsuccessful, Business Associate may terminate this Business Associate and the Participation Agreement, if feasible, subject to and in accordance with the terms and conditions of Section 3.4 of the Participation Agreement.

(d) Conduct Upon Termination. Upon termination or expiration of this Business Associate Agreement, Business Associate shall, at Covered Entity's written direction, either

destroy or return to Covered Entity all PHI in Business Associate's possession and/or in the possession of any subcontractor of Business Associate, and shall not retain any copies of such PHI; provided, however, that Business Associate and/or Business Associate's subcontractor may retain PHI as and to the extent necessary, and only for so long as necessary, for Business Associate or that subcontractor to continue its proper management and administration or to carry out its legal responsibilities. In the event that return or destruction of PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction of the PHI not feasible, and Business Associate shall extend the protections of this Business Associate Agreement, including without limitation Section 2(e) (Safeguards), to such PHI that is not returned or destroyed, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for as long as Business Associate or any subcontractor of Business Associate maintains such PHI. If PHI is to be destroyed pursuant to this Section 4(d), Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(J)*].

5. Relationship to Participation Agreement. In the event that a provision of this Business Associate Agreement is contrary to a provision of the Participation Agreement pertaining to Business Associate's performance of its obligations as a business associate, the provisions of this Business Associate Agreement shall control.

6. Amendment. The parties agree to take such action from time to time as is necessary to amend this Agreement for Covered Entity and Business Associate to comply with HIPAA or other applicable law. The parties agree that this Agreement may only be modified by mutual written amendment, signed by both parties, effective on the date set forth in the amendment.

7. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA.

8. No Third Party Beneficiaries. Unless otherwise set forth herein, nothing contained herein is intended nor shall be construed to create rights running to the benefit of third parties.

9. Waiver. Any failure of a party to insist upon strict compliance with any term, undertaking or condition of this Agreement shall not be deemed to be a waiver of such term, undertaking or condition. To be effective, a waiver must be in writing, signed and dated by the parties to this Agreement.

10. Counterparts. This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed one and the same instrument. Any photocopy of this executed Agreement may be used as if it were the original.

11. Governing Law. Notwithstanding any other provision to the contrary, this Agreement shall be governed and construed in accordance with the laws of the State of California.

Signature Page Follows

BUSINESS ASSOCIATE AGREEMENT

Signature Page

In witness whereof, Covered Entity and Business Associate have entered into this Agreement as of the Effective Date of the Participation Agreement.

“Covered Entity”

County of Fresno
1221 Fulton Mall
Fresno, CA 93721

“Business Associate”

Inland Empire E.H.R. Resource Center, a
California 501(c)(3) nonprofit corporation, on
behalf of the Inland Empire Health Information
Exchange (“IEHIE”) project.

3993 Jurupa Avenue
Riverside, CA 92506

By: Ernest Buddy Mendes

Name: Ernest Buddy Mendes

Title: Chairman Board of Supervisors

Date: October 11, 2014

By: Dolores Green

Name: Dolores Green

Title: Chief Executive Officer

Date: 9/1/12

ATTEST:

BERNICE E. SEIDEL, Clerk
Board of Supervisors

By: Bernice E. Seidel
Deputy

Exhibit B

Inland Empire Health Information Exchange

EXCHANGE OVERVIEW

Inland Empire E.H.R. Resource Center, a California 501(c)(3) nonprofit corporation, on behalf of the Inland Empire Health Information Exchange (“IEHIE”), provides or arranges for the provision of data transmission and related services to allow Participants to conduct searches for Patient Data, and to exchange Patient Data identified from those searches, from a centralized data repository that includes stakeholder oversight from community participants (“System & Services”). The System & Services are governed by the stakeholder Participants and is not owned by one entity. The System & Services have contracted with Orion Health Systems to provide community Participants the ability to securely access Patient Data at the point of care for treatment of patients in the System & Services.

Participant is accessing the System & Services through participation in CVHIE.

1. IEHIE BASE FEATURES

(a) **COMPREHENSIVE PATIENT INFORMATION FROM A SINGLE LOCATION**
Secure, online access to patient records for all authorized healthcare providers.

(b) **WEB-BASED CLINICAL PORTAL**
Access a complete patient record which displays important and clinically relevant information. Clinical Portal integrates directly with your existing EMR so you can get up and running quickly.

(c) **ORION HEALTH® PATIENT PORTAL**
Provides patients with 24x7 access to their patient record, so they can become an integral part of the care process and are more engaged in their own care management.

(d) **CLINICAL TIMELINE VIEW**
Provides a graphical representation of all patient encounters over the course of an entire patient history. Clinicians can quickly select and drill into a period of time and view complete details of the patient results.

(e) **USER-SUBSCRIBED NOTIFICATIONS**
Customizable notifications to suit a provider’s specific care setting, specialty or practices by deciding what information they get, and when and how they get it.

(f) **FLEXIBLE PRIVACY AND CONSENT**
A flexible, rules-based privacy solution allows access based on multiple criteria, including support for Opt-In, Opt-Out, relationship, location- and age-based privacy, as well as regulations surrounding minors and sexual and mental health.

(g) **ROBUST SECURITY**
With support for two-form factor authentication where required, the Orion Health security model can be tailored to provide specialized access to all roles - from clinical users to administrators and IT staff.

(h) STANDARDS-BASED

HIE standards for cross enterprise document sharing have been widely adopted and present a standards-based approach. Our solution shares a continuity of care document (CCD) formed from the content contained in the HIE's clinical document repository, ensuring standards compliant systems can integrate with non-compliant systems via the HIE's technology.

(i) CONTINUITY OF CARE EXCHANGE

Provides the generation and exchange of CCD (HITSP C32 CCD) and allows these documents to be shared with other organizations. Through Orion Health Direct Secure Messaging, the CCD can be exchanged with anyone with a "Direct" account. Also with one click, the CCD can be seamlessly transmitted and retained within your EMR.

(j) MASTER PATIENT INDEX

Links identifiers for the same patient from different organizations and facilitates the aggregation of the complete patient record.

(k) MOBILE ACCESS

Accessible from any secure, web-enabled workspace as well as an iPad for improved mobility and remote access for the user.

(l) ORION HEALTH® ORDERS

Enables clinicians to rapidly create and send individual or sets of electronic orders for radiology and laboratory tests, allied health and ancillary services.

(m) ORION HEALTH® PROBLEM LIST

Allows clinicians to update, manage and change a patient's problem list in a single view through Orion Health Clinical Portal. Provides accurate and up-to-date decision support.

2. IEHIE BASE SERVICES

(a) TRAINING

Provides one-time initial training for "train the trainer" and one-time training for physician staff. Provide training materials to support each session and as future reference.

(b) HELP DESK

For our direct participants, IEHIE will provide second level support to end user and first level support administrative staff, once the system is considered in production.

(c) SUPPORT

- IEHIE will provide Help Desk support, available by phone 8-5 M-F, and email.
- IEHIE will provide disciplines to each statement of work: project management, interface development and business analyst operations support.

(d) AUDITING

Conduct routine auditing of HIE usage for purposes of compliance with HIE policies and HIPAA-related compliance

(e) PRODUCTION STANDING OPERATING PROCEDURES

- Nextgate EMPI maintenance: Enterprise Master Patient Index required monitoring and maintenance to address orphan records
- Consent (opt-in and opt-out) audit processing (ad-hoc)
- Validation of portal access and functionality
- Monitoring of interfaces (queue size, activity, up time and processing)
- Managing of schedules processes (file feeds)
- State base reporting exception handling management
- Communication for scheduled downtime and maintenance
- System health monitoring
- Issue management

(f) BASE ARTIFACTS FOR CONSENT PROCESSING

IEHIE will provide materials that can help with consent management for patients

3. IEHIE ADDITIONAL FEATURES (SUBJECT TO ADDITIONAL FEES)

(a) ORION HEALTH® CARE PATHWAYS

Manage long-term conditions with confidence, improving population health and efficiency of healthcare. Healthcare Pathways coordinates patient care across all settings, using defined clinical pathways, giving all care providers the knowledge to improve patient outcomes regardless of where the patient is treated.

(b) ORION HEALTH® PUBLIC HEALTH REPORTING

Orion Health Collaborative Care can automate the process of alerting public health authorities of specific health conditions and cases. Our HIE integrates directly with local public health systems to provide timely and accurate reporting for facilities connected to the exchange. Nearly all state health departments use Orion Health Rhapsody Integration Engine for their secure exchange needs, so our HIE can enable your organization to quickly and efficiently begin interacting with them.

- California Reportable Diseases Information Exchange (CalREDIE)
- Regional Immunization Data Exchange (RIDE)
- California Immunization Registry (CAIR)

(c) ORION HEALTH® DIRECT SECURE MESSAGING

When integrated with Orion Health Collaborative Care, Direct Secure Messaging allows HIE participants to securely share patient summaries with providers and specialists who are not currently HIE participants. Orion Health offers Healthcare Information Service Provider (HISP) and certificate management services for HIE participants to encourage participation in these national standards.

(d) ORION HEALTH® EXCHANGE GATEWAY

Enables the HIE to connect to the Nationwide Health Information Network (NwHIN) so HIE users can query federal organizations and other HIEs, and vice versa.

(e) ORION HEALTH® BUSINESS INTELLIGENCE

Provides standard or additional reports to trend population growth, condition growth or healthcare consumption growth over time.

4. IEHIE ADDITIONAL SERVICES (SUBJECT TO ADDITIONAL FEES)

(a) TRAINING

IEHIE can provide additional training of users to support all user levels (1-7).

(b) TECHNICAL SERVICES

IEHIE can provide technical assistance with experts in the field of message types and interfaces to assist participants that may require additional support.

Exhibit C

Inland Empire Health Information Exchange

FEES AND PAYMENTS

In order to access the System & Services, Participant agrees to pay System & Services the applicable subscription fees specified below, plus any applicable Taxes, within forty-five (45) days of receipt of an invoice from the Exchange.

1. Fee Schedule. The subscription fees are described below and are subject to the Terms and Conditions of Section 13 (Fees and Charges) of the Participation Agreement. Implementation and Annual Fees include all Fresno County public health, behavioral health, and EMS entities.

County Population	Implementation Fees	Annual Fees Year 1	Annual Fees Year 2	Annual Fees Year 3	Annual Fees Year 4	Annual Fees Year 5
972,000	\$ 7,500	\$20,000	\$20,000	\$20,000	\$20,000	\$20,000

Fees by County Population			
Minimum	Maximum	Implementation Fee	Annual Fee
1	199,999	\$5,000	\$10,000
200,000	699,999	\$5,000	\$15,000
700,000	1,199,999	\$7,500	\$20,000
1,200,000	1,499,999	\$15,000	\$35,000
1,500,000	1,999,999	\$25,000	\$50,000
2,000,000	3,000,000	\$30,000	\$75,000
3,000,000	4,999,999	\$50,000	\$150,000
5,000,000	15,000,000	\$100,000	\$300,000

1.1 Implementation Fees. Non-reoccurring start-up fee which is design to cover all costs related to technical implementation of data exchange and query. There are no Implementation Fees associated with this Agreement. Any technical services requested in addition to the existing infrastructures of a Participant's facilities may be subject to an additional fee, and will be included in this Agreement as an addendum and signed by both parties.

1.2 Annual Fees. Annual Fees are kept minimal and support the continuing nonprofit goals and objectives of the IEHIE, their Participants, and similarly situated data exchange entities across the state and across the nation.

2. Termination Fees. There are no termination fees associated with this Agreement.

Exhibit D

Inland Empire Health Information Exchange

PARTICIPANT INSURANCE REQUIREMENTS OF IEHIE

Without limiting the COUNTY's right to obtain indemnification from IEHIE or any third parties, IEHIE, at its sole expense, shall maintain in full force and effect the following insurance policies throughout the term of this Agreement:

A. Commercial General Liability. Commercial General Liability Insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence and an annual aggregate of Two Million Dollars (\$2,000,000). This policy shall be issued on a per occurrence basis. COUNTY may require specific coverage including completed operations, product liability, contractual liability, Explosion, Collapse, and Underground (XCU), fire legal liability or any other liability insurance deemed necessary because of the nature of the Agreement.

B. Automobile Liability. Comprehensive Automobile Liability Insurance with limits for bodily injury of not less than Two Hundred Fifty Thousand Dollars (\$250,000) per person, Five Hundred Thousand Dollars (\$500,000) per accident and for property damages of not less than Fifty Thousand Dollars (\$50,000), or such coverage with a combined single limit of Five Hundred Thousand Dollars (\$500,000). Coverage should include owned and non-owned vehicles used in connection with this Agreement.

C. Professional Liability. If IEHIE employs licensed professional staff (e.g. Ph.D., R.N., L.C.S.W., M.F.C.C.) in providing services, Professional Liability Insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence, Three Million Dollars (\$3,000,000) annual aggregate.

D. Worker's Compensation. A policy of Worker's Compensation Insurance as may be required by the California Labor Code.

E. IEHIE shall obtain endorsements to the Commercial General Liability insurance naming the County of Fresno, its officers, agents, and employees, individually and collectively, as additional insured, but only insofar as the operations under this Agreement are concerned. Such coverage for additional insured shall apply as primary insurance and any other insurance, or self- insurance, maintained by the COUNTY, its officers, agents and employees shall be excess only and not contributing with insurance provided under the IEHIE's policies herein. This insurance shall not be cancelled or changed without a minimum of thirty (30) days advance written notice given to COUNTY.

F. Within thirty (30) days from the date IEHIE executes this Agreement,

IEHIE shall provide certificates of insurance and endorsements as stated above for all of the foregoing policies, as required herein, to:

County of Fresno
Attention: Contracts Section – 6th Floor
Department of Public Health
P.O. Box 11867
Fresno, California 93775

IEHIE shall certify that such insurance coverage have been obtained and are in full force; that the County of Fresno, its officers, agents and employees will not be responsible for any premiums on the policies; that such Commercial General Liability insurance names the County of Fresno, its officers, agents and employees, individually and collectively, as additional insured, but only insofar as the operations under this Agreement are concerned; that such coverage for additional insured shall apply as primary insurance and any other insurance, or self-insurance, maintained by the COUNTY, its officers, agents and employees, shall be excess only and not contributing with insurance provided under the IEHIE's policies herein; and that this insurance shall not be cancelled or changed without a minimum of thirty (30) days advance, written notice given to COUNTY.

G. In the event IEHIE fails to keep in effect at all times insurance coverage as herein provided, the COUNTY may, in addition to other remedies it may have, suspend or terminate this Agreement upon the occurrence of such event.

H. All policies shall be with admitted insurers licensed to do business in the State of California. Insurance purchased shall be from companies possessing a current A.M. Best, Inc. rating of A FSC VII or better.

INLAND EMPIRE HEALTH INFORMATION EXCHANGE (IEHIE) POLICIES & PROCEDURES MANUAL – V2.1.2

CONTENTS

REVISION HISTORY	3
INTRODUCTION	4
EXECUTIVE SUMMARY	5
1. OPENNESS, TRANSPARENCY AND PRIVACY	6
1.1. HIE PARTICIPATION REQUIREMENTS	6
1.2. NOTICE OF PRIVACY PRACTICES	7
1.3. CLEAR NOTICE TO PARTICIPANTS	7
1.4. ACCESS TO PHI	7
1.5. DECEASED INDIVIDUALS	7
2. PURPOSE SPECIFICATION AND MINIMIZATION	8
2.1. ROLE-BASED ACCESS TO PROTECTED HEALTH INFORMATION	8
2.2. RESTRICTIONS ON ACCESS TO SENSITIVE INFORMATION	9
2.3. ACCESS TO PATIENT INFORMATION THROUGH THE “CIRCLE OF CARE”	9
3. USE LIMITATION AND DE-IDENTIFIED DATA	10
3.1. USE LIMITATION	10
3.2. DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR MARKETING PURPOSES	10
3.3. DE-IDENTIFIED DATA AND LIMITED DATA SETS	10
3.4. HEALTH PLAN PARTICIPATION	10
3.5. BEHAVIORAL HEALTH ACCESS AND USE	11
4. INDIVIDUAL PARTICIPATION AND CONTROL	12
4.1. INDIVIDUAL ACCESS TO DATA	12
4.2. CONSENT	12
5. DATA INTEGRITY, AND QUALITY	14
5.1. ROLE OF HIE PARTICIPANTS IN MAINTAINING DATA QUALITY AND INTEGRITY	14
5.2. ENCRYPTION AND PROGRAM ACCESS	14
6. ADMINISTRATION	15
6.1. ROLES AND RESPONSIBILITIES	15
6.2. BREACH NOTIFICATION POLICY	19
7. SYSTEM SUPPORT AND MAINTENANCE	22
7.1. DISASTER RECOVERY PLAN	22
7.2. DISASTER RECOVERY OBJECTIVES	22
8. SECURITY SAFEGUARDS AND ACCESS CONTROLS	23
8.1. ACCESS CONTROL POLICY	23
8.2. LOGICAL ACCESS CONTROLS	23
8.3. GRANTING OR CHANGING USER ACCESS RIGHTS AND PASSWORDS	24
9. OPERATIONAL SECURITY	25
9.1. ASSIGNING PRIVACY AND SECURITY RESPONSIBILITIES	25
9.2. ACCEPTABLE USE GUIDELINES	25
9.3. INTERNET ACCESS ACCEPTABLE USE	26
9.4. REMOTE ACCESS ACCEPTABLE USE GUIDELINES FOR NON-PARTICIPANTS	26

10.	ADMINISTRATIVE SECURITY POLICIES	28
10.1.	PRE-EMPLOYMENT BACKGROUND CHECKS	28
10.2.	PERSONNEL EDUCATION SCHEDULE.....	28
10.3.	EMPLOYMENT TERMINATION SECURITY PRACTICES	28
11.	SYSTEM AND NETWORK ADMINISTRATION AND SECURITY POLICIES	29
11.1.	INDIVIDUALS COVERED BY THIS POLICY	29
11.2.	AUDIT TRAIL SECURITY	29
11.3.	IDENTIFICATION AND AUTHENTICATION	30
11.4.	ADMINISTRATIVE ACCOUNT MANAGEMENT	30
12.	RISK MANAGEMENT REVIEWS.....	31
12.1.	MANAGEMENT AND OVERSIGHT	31
12.2.	COMPLIANCE MANAGEMENT.....	31
13.	OPERATION OF THE INCIDENT RESPONSE PLAN.....	32
	APPENDIX A – CMIA DISCLOSURE EXCEPTIONS	33
	APPENDIX B – SAMPLE NOTICE OF PRIVACY PRACTICES	37
	APPENDIX C – SAMPLE NOTICE OF PRIVACY PRACTICES (SPANISH)	39
	APPENDIX D – SAMPLE OPT-OUT REQUEST FORM.....	41
	APPENDIX E – STATEMENT OF UNDERSTANDING.....	42
	APPENDIX F – ACCESS REQUEST FORM	43
	SUPPLEMENTAL 1: CTEN POLICIES FOR DIRECT PARTICIPANTS	47
101.	PRIVACY, SECURITY AND CONFIDENTIALITY OF DIRECT SECURE MAIL	47
102.	USER IDENTITY VERIFICATION	50
103.	CTEN BREACH NOTIFICATION	53
104.	CTEN ENTERPRISE SECURITY.....	55
105.	CTEN REQUIREMENT TO RESPOND	56
106.	CTEN DUTIES WHEN SUBMITTING A MESSAGE	57
107.	CTEN APPLICABILITY OF HIPAA REGULATIONS	58
108.	CTEN AGREEMENTS WITH PARTICIPANTS	59
109.	CTEN INCOMPLETE MEDICAL RECORD.....	60
1010.	CTEN DIRECT MESSAGING CERTIFICATE VERIFICATION PROCESS	61
1011.	CTEN USE OF MESSAGE CONTENT	66
1012.	CTEN CONFIDENTIAL PARTICIPANT INFORMATION	68
1013.	CTEN SAFEGUARDS	69
1014.	DIRECT SECURE MESSAGING USER SETUP	71

Revision History

Name	Date	Reason For Changes	Version
Rich Swafford	03/20/2012	Initial, IEEHRC Board Approved	1.0
Rich Swafford	10/25/2012	Add, Sec 3, "Health Plan", "Behavioral Health" policies	1.1
Dawn Goodman	04/04/2013	Change, HITECH Act modifications	1.2
Linda Ackerman	04/04/2013	Change, HIPAA Omnibus Rule compatibility updates	1.2
Leo Pak	05/17/2015	Change, Sec 6, "ED" to "CTO"	1.3
Leo Pak	05/17/2015	Change, Sec 4, "break the glass" to "break the seal"	1.3
Lyman Dennis	10/23/2015	Add, Appx C-F, CTEN Policies for Direct	2.0
Leo Pak	01/27/2016	Change, Sec 11, 72-hour notification of terminated employees	2.0.3
Leo Pak	02/26/2016	Change, Sec 2 – Clarification of User Profiles Change, Appx F – Reflect changes to Sec 2	2.0.4
Leo Pak	03/08/2016	Add, Sec 1.1 – HIE Participation descriptions	2.1.0
Leo Pak	05/03/2016	Change, IEHIE new logo	2.1.1
Leo Pak	06/03/2016	Add, Sec 5 – Encryption procedure Change, Sec 6, 8, 9, 12 – Officer roles and responsibilities Add, Sec 7 – Disaster Recovery Plan Add, Sec 10 – Employee hiring and training practices	2.1.2

Introduction

The IEHIE Policies and Procedures govern the operation of the Inland Empire Health Information Exchange (HIE), and are specific to its function and technology. They set a minimum or base standard for participants in the IEHIE. Participants should develop their own policies and operational procedures accordingly knowing that they may exceed the IEHIE standards but not fall below them.

These policies:

- Set forth the expectations of IEHIE management for the performance, behavior, and accountability for information security and privacy in the operation of the HIE, by all employees, participants, and business associates.
- Identify policies and procedures governing the protection of protected health information (PHI) and other sensitive information whose transmission is facilitated by IEHIE.
- Establish an infrastructure and operational guidance for policy implementation, enforcement, exception handling and maintenance.
- Identify security-related roles and responsibilities.
- Supplemental IEHIE CTEN Policies (101-1014) address the requirements of the California Trusted Exchange Network (CTEN) and the California Data Use and Reciprocal Support Agreement (CalDURSA). For Direct participants, when the IEHIE CTEN Policies and the Policies and Procedures Manual are in conflict, the CTEN Policies shall take precedence.

To ensure that these policies are properly implemented, IEHIE requires all its employees, HIE participants, and business associates to be trained in:

- procedures governing protected health information (PHI);
- IEHIE procedures and requirements to maintain compliance with HIPAA Privacy and Security Rule (45 CFR Parts 160 and 164);
- 42 Code of Federal Regulations (CFR) Part 2: Substance Abuse Records;
- Welfare & Institution Code (W&I) 5328: Confidentiality of Mental Health Records; and
- all other federal and State laws and regulations pertaining to the privacy and security of personal health information exchange.

Executive Summary

These policies are organized as follows, according to recognized Fair Information Practices:

1. Openness, Transparency and Privacy

IEHIE is committed to developing and maintaining a trust relationship with individuals whose protected health information it facilitates the sharing of through its community health information exchange. In order to do this, IEHIE will be open about its information-handling practices and will strive to maintain the highest levels of privacy and security in its operations. It will also require the same or higher standards of participants in the HIE and business associates as a condition of their participation.

2 - 3. Purpose Specification, Minimization, and Data Limitations

The IEHIE will facilitate the sharing and hosting of PHI for patient evaluation and treatment purposes only, although authorized data users may subsequently use information for other legally permitted purposes, including payment and health care operations. Access to sensitive health information is role based and is granted on a need-to-know basis designed to allow access to the minimum necessary amount of data to perform assigned responsibilities. All PHI is subject to federal and state statutory and regulatory requirements, including proper legal process, and to public health exceptions. Data that has been de-identified according to HIPAA standards may be used for other purposes, subject to the strict requirements set forth in these policies.

4. Individual Participation and Control

Individuals will have the ability to opt-out of having their protected health information shared through the HIE. They will be able to request information about who has requested and received their PHI through the HIE. In the event an individual opts-out of the HIE, their information will continue to be collected and managed; however, no access will be provided to that information without the expressed consent of the individual.

5. Data Integrity and Quality

The success of the HIE depends upon its ability to provide the most complete, accurate and up-to-date information possible. IEHIE maintains the highest security standards to protect data and expects HIE participants to do the same. Participants are also responsible for the quality of data they provide to the HIE in response to user requests.

6 - 7. Organizational Administration, System Support, and Maintenance

IEHIE aspires to the highest standards of performance in the administration and management of the organization. Roles and responsibilities are assigned in order to meet the operational privacy and security requirements of the HIE and business associates.

8 - 13. Security Safeguards and Access Controls

Because safeguarding protected health information is the highest priority of IEHIE, the greater part of these Policies and Procedures is concerned with security safeguards and access controls. IEHIE maintains the best possible security technologies and procedures that are compatible with its business purpose of locating data and facilitating its exchange between providers and users.

1. Openness, Transparency and Privacy

Openness about developments, procedures, policies, technology, and practices with respect to the treatment of protected health information (PHI) is essential to protecting privacy. Individuals should be able to understand what information exists about them, how it is used, and how they can exercise reasonable control over it. Transparency encourages a commitment to strong privacy practices and instills patient confidence in the privacy of their information, which in turn increases participation in health information exchanges.

1.1. HIE Participation Requirements

Only persons who enter into Participation Agreements with IEHIE shall be permitted to access the System and use the Services. A participant must act as a Data Provider and a Data Recipient, as described in this Section 1.1.1. A participant may use some or all of the Services, as specified and in accordance with Section 1.4 (Description of Services) and Exhibit C (Fees and Payments) of that participant's Participation Agreement.

1.1.1. Participant Type

Any party may inquire to enter into a participation agreement with IEHIE. IEHIE shall not be required to approve any inquiry to be a participant. IEHIE will review all requests to join the HIE, but applicants must have a use for clinical data. The following list seeks to categorize applicants into their respective roles in the healthcare system, but is only meant to be illustrative, not exhaustive.

Examples of Participant Types include:

- a) Physician, medical group, or independent physician association;
- b) Laboratory;
- c) Hospital;
- d) Public health agency;
- e) Emergency medical services (EMS);
- f) Pharmacy; and
- g) Health plan, insurer, or other payor.

Each IEHIE participant is expected to be both a Data Recipient and a Data Provider*, and therefore subject to both provisions in Section 6 (Data Recipients' Use of System and Services) and Section 7 (Data Providers' Use of System and Services) of the IEHIE Participation Agreement.

- "Data Provider" means a participant that is registered to provide information to HIE for use through the Services. IEHIE receives labs, radiology reports, discharge summaries, consultations, electronic orders, demographic and financial data, discharge summaries, and chart notes, as well as other data types that may be deemed appropriate or necessary in the future.
- "Data Recipient" means a Participant that uses the Services to obtain health information.

*With the approval of the IEHIE Governing Council and management team, a participant may, under certain circumstances or specific use cases, be permitted to become a Data Recipient-only. Participants approved as Data Recipients-only will have their agreements reviewed from time to time, and not less than annually, to determine if it is appropriate for them to begin sharing data as Data Providers.

1.2. Notice of Privacy Practices

IEHIE will publish a Notice of Privacy Practices that meets the requirements of the HIPAA Privacy rule (45CFR 164.520(b)), and includes all necessary information as outlined in the Policies and Procedures Manual, although it is not legally required to do so.

1.3. Clear Notice to Participants

IEHIE also expects each participant to have its own Notice of Privacy Practices, consistent with these Policies and Procedures, and in compliance with applicable laws and regulations. A sample Notice of Privacy Practices and Consent are included in Appendix B and Appendix C (Spanish-language version).

IEHIE will respond to requests for protected health information (PHI) for treatment and other legally permitted purposes only. Since HIPAA notice requirements specify that patients must be informed how their information may be used and disclosed, HIE participants must clearly notify patients that their PHI, and specifically what kinds of PHI, may be shared with other participants in the HIE.

Section 164.520 also requires that patients be informed how they can access to their medical information and Sections 164.524 and 164.528 sets out the disclosure requirements for covered entities. IEHIE accordingly expects all HIE participants to inform patients how they can access their medical records and request information about the disclosure of those records. HIE participants, and not IEHIE, shall provide such information.

1.4. Access to PHI

Access to PHI has different use cases for different situations.

1. “Break the glass” is an activity whereby a provider who requires access to a patient’s PHI when that patient has expressly opted out of sharing their PHI with the HIE. In a situation where the patient is unable to give consent (for example, if they are unconscious), the provider will “break the glass” to access their PHI in lieu of an explicit consent.
2. “Break the seal” is an activity whereby a provider without a previously established relationship, such as “circle of care or facility relationship” with the patient and requires access to the patient’s PHI via a “break the seal” activity to document the rationale for access.

Since the IEHIE maintains an opt-out consent management policy, facilities and providers are far more likely to “break the seal” of known care boundaries rather than “break the glass” of a patient’s expressly withdrawn consent from sharing their PHI. Both authorizations produce required audit trails to examine the provider who accessed the PHI and the reason for the access.

1.5. Deceased Individuals

It is IEHIE policy that privacy protections extend to information concerning deceased individuals. An HIE participant that is a covered entity may, but is not required to, use or disclose for any purpose the PHI of individuals who have been deceased for 50 years or longer, although a covered entity is not required to retain records for 50 years.

2. Purpose Specification and Minimization

Data requests by participants or their business associates should be limited to only what is necessary to accomplish specified purposes. In the IE health information exchange, these purposes must be for treatment and health care operations only. Strict minimization is intended to help reduce privacy violations, which can easily occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

Along with minimization of use, the purpose for which HIE participants collect PHI should be specified at the time of data collection. This includes notification that one purpose of collection is for sharing of PHI through the IE health information exchange.

2.1. Role-Based Access to Protected Health Information

It is IEHIE policy that access to protected health information received as the result of a request to IEHIE must be granted to each HIE participant, employee or business associate based on their assigned job functions. Such role-based access privileges should not exceed those necessary to accomplish the assigned job function.

Access to PHI by HIE participants is also based on defined roles or profiles. For additional information on role-based access, see Section 8.1 “Access Control Policy.”

The following user profiles and descriptions are established in the IEHIE environment:

Level 1 – Primary Provider: Designed to access all clinical content available within the Clinical Data Repository (CDR). This role will assume responsibility to unfetter access to full clinical information as is aligned to access privilege under HIPAA to support point of care clinical treatment.

- Full access to all clinical views, including sensitive data
- May “break the seal” to access patient information without an established relationship
- May “break the glass” for patients who have chosen to opt-out of the IEHIE
- Access to patient notifications
- Access to Direct Secure Messaging (additional feature)

Level 2 – Secondary Provider: Designed to access limited clinical content available within the Clinical Data Repository (CDR). This role will assume responsibility to access non-sensitive clinical content within the CDR to support point of care clinical treatment.

- Full access to all clinical views, but NOT sensitive data
- May “break the seal” to access patient information without an established relationship
- Access to patient notifications
- Access to Direct Secure Messaging (additional feature)

Level 3 – Reporting: Designed to obtain non-clinical information via utilization reports.

Level 4 – Front Desk: Designed to access patient information to provide administration services to their supporting organization. It is not intended to support point of care or clinical treatment.

Level 5 – HIE Administrator: Designed to support the operational nature of providing user access controls and onboarding of facility user. It is not intended to support point of care for clinical treatment.

- Access to user administration and auditing screens
- Access to Direct Secure Messaging (additional feature)

Level 6 – HIE Chief Privacy Officer: Designed to support auditing capabilities with access to usability reports and basic configurations of the system. It is not intended to support point of care for clinical treatment.

- Access all patient administration screens to manage consent
- Access to Direct Secure Messaging (additional feature)

Clinical Portal Access	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
Access to Clinical Data (including sensitive)	X					
May “break the glass” for patients who have chosen to opt-out of the IEHIE	X					
May “break the seal” to access patient information without an established relationship	X	X				
Access to patient notifications	X	X				
Direct Secure Messaging - Additional Feature	X	X			X	X
Access to Clinical Data (non-sensitive)		X				
Patient Administration – Consent Management						X
User Administration					X	

2.2. Restrictions on Access to Sensitive Information

Data maintained in the patient record that is sensitive in nature, is flagged as such by the system. This serves as a warning to users that they are about to access a record with sensitive data. The IEHIE user authorization model allows for the creation of user classes that do not have access to sensitive records. Management may also create user classes that restrict access to records based on a proven relationship between a patient and a physician. Examples of sensitive data include but are not limited to: information related to minors, and to sexual and mental health, and substance abuse. Sensitive data criteria will be reviewed to ensure changes are included in the policy restrictions.

Data kept online is also secure from non-authorized users accessing a terminal on the customer’s site through application level security. All access is by username and password. Each username is allowed certain right of access.

Communication between the Participants browser and the application server happens over a secure channel through the use of an expiring one-time session key that maintains the user’s session until a time-out or log-off (which ever happens first). The expiring nature of the session prevents unauthorized access when the user leaves the terminal unattended while logged in.

2.3. Access to Patient Information Through the “Circle of Care”

Each patient within the HIE’s clinical data repository (CDR) maintains a list of providers and facilities with a clinical link to that patient called the “Circle of Care”. When a patient is seen by a particular provider and/or in a particular facility, that provider and/or facility is added to the circle of care. A facility or provider not in the circle of care does not have access to the patient information unless the provider or facility has “Break the Seal” privileges. Primary Care Providers will remain within the circle of care for a period of 36 months and referring providers will remain for 18 months following the most recent update of information to the patient record in the exchange.

3. Use Limitation and De-Identified Data

IEHIE will facilitate the sharing and hosting of PHI for treatment and other legally permitted purposes, including payment and health care operations, provided there is an established treatment relationship with the patient whose data is requested. HIE users' access to PHI is conditioned on their acceptance of these limits. Subject to certain exceptions discussed below, only data that has been properly de-identified may be used for certain other purposes.

3.1. Use Limitation

In addition to the limitations set forth in Section 3, above, certain statutory exceptions contained in California Civil Code Sec. 56.10(b), including those for law enforcement and public health reporting requirements, may permit or require disclosure of data for other purposes. A complete list of these exceptions and the type of authorization they require, where applicable, is attached as Appendix A to this document.

3.2. Disclosure of Protected Health Information for Marketing Purposes

IEHIE will not release personally identifiable information from the HIE for any marketing purposes, excluding the permitted purpose of sending prescription refill reminders.

Regulatory resources for disclosure of information:

1. 45 CFR 164.514, other requirements relating to uses and disclosures of protected health information;
2. California Medical Information Act (CMIA) California Civil Code Section 56.10, Disclosure of Medical Information by Providers.

3.3. De-identified Data and Limited Data Sets

IEHIE may use data that has been de-identified or that is a limited data set according to HIPAA standards without consent or authorization. The CMIA also permits such use of de-identified data (Civil Code Section 56.05(g)).

The standard for de-identification is that there is no reasonable basis to believe the data can be used to identify an individual. Data that has had 18 specific elements of individually identifiable information removed is considered de-identified under HIPAA. (45 CFR 164.514)

IEHIE may use "limited data sets" for specified purposes (e.g., public health reporting, research, and health care operations), without authorization or a waiver of authorization, pursuant to a data use agreement with the recipient. A limited data set is not the same as de-identified data, but it has been stripped of almost all personal identifiers. (45 CFR Section 164.514(e)(2))

3.4. Health Plan Participation

A health plan or health insurance provider may participate in the exchange with the sole purpose of providing case management for those patients with current eligibility or an eligibility hold status. Health Plan participants are considered Level 3 providers (as outlined in Section 2.1) with no capacity to "break the seal" or access the record of a patient for whom current enrollment and eligibility have not been

established. Health Plan participants may perform population-level reporting of currently enrolled and eligible patients in a de-identified manner for the purpose of performing chronic illness or population management activities.

3.5. Behavioral Health Access and Use

Behavioral Health providers may access clinical information in the HIE in order to provide care within the behavioral health setting. Behavioral health providers are considered Level 1 based upon the configuration to allow explicit permission to view such data as outlined in section 2.1.

4. Individual Participation and Control

Individuals have the right to request and receive in a timely and intelligible manner information regarding who has their health data and what specific data the party has, to know any reason for a denial of such request and to challenge or amend any such data. Because individuals have a vital stake in their own PHI and the privacy of that information, its collection and use should be transparent to them. Individual participation promotes data quality, and confidence in privacy and security practices.

4.1. Individual Access to Data

IEHIE retains demographic data in the Master Patient Index (MPI) and Record Locator System (RLS) and clinical data. Patients who become aware of errors in their demographic or clinical data either through access to the Patient Portal or through their treating physician should request that the HIE participant that provided the incorrect data to the MPI or RLS correct that data.

Patients who wish to access their Protected Health Information (PHI) stored in the HIE, or obtain information about who has requested or received their PHI may request that the HIE participant release such data to the Patient Portal for such access. HIE participants must fulfill patients' requests within the timeframe required by the HIPAA Privacy Rule 164.524, "Access of individuals to protected health information." Participants that maintain EHRs (electronic health records) must account for all disclosures of PHI for treatment, payment and health care operations made up to three years prior to the date of the request. Participants have 30 days to fulfill requests for electronic records and also for records in any format that are stored off-site.

4.2. Consent

IEHIE allows individuals to choose whether to have their information included in the HIE. Patients may choose to opt-out of electronic data sharing at their initial point of contact with an HIE participant. It is the responsibility of IEHIE participants to notify patients of their choice to share their information with IEHIE through material provided by the IEHIE participant, not IEHIE.

Failure to opt-out results in being automatically opted into the HIE. For opt-out requests made directly to the IEHIE, participants or patients can utilize the Sample Opt-Out Request Form, included as Appendix D. The Sample Opt-Out Request Form is not intended to be used in place of Notice of Privacy Practices.

Validation of a patient's consent to share information through the HIE is one factor taken into account by the IEHIE system in facilitating participants' access to medical records.

This protection makes individuals active participants in the process of sharing electronic health information. Also, patients' ability to allow the use of their data, or not, will help them understand the conditions under which information might be used and promote confidence in the security surrounding the use of their data.

4.2.1. Effect of Individual Choice

A patient's choice not to allow PHI to be made available shall be exercised through HIE participants; at a patient's request, their PHI will no longer be visible in the HIE. While that patient's data will reside in the HIE, access to such information will be based on the patient's level of consent. For example, a patient may choose to "opt-out" of the HIE for his or her primary care provider, but remain active for the purpose of emergency care. In this case, the patient may determine his or her optimal access conditions.

4.2.2. Revising Individual Choice

Someone who has previously chosen to opt-out of the HIE, and who later wishes to opt-in may do so. This choice shall be exercised through HIE participants, who will then notify the IEHIE. Patients must notify IEHIE in writing of the change, not only the participant who is the patient's initial point of contact with the health information exchange system. A decision to opt-out after having previously opted in shall not be retroactive as to information already released through IEHIE, but it will restrict future dissemination of data retained by properly notified participants.

4.2.3. Provision of Coverage or Care

No one may be denied coverage or care based on a decision to opt-out of the HIE.

4.2.4. Patient Identification Process Protects Privacy

IEHIE patient identification mechanisms afford additional protection to protected health information through the Master Patient Index (MPI) and Record Locating System (RLS). Both employ probabilistic matching to determine if a requested patient's information is in the system and to ensure with a high degree of certainty that the correct patient's records have been identified.

5. Data Integrity, and Quality

5.1. Role of HIE Participants in Maintaining Data Quality and Integrity

IEHIE participants must develop policies and procedures to verify the quality and integrity of the data they provide to those who request it through IEHIE. This should include policies related to data access (i.e., “minimum necessary” standards) and technical security and controls. Policies and procedures should include at a minimum all requirements under HIPAA, and other state and federal regulations related to the use and disclosure of personal health information among covered entities.

5.2. Encryption and Program Access

Because IEHIE is strongly committed to ensuring the confidentiality and integrity of data that is shared through the HIE, it uses either encryption or some other form of secure messaging for any transmission of sensitive information or data. All data providers who participate in the HIE must encrypt PHI prior to transmission. The IEHIE information exchange system includes a progressive strategy of assimilating encryption into applications as the technologies mature.

Encryption is required for all of the following:

- Data housed in the HIE is “encrypted at rest”.
- Sensitive information stored on portable devices.
- Passwords of all systems accessing sensitive information on public networks.

Verification of system and device encryption, and access to all company and HIE system programs is verified monthly and is the responsibility of the HIE Chief Compliance Officer.

6. Administration

This policy establishes formal guidelines for assigning responsibilities and duties related to managing and operating IEHIE systems, policies and procedures. In order to effectively implement and enforce information security and privacy throughout IEHIE operations specific roles and responsibilities have been assigned to the Board of Directors, the Chief Compliance Officer, and IEHIE management. The Board will periodically assess the capabilities and expertise of staff and outside business associates, vendors and other third parties to ensure that all systems and services are effectively managed and that responsibilities have been assigned that accomplish IEHIE security and privacy program objectives and also segregate roles to assure adequate oversight. The roles and responsibilities assigned in this policy impact the entire organization, along with participants in the HIE, individual consumers, business associates, vendors and third parties.

6.1. Roles and Responsibilities

The Board of Directors has ultimate responsibility for oversight of systems, data security and technology integration for delivery of IEHIE services. The Board has assigned oversight responsibility for the Information Security Program to the Chief Technology Officer (CTO). The CTO will also manage the Information Security Program and the Privacy Program. Depending on levels of staffing, the CTO may delegate management of the Privacy Program to another qualified employee. IEHIE managers and key staff are assigned responsibilities as defined in the guidelines below.

6.1.1. IEEHRC Board of Directors

The IEEHRC Board of Directors shall oversee the development, implementation, maintenance and enforcement of the Policies and Procedures, approving the initial policies and all subsequent changes to them. The Board shall assign specific implementation responsibilities, mindful of the need for proper segregation of duties in making these assignments. The Board shall periodically review and audit the Policies and Procedures Manual to ensure that they are compliant with regulatory changes and that appropriate controls are in place to manage risks successfully. At a minimum, the Board shall review an annual information security report presented by the Information Security Officer and a privacy report presented by the HIE Chief Compliance Officer or other qualified employee acting in that capacity, which includes updated assessments of security and privacy risks and policy adjustments necessary to address them.

To ensure continued alignment of the Policies and Procedures with risks and consistent enforcement of the standards and guidelines they establish, the Board has delegated responsibility for oversight of these policies to the CTO.

6.1.2. Duties of the Chief Technology Officer

The Chief Technology Officer (CTO) and Chief Officers of Privacy, Security, and Compliance will meet to review the Policies and Procedures and recommend changes to the Board. Reviews will include standard agenda items to analyze losses due to cyber events, security assessments, audits and other management reports. With this information, the CTO shall determine whether appropriate controls are deployed and are being enforced to successfully manage risk in accordance with the Policies and Procedures Manual.

6.1.2.1. Risk Management

The CTO is assigned duties to ensure the effective management of the physical and technological risks affecting all IEHIE systems and networks in accordance with the Policies and Procedures Manual.

6.1.2.2. Security Monitoring

The CTO must perform all of the duties related to security monitoring as specified in the Policies and Procedures Manual.

6.1.2.3. Internal Auditing and Testing

IEHIE HIE systems will be audited periodically and the results reported to the Board of Directors. The CTO and the auditor shall track all exceptions; the CTO will prepare a response for deficiencies identified in the audit report. The CTO will use the following audit schedule conducted by its system vendor Orion Health Incorporated to perform this reporting:

Quarterly

- Review of corporate firewall rules, updating of policies to address new/removed rules and their justification
- Review of stored data on corporate network to determine if stored data is exceeding the data retention requirement. If so, extraneous data will be purged according to accepted standards (Department of Defense standard 5220-22M).
- Review of changes to network that may require penetration testing
- Application of non-critical system-level patches
- Penetration testing of all networks in hosting facilities

Monthly

- Run wireless sniffer at corporate office, data center facilities

Weekly

- Evaluation of newly discovered security vulnerabilities with recommendations for action
- Review of video camera data

Daily

- Review of event/security logs
- Ongoing security checks such as third-party intrusion detection hardware

Results will be reported to the IEEHRC Board in accordance with the Policies and Procedure Manual.

6.1.2.4. External Examination

The CTO will supervise an independent annual review of the effectiveness of the IEHIE information security program. This may include evaluating system security parameters and profiles such as access controls, password strength, staff training, start-up files and log-in violations. See generally, Section 9 "Operational

Security.” All assessments will be presented to Board of Directors to assist in their understanding of threats and hazards to protected health information and systems.

6.1.2.5. Staying Current with Security and Privacy Technology, Laws and Regulations

The IEHIE will operate at the most current level of privacy and security laws and regulations and will stay current with any changes in those laws and regulations in order to:

- Support the research, development, distribution, and maintenance of information security and privacy policies that comply with all federal and state laws and regulations.
- Maintain an active oversight role of new or improved products, services and technologies.

6.1.3. Duties of the Chief Privacy Officer

The HIE Chief Privacy Officer (CPO) oversees that all IEHIE personnel are responsible for protecting all PHI information assets and is ultimately accountable for ensuring all personnel know, understand and follow the privacy policies.

6.1.4. Duties of the Chief Information Security Officer

The HIE Chief Security Officer (CSO) has primary responsibility for the security of IEHIE systems, and must establish a monitoring and reporting program that is outlined in the Policies and Procedure Manual and includes at a minimum risk management reviews with Orion Health Systems and reporting to the IEEHRC Board.

6.1.5. Duties of the HIE Chief Compliance Officer

The HIE Chief Compliance Officer (CCO) has primary responsibility for day-to-day oversight of information security at IEHIE. IEHIE outsources its information services and the CCO is responsible for maintaining those appropriate contracts and delegation agreements and for continuous oversight of operations. IEHIE is responsible for all operational services, whether performed by its employees or outsourced to third parties.

6.1.6. Duties of the Security Incident Response Team

The IEHIE Security Incident Response Team (SIRT) is an identified cross-disciplinary group entrusted to provide effective leadership in the event of an Information Services-related security incident. SIRT will include technical staff whose role is to halt or minimize the effects of an incident and facilitate speedy recovery. It will also include IEHIE personnel with the authority to make governing decisions, and individuals who can appropriately communicate messages about the incident to external parties.

The SIRT may include the Chief Technology Officer, Chief Compliance Officer and/or Participant Representatives from the stakeholders of the HIE.

6.1.7. Duties of Employees, Contractors and Temporary Staff

IEHIE employees are responsible for safeguarding all sensitive, confidential or personally identifiable information collected, retained or transmitted by IEHIE, from unauthorized access, modification,

destruction, or disclosure, whether accidental or intentional. In addition, they are responsible for complying with this and all other IEHIE policies defining computer, network and information security and privacy measures. All employees, contractors or temporary staff members with access to sensitive, confidential or personally identifiable information must sign an Access Request Form and acknowledge willingness to comply with these Policies and Procedures in a signed Statement of Understanding, included here as Appendix E. The HIE Chief Compliance Officer shall be responsible for verifying, logging, enforcing, and auditing the Statement of Understanding for relevant staff and contractors on an annual basis, at minimum.

All employees, contractors and temporary staff are expected to:

- Protect the security and confidentiality of sensitive, confidential or personally identifiable information transmitted by IEHIE systems and networks.
- Use IEHIE resources only for the purposes specified.
- Comply with the security controls and guidance established by IEHIE.
- Notify the proper level of management of security breaches.

6.1.8. Duties of IEHIE Business Associates

The IEHIE Information Security and Privacy programs and policies require that business associates such as service partners and vendors entrusted with aspects of IEHIE sensitive operations also develop and enforce their own information security and privacy programs that are equivalent to or more stringent than the IEHIE Policies and Procedures.

- IEHIE relies on a third party for hosting web operations, and may also rely on a third party for security scanning at regular intervals.
- IEHIE uses operating systems and network devices, and relies upon respective vendors for secure functionality and timely release of necessary security patches.

6.1.9. Duties of Legal Counsel

IEHIE may require the services of legal counsel from time to time, to provide critical guidance concerning legal matters (e.g., incident liability, partnership and business associate agreements, etc.). IEHIE has contracted with legal counsel who is knowledgeable about HIPAA and the California Confidentiality of Medical Information Act (CMIA), as well as other federal and state laws and regulations relevant to electronic health information exchange.

6.2. Breach Notification Policy

California law and HIPAA and HITECH Act regulations impose very specific notification requirements on covered entities and their business associates in the event of a breach of unsecured personal health information. This policy represents the IEHIE's implementation of breach notification requirements found in 45 CFR 164.402, Subpart D and California Civil Code Sec. 1798. For Direct participants, breach reporting requirements are described in CTEN Policy 103.

6.2.1. Breach Defined

California Civil Code Sec. 1798.82 requires notification when unencrypted personally identifiable information, including PHI, is "reasonably believed to have been, acquired by an unauthorized person." The federal notification standard is now equivalent to California's. The standards for assessing whether notification is required are in Section 6.2.3, below. The current applicable standards are as follows:

- For electronic PHI at rest, data that have been encrypted using a process consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, Guide to Storage Technologies for End User Devices.
- For electronic PHI in motion, data that have been encrypted using a process that complies with the requirements of Federal Information Processing Standards (FIPS) 140-2.
- Paper, film or other hard copy media that have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.
- Electronic media that have been cleared, purged or destroyed consistent with NIST Special Publication 800-88

6.2.2. Who Is Covered by Breach Notification Requirements?

All covered entities and business associates, as defined by HIPAA and the HITECH Act, must provide notification of breaches if the conditions described in this policy are met. All business associates of covered entities are required to inform the covered entity with which they have a business associate agreement of known or suspected breaches, as well as breaches they should have known about through the exercise of reasonable diligence. All subcontractors of business associates are required to inform the business associate with which they have a business associate agreement of known or suspected breaches, as well as breaches they should have known about through the exercise of reasonable diligence. Business associates must inform covered entities of a breach without unreasonable delay, but in no case later than 60 days after discovering the breach.

6.2.3. Assessment of Need for Breach Notification

Breach notification may be triggered by the unauthorized acquisition of unencrypted personal health information. In order to determine whether a breach requires notification to affected individuals, a covered entity must assess the risk that PHI has been "compromised" by a data breach. Such an assessment must take these four factors into account:

- The nature and extent of the PHI;
- The unauthorized person who used or received the PHI;

- Whether the PHI was actually viewed or acquired; and
- The extent to which the risk to the PHI has been mitigated (e.g., by encryption or de-identification).

All actions taken to assess risk that PHI has or has not been compromised must be carefully documented, because IEHIE has the burden of proving to the Secretary of HHS why notification is not required.

6.2.4. Exceptions to Breach Notification Requirements

Section 164.402 of the HIPAA regulations provides three exceptions to the definition of a breach, which IEHIE will take into account in assessing whether a breach has occurred:

- A workforce member who unintentionally accesses or uses PHI in good faith does not trigger a breach.
- An inadvertent disclosure between two individuals authorized to access PHI at the same covered entity, business associate, or organized health care arrangement is not a breach.
- A disclosure where the covered entity has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI is not a breach.

6.2.5. Who Must Be Notified

In the event of a data breach that requires notification, the provisions below shall apply.

6.2.5.1. Affected Individuals

IEHIE is responsible for notifying all individuals whose unsecured PHI has been or is reasonably believed to have been breached; that is, when it is reasonably believed to have been acquired by an unauthorized person and no exception applies.

6.2.5.2. Media

IEHIE will work with the covered entities to determine who will notify and manage the prominent media outlets in the counties where affected individuals reside in the event of a breach of the unsecured PHI more than 500 individuals within the area of the state where IEHIE facilitates the sharing of such information.

6.2.5.3. Secretary of HHS

IEHIE will notify the Secretary of Health and Human Services within 60 days by means determined by HHS of all breaches of unsecured PHI involving 500 or more individuals. HHS will post information concerning breaches of this size on its web site. IEHIE will maintain a log of breaches concerning fewer than 500 persons to submit annually to the Secretary of HHS.

6.2.5.4. Timeliness

A breach is considered to have occurred either on the day it was discovered or the day when, in the exercise of reasonable diligence, it should have been discovered. "Reasonable diligence" means the level

of business care and prudence expected from an individual satisfying a legal requirement. Since IEHIE and its business associates are liable for failing to notify of a breach they did not know of but should have known in the exercise of reasonable diligence, IEHIE will adhere to security procedures and auditing policies that minimize to the greatest extent possible the likelihood of a breach going undetected.

Once a breach is discovered, IEHIE will work with covered entities to determine who will provide notification to all individuals whose PHI has been or is believed to have been acquired by an unauthorized person without unreasonable delay and in no case later than 5 business days after the discovery. California's notification period is far more stringent than federal requirements. The same timeliness requirement applies when the size of the breach requires IEHIE to notify media outlets. Notification time for breaches reported by business associates begins when they are discovered, not when they are reported to IEHIE.

6.2.6. Content and Methods of Notification

The breach notification standards described below shall apply.

6.2.6.1. Content of Notice

IEHIE will work with covered entities to determine who will provide individual breach notifications that are written in plain language and include all the elements required by HHS in accordance with Civil Code 1798.82(b) which exceeds the HITECH Act breach notification requirements.

6.2.6.2. Methods of Notice

IEHIE will work with covered entities to provide written notice to all individuals affected by a breach by first-class mail at their last known address. E-mail notice will be substituted for individuals who have previously agreed to electronic notice. In the case of minors and persons lacking capacity, IEHIE will notify parents or legal representatives. If IEHIE knows that an affected individual is deceased, it will notify the next of kin or a legal representative if it has such person's address.

If IEHIE or a covered entity has no address for an affected individual or a notification is returned as undeliverable, IEHIE or the covered entity will provide substitute notice as soon as reasonably possible. If fewer than ten people are involved and the information is known, substitute notice may be by e-mail or telephone. If more than ten affected individuals cannot be notified by first-class mail, IEHIE or the covered entity will provide substitute notice by conspicuously posting the breach and remedial information on its web site or through major media outlets in the areas where the affected individuals reside.

Such public forms of substitute notice will not include the names of affected individuals, but will ask all patients of IEHIE participants to call a toll-free number to find out if their PHI has been compromised by a breach. To facilitate this, IEHIE will maintain a toll-free telephone number for at least 90 days after publicly posting a breach notification.

7. System Support and Maintenance

IEHIE aspires to the highest standards of performance in the administration and management of the organization. Roles and responsibilities are assigned in order to meet the operational privacy and security requirements of the HIE. IEHIE has secured services for the operation of the hardware, software and management of the HIE operations from Orion Health Systems. The Operations Agreement outlines the roles and responsibilities for system support and maintenance.

7.1. Disaster Recovery Plan

Since IEHIE has secured operations and management services of the HIE operations from Orion Health Systems, their Disaster Recovery Plan informs any response in the occurrence of a catastrophic disruption.

The Disaster Recovery Plan documents and describes the activities and initiatives to anticipate and manage an IT failure. In support of the SaaS Business Continuity Program, the IT disaster recovery plan provides reliable and repeatable processes that support recovery of critical systems and applications within the agreed upon recovery time objective. The mission of disaster recovery is proactive protection and resumption of critical SaaS infrastructure for defined failure scenarios with minimal impact to clients through ongoing controllership to test, validate, and improve the plan.

7.2. Disaster Recovery Objectives

The Disaster Recovery Plan is Commercial in Confidence, so a high level description of functions will be described here. The Disaster Recovery Architecture is set up to provide for a continuous flow of data from the Production facility to the Disaster Recovery (DR) Facility. Backups are processed daily, and any switch over to the DR Facility would result in the most up to date data present and available to participants, up until the last 10 minute segment from the Production facility is received.

8. Security Safeguards and Access Controls

Security safeguards are essential to preventing the loss, corruption, unauthorized use, modification and disclosure of data. Networked data is particularly vulnerable to unauthorized exposure. Adequate controls, rigorously enforced, are essential to protecting the security and privacy of networked information. The design and implementation of policies and technical security precautions governing access to IEHIE systems are necessary to providing effective information privacy.

8.1. Access Control Policy

Individual access to IEHIE systems and data they transmit is subject to strict controls.

8.1.1. Role-Based Access

Role-based access, dependent on a user's proven "need to know" and granting the minimum necessary access to meet the responsibilities of a given job, is a fundamental security policy identified in Section 2.1.

8.1.2. Basis for Being Granted Access to the HIE

IEHIE employees and business associates requesting access must submit an Access Request Form, included here as Appendix F, which has been approved by the applicant's supervisor. Access will be granted by the HIE Administrator to specific applications, menus and data as stipulated on the form. The Chief Compliance Officer shall be responsible for verifying, logging, enforcing, and auditing the Access Request Form of IEHIE staff, contractors, and facility administrators, and annually for the system users of each facility administrator.

HIE participants' access will be based on acceptance of terms of use set forth in the IEHIE Participation Agreement. Anyone who requests access, including participants, IEHIE employees and business associates must sign a confidentiality agreement annually prior to being granted access.

8.2. Logical Access Controls

Access controls must be implemented for all system objects including files, directories and whole computers. IEHIE shall implement specific procedures to support logical access controls. Group policies will be defined to achieve the requirements that follow. These policies will be deployed at the domain level and also be implemented on any self-contained systems.

The minimal logical access controls shall be as follows:

No shared administrative user accounts; this is necessary to ensure proper control and access to network and system resources,

- Accounts will be disabled after a specific number of failed log-in attempts, to be determined by the Chief Security Officer (CSO) and enabled by a system administrator.
- Desktops will be set to lock after being idle for a period determined by the HIE CSO. The HIE CCO will be responsible for verifying and logging system machines monthly.
- Accounts that have been inactive for 45 days will be removed.

- All guest accounts (i.e., default accounts that are part of hardware as delivered by vendors) will be disabled and the use of shared accounts is prohibited on all IEHIE systems.
- Accounts used by vendors and other business associates for remote maintenance will be activated only during a requested time needed during a short maintenance window.

8.3. Granting or Changing User Access Rights and Passwords

The IEHIE Participants shall enforce the following access control guidelines to prevent unauthorized access to sensitive systems and protected medical information through their systems in accordance with the IEHIE Participation Agreement.

- Supervisor approval is required prior to granting access or privileges. Approval is based upon a “business need to know” as determined by the supervisor.
- All users whose access to protected health information is facilitated by the HIE will be given a unique username and an initial password to permit access to system components or sensitive data. Users will choose their own password at the time of their first login.
- User identification must be verified and supervisor approval obtained prior to processing changes to user access including passwords or privileges.
- Supervisor approval for making changes to user access rights must be recorded and stored in writing.
- Access for terminated users will be revoked immediately.

8.3.1. Administrator Privileges

Administrator privileges at the Participant sites are limited to the minimum number of staff required to perform sensitive duties (e.g., granting access to sensitive systems and confidential information).

9. Operational Security

IEHIE operations and systems change constantly, as do the general threat environment and security controls available. System and operation changes and periodic turnover of staff and critical partners may introduce new threats into the environment. To enforce security and privacy criteria and identify new threats, IEHIE will regularly monitor program effectiveness and compliance, making adjustments to minimize risk. IEHIE will actively perform ongoing system security reviews and audits, ensure company-wide security awareness and adherence to policies at all staff levels, and clearly define enforcement procedures and disciplinary actions associated with security breaches and the misuse of IEHIE systems.

Security operations, including reviews and audits, will impact all IEHIE managers of employees with access to sensitive information, regarding staff training, risk management and effective security controls. This policy will be enforced by the IEHIE management and the IEEHRC Board of Directors.

9.1. Assigning Privacy and Security Responsibilities

Designated IEHIE employees will be responsible for implementing and maintaining the HIPAA Privacy and Security Rule and the IEHIE Policies and Procedures. They will have the resources and authority needed to meet their responsibilities. At a minimum, one individual or job description will be designated as the HIE Chief Security Officer and another one as the HIE Chief Privacy Officer, though one person may be designated to fill both roles. The CTO will also designate a different person as the HIE Chief Compliance Officer, or select a qualified employee to carry out the duties of the HIE Chief Compliance Officer if that position has not been officially filled. The HIE CCO may also be designated to serve as the CSO or the CPO if those positions have not been filled, but no single employee may serve as designee to all three Officer positions.

9.2. Acceptable Use Guidelines

The acceptable use of the IEHIE system includes the provisions below.

9.2.1. Access of Administrative System Usage and Data without Consent

Users have no expectation of privacy or confidentiality in any of their system usage, including Internet access and e-mails. Usage may be monitored for policy, security, and/or network management reasons from time to time and is subject to inspection at any time. Inspection of IEHIE systems, data, e-mail and voicemail by management does not require the consent of individual users. Any personal information placed on IEHIE information system resources becomes the property of IEHIE.

9.2.2. Users Are Responsible for All Entries Made Under Their User ID or User Name

A user ID or user name is equivalent to a user signature. Individuals are responsible for all entries under their user ID and/or user name. Shared accounts or passwords are prohibited.

9.2.3. Unacceptable Use Guidelines

Although the behaviors described in this section do not constitute an exhaustive list, the following uses of IEHIE systems are expressly prohibited:

- Communicating sexual or other types of harassment by any means. While online, employees

should avoid using language that could be construed as derogatory, based on race, color, gender, age, disability, national origin or any other category.

- Any attempt to negate or circumvent IEHIE security controls, policies and procedures (e.g., disabling virus protection or tunneling a protocol through a firewall) is strictly prohibited.
- The unauthorized use, destruction, modification and distribution of IEHIE information or information systems are prohibited. Release of IEHIE information must be in accordance with IEHIE policies and business associate agreements.
- Removal of any equipment or software from IEHIE premises or computers is not allowed without prior approval by the employee's immediate supervisor. Removal of any IEHIE equipment or software for personal use is not permitted.
- Use of tools that compromise security (e.g., password crackers and network sniffers) is prohibited except by the Information Services Department staff as part of an ongoing security program authorized by the CSO.
- Intentional interference with the normal operation of the network, including propagation of computer viruses and sustained high-volume network traffic, which substantially hinders others in their use of the network is prohibited.
- Theft of IEHIE resources including sensitive information is prohibited. Any use that violates local, state or federal laws is also prohibited.

9.3. Internet Access Acceptable Use

Employees using IEHIE Internet access are responsible for acting in an ethical and lawful manner. Since it is well known that the Internet is not secure, employees must be aware of the guidelines identified in the Policies and Procedure Manual when using the IEHIE Internet service:

9.4. Remote Access Acceptable Use Guidelines for Non-Participants

Business associates including vendors, contractors and third-party providers accessing IEHIE networks must adhere to the guidelines set forth in this section.

- The Chief Compliance Officer must approve the configuration of all remotely connected systems. If the remote access software used has logging capability, a log must be produced.
- Vendors will be limited to the minimum amount of access required to perform the necessary duties while the session is active. All other access and privileges will be limited to the specific function performed by each vendor or service provider.
- Remote access users must disconnect from any other network connection prior to connecting remotely to IEHIE systems. No split tunnels are allowed. All devices that remotely access IEHIE systems and data must employ boot protection via a password on all computers containing sensitive IEHIE data. Wireless networks will have their access passwords changed no less than monthly by the CSO and confirmed by the HIE Chief Compliance Officer.
- When it is not in use, any equipment and media used to remotely access IEHIE systems should

be stored where it can be securely locked up.

- Current virus protection and a personal firewall should be maintained on remote systems to protect IEHIE systems from viruses and other remote attacks. Current anti-virus update verification is performed monthly and is the responsibility of the HIE Chief Compliance Officer.
- To terminate a remote session with IEHIE systems, a user must log out rather than just disconnect. If the connection is through a web browser, the browser must be closed at the conclusion of the session. If remote processing is inactive for a 20-minute period, remote accesses will time out, resulting in a forced log-off.

10. Administrative Security Policies

10.1. Pre-Employment Background Checks

IEHIE will perform background checks, criminal checks and other investigations as determined appropriate for job and information access responsibilities. Such checks will be carried out in accordance with relevant laws, regulations and ethics, and in compliance with Foundation Administrative Services, Inc., the Human Resources department for all new hires. The following two background checks are performed on every employment candidate:

- a. **County Criminal Court Search:** A County Criminal Court Search will include a minimum of seven years for both felony and misdemeanor court convictions.
- b. **Social Security Address/Alias Trace:** Using information found in credit headers and other sources associated with an applicant's social security number, the Social Security Address/Alias Trace provides historical address information as well as AKA names.

If the employee is fulfilling a position which requires access to PHI, the following investigations may further be performed by the Human Resources department:

- Check of prior employment references;
- Driver's license check; and/or
- Check of industry sanctions and government debarment lists.

10.2. Personnel Education Schedule

All IEHIE Personnel will receive privacy and security training as it relates to these Policies and Procedures and will continue to receive ad hoc policy updates during their employment. Training will include a review of relevant information security and privacy policies, regulatory information, technology changes and procedures to follow in order to properly protect sensitive information.

Affected Employees	Description	Frequency
All IEHIE Personnel	HIPAA and security policies and protocols	Annually
All IEHIE Personnel	Updates to IEHIE Policies & Procedures Manual	Ad hoc
All IEHIE Personnel	Updates to HIE system and/or change in functionality	Ad hoc

All new Personnel are required to attend a HIPAA training, a two-hour online course that concludes with an exam. In addition to emphasizing the importance of privacy and security awareness, the curriculum also covers the following topics (illustrative, not comprehensive):

Information Security Essentials	Business Associates and Covered Entities
Security Awareness Training	Data Security Breaches
Workstation, Laptop, Software, and Physical Threats	HITECH regulations
Red Flag Rules	HIPAA Security Rule
Protecting PHI and PII	HIPAA Privacy Rule
Account Security and Access Rights	Final Omnibus Rule Change; FERPA; FACTA
Malware, Phishing, and other Internet Scams	

10.3. Employment Termination Security Practices

Upon termination, employees shall return property and access devices they were provided with for their work. Supervisors of terminated employees shall be responsible for notifying the CSO to ensure that all associated accesses and accounts are immediately removed. Termination of administrative users shall require re-keying of all user accesses that they managed.

11. System and Network Administration and Security Policies

The following information applies to the administration and security of IEHIE systems and networks.

11.1. Individuals Covered by this Policy

The IEHIE System and Network Administration and Security Policies apply to all IEHIE employees, business associates, affiliate companies, partners, contractors, vendors and any other person or entity using or accessing sensitive data or information systems connected to IEHIE networks. The CTO or designated representatives must approve exceptions to this policy.

The policies discussed in this section provide guidelines for administration of the IEHIE systems and networks and set forth the requirements for their operational security.

System and network administration will be performed to protect all sensitive data in addition to providing a platform to meet technical services function requirements. At a minimum, the CSO, CCO, or a designated member of IEHIE Personnel will define and publish procedures, diagrams and inventories to accomplish the objectives outlined in this section. A copy of the operating procedures will be submitted to the Boards of Directors for approval annually as the policies are updated. Operating procedures shall cover the functions in the sections that follow.

11.2. Audit Trail Security

Audit trails will be secured so they cannot be altered in any way. Orion Health Systems has been contracted to control the security of audit trails in the following ways:

- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files from unauthorized modifications.
- Promptly back up audit trail files to a centralized log server or other difficult to alter media.
- Copy logs for wireless networks onto a log server on the internal LAN.
- Use file integrity monitoring/change detection software (such as a Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts; adding new data should not cause an alert.
- If HIPAA logging and auditing is done, it must be performed on systems processing and storing PHI or Personal Information (PI). Such sensitive data will be stored on cache servers located on HIE participants' premises.
- Logs will be audited and monitored for individual access to records containing sensitive, personally identifiable or confidential information.
- Logs will contain at a minimum, date and time stamp, user account accessing the data, and function performed.

11.3. Identification and Authentication

Administrative access control is based on permission to use the IEHIE system. Permissions must be applied for and will be granted based on employment and/or contractual agreements. Any grant of permission requires a signed Statement of Understanding. All permissions to access the system are restricted by the user's role and need to know.

11.4. Administrative Account Management

The Chief Privacy Officer administratively controls user accounts by following the procedures discussed in the sections below.

11.4.1.Account Activation

Accounts associated with sensitive operations shall be activated only for individuals with a business need to know and proper authorization. Shared accounts are not permitted, and users must choose strong passwords upon initial log-in. All default accounts must be removed prior to installing a system or device.

11.4.2.Account Termination

Account access shall be terminated immediately upon termination of employment. Supervisors of employees who are terminated or end their association with IEHIE should immediately report this change to the HIE Administrator, and in no case later than 72 hours. Administrators shall also check existing accounts regularly to identify dormant accounts and escalate the need for their termination.

11.4.3. Sanctions and Enforcement

Neglect or intentional violation of these account management policies will result in disciplinary action, which may include termination of employment or cancellation of a contract. Other actions could include civil lawsuits and notification of law enforcement agencies.

11.4.4. Exceptions

Should this policy prevent access to a computer system during an emergency, the IEHIE CTO may authorize a password to be generated, reset, regenerated or delivered in a manner not covered in the policy.

12. Risk Management Reviews

In order that the IEEEHRC Board of Directors may be kept up to date on the types of information security risks the HIE is exposed to, risk management reviews shall be implemented to:

- Delineate clear accountability and lines of authority across IEHIE businesses and information security activities. Provide clear guidance regarding acceptable levels of security over sensitive, personally identifiable or confidential information stored in or transmitted by IEHIE systems.
- Ensure that the established policies, procedures, and controls are communicated to and observed by all employees. Perform a periodic review and approval of the IEHIE internal audit program for scope and frequency.

12.1. Management and Oversight

Business Associates such as vendors and other independent third parties that provide support or services to IEHIE information systems shall be required to observe the same standards and level of data confidentiality and controls as those instituted by IEHIE.

IEHIE is responsible for periodically reviewing the financial condition, stability, system security, recovery plans/testing, security assessment tests and internal control practices of all service providers and vendors. The HIE Chief Compliance Officer shall be responsible for maintaining logs of current vendors, their access to PHI (if any) and all supporting contracts and access forms, including business associate agreements, at least annually. A summary of the vendor review will be presented to the Board of Directors on an annual basis.

12.2. Compliance Management

It is the responsibility of the HIE Chief Compliance Officer to oversee and review new and current vendors' compliance with IEHIE Policies and Procedures.

13. Operation of the Incident Response Plan

Orion Health Systems has developed and implemented a plan to prevent and respond to cyber incidents. This plan includes immediate notification to IEHIE as required by State and Federal regulations. IEHIE upon receiving notification will operate and Incident Response Plan. To respond to cyber incidents as effectively as possible, IEHIE will ensure that all procedures outlined in the Policies and Procedures Manual are followed.

APPENDIX A – CMIA DISCLOSURE EXCEPTIONS

Confidentiality of Medical Information Act Disclosure Exceptions: CMIA Sections 56.10 and 56.1007

56.10. (a) No provider of health care, health care service plan or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).

(b) A provider of health care, a health care service plan, or a contractor shall disclose medical information if the disclosure is compelled by any of the following:

(1) By a court pursuant to an order of that court.

(2) By a board, commission, or administrative agency for purposes of adjudication pursuant to its lawful authority.

(3) By a party to a proceeding before a court or administrative agency pursuant to a subpoena, subpoena duces tecum, notice to appear served pursuant to Section 1987 of the Code of Civil Procedure, or any provision authorizing discovery in a proceeding before a court or administrative agency.

(4) By a board, commission, or administrative agency pursuant to an investigative subpoena issued under Article 2 (commencing with Section 11180) of Chapter 2 of Part 1 of Division 3 of Title 2 of the Government Code.

(5) By an arbitrator or arbitration panel, when arbitration is lawfully requested by either party, pursuant to a subpoena duces tecum issued under Section 1282.6 of the Code of Civil Procedure, or another provision authorizing discovery in a proceeding before an arbitrator or arbitration panel.

(6) By a search warrant lawfully issued to a governmental law enforcement agency.

(7) By the patient or the patient's representative pursuant to Chapter 1 (commencing with Section 123100) of Part 1 of Division 106 of the Health and Safety Code.

(8) By a coroner, when requested in the course of an investigation by the coroner's office for the purpose of identifying the decedent or locating next of kin, or when investigating deaths that may involve public health concerns, organ or tissue donation, child abuse, elder abuse, suicides, poisonings, accidents, sudden infant deaths, suspicious deaths, unknown deaths, or criminal deaths, or when otherwise authorized by the decedent's representative. Medical information requested by the coroner under this paragraph shall be limited to information regarding the patient who is the decedent and who is the subject of the investigation and shall be disclosed to the coroner without delay upon request.

(9) When otherwise specifically required by law.

(c) A provider of health care or a health care service plan may disclose medical information as follows:

(1) The information may be disclosed to providers of health care, health care service plans, contractors, or other health care professionals or facilities for purposes of diagnosis or treatment of the patient. This includes, in an emergency situation, the communication of patient information by radio transmission or other means between emergency medical personnel at the scene of an emergency, or in an emergency medical transport vehicle, and emergency medical personnel at a health facility licensed pursuant to

Chapter 2 (commencing with Section 1250) of Division 2 of the Health and Safety Code.

(2) The information may be disclosed to an insurer, employer, health care service plan, hospital service plan, employee benefit plan, governmental authority, contractor, or any other person or entity responsible for paying for health care services rendered to the patient, to the extent necessary to allow responsibility for payment to be determined and payment to be made. If (A) the patient is, by reason of a comatose or other disabling medical condition, unable to consent to the disclosure of medical information and (B) no other arrangements have been made to pay for the health care services being rendered to the patient, the information may be disclosed to a governmental authority to the extent necessary to determine the patient's eligibility for, and to obtain, payment under a governmental program for health care services provided to the patient. The information may also be disclosed to another provider of health care or health care service plan as necessary to assist the other provider or health care service plan in obtaining payment for health care services rendered by that provider of health care or health care service plan to the patient.

(3) The information may be disclosed to a person or entity that provides billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for any of the persons or entities specified in paragraph (2). However, information so disclosed shall not be further disclosed by the recipient in a way that would violate this part.

(4) The information may be disclosed to organized committees and agents of professional societies or of medical staffs of licensed hospitals, licensed health care service plans, professional standards review organizations, independent medical review organizations and their selected reviewers, utilization and quality control peer review organizations as established by Congress in Public Law 97-248 in 1982, contractors, or persons or organizations insuring, responsible for, or defending professional liability that a provider may incur, if the committees, agents, health care service plans, organizations, reviewers, contractors, or persons are engaged in reviewing the competence or qualifications of health care professionals or in reviewing health care services with respect to medical necessity, level of care, quality of care, or justification of charges.

(5) The information in the possession of a provider of health care or health care service plan may be reviewed by a private or public body responsible for licensing or accrediting the provider of health care or health care service plan. However, no patient-identifying medical information may be removed from the premises except as expressly permitted or required elsewhere by law, nor shall that information be further disclosed by the recipient in a way that would violate this part.

(6) The information may be disclosed to the county coroner in the course of an investigation by the coroner's office when requested for all purposes not included in paragraph (8) of subdivision (b).

(7) The information may be disclosed to public agencies, clinical investigators, including investigators conducting epidemiologic studies, health care research organizations, and accredited public or private nonprofit educational or health care institutions for bona fide research purposes. However, no information so disclosed shall be further disclosed by the recipient in a way that would disclose the identity of a patient or violate this part.

(8) A provider of health care or health care service plan that has created medical information as a result of employment-related health care services to an employee conducted at the specific prior written request and expense of the employer may disclose to the employee's employer that part of the information that:

(A) Is relevant in a lawsuit, arbitration, grievance, or other claim or challenge to which the employer and the employee are parties and in which the patient has placed in issue his or her medical history, mental or physical condition, or treatment, provided that information may only be used or disclosed in connection with that proceeding.

(B) Describes functional limitations of the patient that may entitle the patient to leave from work for medical reasons or limit the patient's fitness to perform his or her present employment, provided that no statement of medical cause is included in the information disclosed.

(9) Unless the provider of health care or health care service plan is notified in writing of an agreement by the sponsor, insurer, or administrator to the contrary, the information may be disclosed to a sponsor, insurer, or administrator of a group or individual insured or uninsured plan or policy that the patient seeks coverage by or benefits from, if the information was created by the provider of health care or health care service plan as the result of services conducted at the specific prior written request and expense of the sponsor, insurer, or administrator for the purpose of evaluating the application for coverage or benefits.

(10) The information may be disclosed to a health care service plan by providers of health care that contract with the health care service plan and may be transferred among providers of health care that contract with the health care service plan, for the purpose of administering the health care service plan. Medical information shall not otherwise be disclosed by a health care service plan except in accordance with this part.

(11) This part does not prevent the disclosure by a provider of health care or a health care service plan to an insurance institution, agent, or support organization, subject to Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code, of medical information if the insurance institution, agent, or support organization has complied with all of the requirements for obtaining the information pursuant to Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code.

(12) The information relevant to the patient's condition, care, and treatment provided may be disclosed to a probate court investigator in the course of an investigation required or authorized in a conservatorship proceeding under the Guardianship-Conservatorship Law as defined in Section 1400 of the Probate Code, or to a probate court investigator, probation officer, or domestic relations investigator engaged in determining the need for an initial guardianship or continuation of an existing guardianship.

(13) The information may be disclosed to an organ procurement organization or a tissue bank processing the tissue of a decedent for transplantation into the body of another person, but only with respect to the donating decedent, for the purpose of aiding the transplant. For the purpose of this paragraph, "tissue bank" and "tissue" have the same meanings as defined in Section 1635 of the Health and Safety Code.

(14) The information may be disclosed when the disclosure is otherwise specifically authorized by law, including, but not limited to, the voluntary reporting, either directly or indirectly, to the federal Food and Drug Administration of adverse events related to drug products or medical device problems.

(15) Basic information, including the patient's name, city of residence, age, sex, and general condition, may be disclosed to a state-recognized or federally recognized disaster relief organization for the purpose of responding to disaster welfare inquiries.

(16) The information may be disclosed to a third party for purposes of encoding, encrypting, or otherwise anonymizing data. However, no information so disclosed shall be further disclosed by the recipient in a way that would violate this part, including the unauthorized manipulation of coded or encrypted medical information that reveals individually identifiable medical information.

(17) For purposes of disease management programs and services as defined in Section 1399.901 of the Health and Safety Code, information may be disclosed as follows: (A) to an entity contracting with a health care service plan or the health care service plan's contractors to monitor or administer care of enrollees for a covered benefit, if the disease management services and care are authorized by a treating physician, or (B) to a disease management organization, as defined in Section 1399.900 of the Health and Safety Code,

that complies fully with the physician authorization requirements of Section 1399.902 of the Health and Safety Code, if the health care service plan or its contractor provides or has provided a description of the disease management services to a treating physician or to the health care service plan's or contractor's network of physicians. This paragraph does not require physician authorization for the care or treatment of the adherents of a well-recognized church or religious denomination who depend solely upon prayer or spiritual means for healing in the practice of the religion of that church or denomination.

(18) The information may be disclosed, as permitted by state and federal law or regulation, to a local health department for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events, including, but not limited to, birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, as authorized or required by state or federal law or regulation.

(19) The information may be disclosed, consistent with applicable law and standards of ethical conduct, by a psychotherapist, as defined in Section 1010 of the Evidence Code, if the psychotherapist, in good faith, believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(20) The information may be disclosed as described in Section 56.103.

(d) Except to the extent expressly authorized by a patient or enrollee or subscriber or as provided by subdivisions (b) and (c), a provider of health care, health care service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient.

(e) Except to the extent expressly authorized by a patient or enrollee or subscriber or as provided by subdivisions (b) and (c), a contractor or corporation and its subsidiaries and affiliates shall not further disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan or insurer or self-insured employer received under this section to a person or entity that is not engaged in providing direct health care services to the patient or his or her provider of health care or health care service plan or insurer or self-insured employer.

APPENDIX B – SAMPLE NOTICE OF PRIVACY PRACTICES

Sample Notice of Privacy Practices

IEHIE Notice of Privacy Practices and Consent Form

You are receiving this Notice of Privacy Practices in addition to the Notice of Privacy Practices you have received from your health care provider. The purpose of this Notice is to advise you that the Inland Empire Health Information Exchange (IEHIE) may facilitate electronic sharing of your personal health information among your health care providers in order for your medical treatment to be based on as complete a record as possible.

What is a health information exchange?

IEHIE is a health information exchange. [PROVIDER] is a participant in the Exchange. The Exchange facilitates the electronic transfer of protected health information among participating health care providers. IEHIE houses and stores data in a secure environment and also makes the exchange of health care data among participating health care providers possible.

What information about you will be disclosed through the Exchange?

To the extent permitted by law, [PROVIDER] may disclose your protected health information to other health care providers who request that information, via the Exchange. Protected health information in this case includes information that has been created or received by a health care provider, which relates to your past, present or future mental or physical condition, and that is personally or individually identifiable as belonging to you.

In cases where your specific consent or authorization is required to disclose certain health information to others, [PROVIDER] will not disclose that health information to other health care providers participating in the Exchange without first obtaining your consent. Information that requires your additional consent in order to be shared includes; psychotherapy notes, treatment for substance or alcohol abuse and records of tests or treatment for sexually transmitted diseases.

Who may access information through the Exchange?

Only participants in the exchange who are your health care providers may access information through the Exchange.

For what purposes such information can be accessed?

Information may be accessed ONLY for the purpose of your medical treatment by your health care provider.

Can you request your medical records and/or an accounting of disclosures of who has received them?

You may access your medical records or obtain information about who has requested or received them by making a written request to each Exchange participant to release such data to you via the Patient Portal for such access. A participant has up to 5 days to respond. Participants that maintain EHRs (electronic health records) must account for all disclosures of your personal health information that were made for treatment, payment and health care operations for up to three years prior to the date of the request.

Can you opt-out of sharing your personal health information with your health care providers via the Exchange?

Consumers have the ability to opt-out of sharing their PHI through the IEHIE system. Please see the information about opting out below. CONSENT:

If you do not opt-out of sharing personal health information with your other health care providers by way of the Exchange your consent to such sharing is assumed.

If you do NOT wish to allow [PROVIDER] to share your personal health information electronically with other providers via the Exchange you may exercise your right to opt-out of sharing by signing and dating this document, below. The effect of opting out of the Exchange is that each health care provider will need to request that a copy of your record be transferred by other means.

If you consent now to sharing your personal health information via the Exchange, you may opt-out at a later date. Data that has already been shared will not be recalled from the provider(s) who have already received it, but no new data will be shared by the Exchange.

You may not be denied treatment or otherwise penalized if you opt-out of sharing your personal health information through the Exchange.

If you opt-out of sharing your personal health information via the Exchange and change your mind, you may opt-in at a later date. All health information collected during the opt-out period will be visible upon opt-in.

- ☐ I do not wish to have my personal health information shared via the Inland Empire Health Information Exchange (IEHIE) and hereby exercise my right to opt-out of such sharing:
- ☐ I have previously opted out of the Inland Empire Health Information Exchange (IEHIE) and wish to now opt back in. I understand that my past and present health information will be visible to my health care provider:

(Name)

(Date)

(Signature)

(Facility)

APPENDIX C – SAMPLE NOTICE OF PRIVACY PRACTICES (SPANISH)

Aviso de Practicas de Privacidad y Consentimiento del Paciente para Participar del Programa de Intercambio de Información sobre Salud de Inland Empire Health Information Exchange (IEHIE)

Usted está recibiendo información sobre IEHIE dedicada a compartir información sobre la salud de las personas en forma electrónica y a mejorar la calidad de los servicios de salud de manera segura.

¿Que es Intercambio de Información sobre Salud?

IEHIE es una organización que contribuye al intercambio de información de salud entre los proveedores de servicios de salud que tienen pacientes en común. Esto ayuda a reunir los archivos médicos que usted tiene en los distintos lugares donde recibe atención de salud, poniéndolos electrónicamente a disposición de los participantes que le brindan servicios.

¿Que Información sobre Usted se Intercambia in IEHIE?

Dentro lo que está permitido por ley, su proveedor de salud podrá acceder a toda la información electrónica sobre su salud disponible a través de IEHIE. Los proveedores Participantes que emplearan la información electrónica sobre su salud únicamente para brindarle tratamiento médico y servicios relacionados. Verificar si cuenta con seguro de salud y lo que este cubre. Evaluar y mejorar la calidad de la atención medica que se brinda a todos los pacientes. Este aviso le informa sobre las maneras en que podemos usar y divulgar su información médica. También describe sus derechos y ciertas obligaciones que tenemos sobre el uso y la divulgación de su información de salud. La siguiente información se necesita su consentimiento antes de dar información de drogas y alcohol y VIH tiene derecho a restricciones especiales relacionadas con su uso y divulgación. Notas de psicoterapia quiere decir notas grabada (encualquier medio) por un proveedor de salud que es un profesional que documenta o analiza el contenido de la conversación en consulta privadas de consejería o en grupo, conjunto o junta de familia de consejería y se separan del resto del expediente medico del individuo.

¿Quiénes pueden acceder a la información sobre usted in el Intercambio (IEHIE)?

Únicamente las personas pertenecientes al intercambio y estén autorizados. Que forman parte de atención a su salud.

¿Propósito de la entrega de información y acceso a sus datos de salud?

Sus datos de salud solo se proporciona para su tratamiento médico y servicios relacionados por su proveedor medico.

¿Se puede retirar de su información médica del Intercambio?

IEHIE puede retirar su consentimiento en todo momento. La información ya compartida con su médico no se puede retirar.

¿Se puede pedir copia sobre su información médica y/o contabilidad sobre quien ha recibido su información del Intercambio?

Para inspeccionar y/o recibir una copia de su información médica, usted debe presentar su solicitud por escrito a cada proveedor medico que intercambia su información de salud en IEHIE. Cada participante en el Intercambio (IEHIE) tiene 5 días para responder a su solicitud. Los hospitales y médicos que usan registros electrónicos de salud (EHR) deben dar información sobre toda vez que se revele información sobre su salud, tratamiento, pagos, y todo movimiento sobre su información por tres años anteriores de su solicitud.

¿Se puede no dar consentimiento para compartir su información médica en el Intercambio (IEHIE)?

Usted puede utilizar el presente Formulario de Consentimiento para decidir no compartir sus datos de

salud a través del Intercambio (IEHIE). Por favor, lea cuidadosamente la siguiente información. Su decisión no afectará su capacidad de obtener atención médica ni su cobertura de seguro de salud. La decisión de no dar consentimiento no podrá ser motivo para que se le nieguen los servicios de salud. Si usted no firma hoy de negar consentimiento, pero luego decide, puede hacerlo en cualquier momento.

Niego Mi Consentimiento, usted está diciendo “No, no deseo que mi proveedor de salud a dar información de mis datos de salud por el Intercambio”

Si usted anteriormente negó su consentimiento a dar información de sus datos de salud por el Intercambio y ahora decide dar su consentimiento para brindarle atención de salud y que reciban su Información.

- ☐ NO DOY MI CONSENTIMIENTO para que todos los participantes involucrados en brindarme atención de salud puedan acceder a la información electrónica sobre mi salud a través de Intercambio de Información sobre Salud de Inland Empire Health Information Exchange (IEHIE).
- ☐ DOY MI CONSENTIMIENTO para que todos los Participantes involucrados en brindarme atención de salud puedan acceder a TODA la información electrónica sobre mi salud a través de Intercambio de Información sobre Salud de Inland Empire Health Information Exchange (IEHIE).

(Nombre en letra de molde)

(Fecha)

(Firma del paciente o representante del paciente)

(Sitio de servicio)

APPENDIX D – SAMPLE OPT-OUT REQUEST FORM

Sample Opt-Out Request Form

I request that my health information not be viewable through the Inland Empire Health Information Exchange (IEHIE) system.

Please initial, sign and date this document that you have read and understand each the following statements:

_____ I understand that by submitting this HIE Opt-Out Request Form my health information will not be viewable by health care providers (including emergency room physicians) through the IEHIE system. However, under HIPAA (45 C.F.R. 164.512) the physician does obtain the right to “break the glass”.

_____ I hereby request that IEHIE to block access to my health information through the IEHIE system.

_____ I understand that I am free to “opt-in” at any time during my next visit to a participating organization.

_____ I understand that if I do not intentionally “opt-out” at my next visit to a participating organization, I will be automatically “opt-in” by default.

Patient’s First Name: _____ Patient’s Middle Name: _____

Patient’s Last Name: _____ Date of Birth: _____ (MM/DD/YYYY)

Previous Name(s) or Nicknames: _____ Gender: ☐ Male ☐ Female

Street Address: _____

City: _____ State: _____ Zip Code: _____ Phone: _____

Signature of Patient (or Authorized Representative)
If under 18 years, signature of parent or guardian

Date Signed

For your protection, IEHIE requires that you verify your identity in order to process this Request.

This form must be completed by a Notary Public.

This form must be returned by mail to IEHIE with original signatures in black or blue ink.

----- Section below to be completed by a Notary Public -----

State of _____ County of _____

The foregoing instrument was acknowledged before me this _____ by _____.
(date) (name of person acknowledged)

Notary Print Name: _____

Notary Signature: _____

Please mail this form to: IEHIE, Attn.: Service Desk – HIE Request
3993 Jurupa Ave, Riverside, CA 92506

Notary Stamp:

APPENDIX E – STATEMENT OF UNDERSTANDING

Statement of Understanding

As per Section 6.1.5 of the Inland Empire Health Information Exchange (IEHIE) Policies and Procedures Manual, employees are responsible for safeguarding all sensitive, confidential or personally identifiable information collected, retained or transmitted by IEHIE, from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. In addition, they are responsible for complying with this and all other IEHIE policies defining computer, network and information security and privacy measures. All employees, contractors or temporary staff members with access to sensitive, confidential or personally identifiable information must sign an Access Request Form (if applicable), and acknowledge willingness to comply with these Policies and Procedures in a signed Statement of Understanding.

All employees, contractors and temporary staff are expected to:

- Protect the security and confidentiality of sensitive, confidential or personally identifiable information transmitted by IEHIE systems and networks.
- Use IEHIE resources only for the purposes specified.
- Comply with the security controls and guidance established by IEHIE.
- Notify the proper level of management of security breaches.

I, _____, hereby acknowledge and declare that:
Print Name

- (i) I am aware that IEHIE's policies have been delivered to me as a printed copy, and are available to me on the internet or upon request to my manager. It is my responsibility to familiarize myself with these policies.
- (ii) I agree to conduct my activities in accordance with IEHIE's policies and understand that breaching these standards may result in disciplinary action up to and including termination or other legal remedy available to the organization.
- (iii) I will be required to sign a new Statement of Understanding at least annually, or, at times sooner than annually, when relevant revisions are made, as determined by a new version.

Signed: _____

Date: _____

This signed copy shall reside with the Director of Finance and Human Resources of Foundation Administrative Services, Inc., and the date shall be recorded by the Administrative Assistant of IEHIE.

APPENDIX F – ACCESS REQUEST FORM

Access Request Form for Authorized Users

The Inland Empire Health Information Exchange (IEHIE) facilitates 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. Access to the HIE is granted to organizations that have entered into a Participation Agreement with IEHIE and to individuals affiliated with these organizations.

Inland Empire Health Information Exchange (IEHIE) policy requires that access to protected health information and other patient information (Patient Data) received as the result of a request to IEHIE, must be granted to each HIE Participant, Business Associate, and employee (collectively “Authorized Users”) based on their assigned job functions. Access privileges should not exceed those necessary to accomplish the assigned job function. Role-based access, dependent on a user’s proven “need to know” and granting the minimum necessary access to meet the responsibilities of a given job, is a fundamental security policy.

Authorized Users requesting access to Patient Data must submit an Access Request Form, which must be requested and approved by the applicant’s supervisor. Authorized Users will be granted access by the manager of the HIE Administrator to specific applications, menus, and data as stipulated on the Form.

For additional information on role-based access and access control policies, refer to Section 2.1 and Section 8.1 of the IEHIE Policies and Procedures, respectively.

Authorized User Confidentiality Agreement

Terms of Access to Inland Empire Health Information Exchange

You have been identified by Participant (the hospital, clinic, physician’s office, health plan or other entity with whom you are affiliated) as an Authorized User (as defined in Section 1.5.3 of the Participation Agreement) who requires access to the HIE. The Inland Empire Health Information Exchange (IEHIE) agrees to provide you with access to the HIE only if you agree to the terms and conditions of this Confidentiality Agreement (Agreement), which are intended to maintain the confidentiality, security and integrity of protected health information and other patient information (Patient Data) accessed via the HIE.

You are being provided with a user name and the ability to select a unique password (your Login Credentials) that will provide you with access to Patient Data available through the HIE. In order to be provided this access, you must agree to abide by the following rules:

- a) You will never reveal your Login Credentials to anyone.
- b) You will not allow others, including other staff members with whom you work, to access the HIE using your Login Credentials.
- c) You will log out of the HIE before leaving your workstation to prevent others from accessing the HIE.

- d) You will not fax/print/email/download/copy/photograph or otherwise provide Patient Data to any third parties except in accordance with IEHIE Policies and Procedures and applicable law. You will not make unauthorized copies of the Patient Data.
- e) You will not save Patient Data to portable media devices (such as CDs, USB drives, or handheld devices) except in accordance with the IEHIE Policies and Procedures.
- f) You will not use the HIE or access or view any Patient Data except as required for your job with Participant. You will only access information as necessary to perform your professional obligations to a patient.
- g) You will notify your point of contact designated by the Participant immediately if you have reason to believe that your Login Credentials have been compromised.
- h) You will maintain the confidentiality of all information in accordance with state and federal laws governing the privacy and security of health information, including HIPAA, and in accordance with Participant's privacy and security policies and procedures as well as the IEHIE Policies and Procedures. This includes but is not limited to obtaining the necessary patient consent or authorizations for disclosing Patient Data.
- i) You will not access the HIE via public-use workstations or devices. Public-use workstations and devices are those where general public access is allowed. HIPAA administrative, technical and physical security requirements cannot be applied and controlled on such devices.
- j) You attest that you have received HIPAA awareness training that meets or exceeds the minimum necessary standard for interacting with Patient Data as explained by the HIPAA Privacy Rule 45 CFR 164.502(b), 164.514(d).

Failure to comply with these terms and conditions may result in disciplinary actions against you, which may include without limitation, denial of your privileges to access Data and other actions in accordance with Participant's policies and the IEHIE Policies and Procedures.

IEHIE and Participant have the right at all times to review and audit your use of the HIE and compliance with the terms of this Agreement.

This Agreement grants you a nonexclusive, nontransferable right to use the HIE. This right is specific to you. You may not share, sell or sublicense this right with or to anyone else.

THIS IS A BINDING AGREEMENT. By completing and signing below, you agree to comply with all terms and conditions for access to Patient Data under this Agreement and all IEHIE Policies and Procedures. This Agreement must be signed annually, with new signatures transmitted to the HIE Administrator.

Dated: _____

Signature: _____

Print Name: _____

To create Authorized User profiles for use in the HIE, please complete the following information for the new Authorized User and the supervisor granting the permission. Access Control Levels have been provided to determine facility access the accurate security control level associated with different job functions and job titles. When complete, the Access Request Form will be retained by the Participant's designated HIE administrators.

Access Control Levels

Please identify the accurate control level for this Authorized User.

Level 1 – Primary Provider: Designed to access all clinical content available within the Clinical Data Repository (CDR). This role will assume responsibility to unfetter access to full clinical information as is aligned to access privilege under HIPAA to support point of care clinical treatment.

- Full access to all clinical views, including sensitive data
- May “break the seal” to access patient information without an established relationship
- May “break the glass” for patients who have chosen to opt-out of the IEHIE
- Access to patient notifications
- Access to Direct Secure Messaging (additional feature)

Level 2 – Secondary Provider: Designed to access limited clinical content available within the Clinical Data Repository (CDR). This role will assume responsibility to access non-sensitive clinical content within the CDR to support point of care clinical treatment.

- Full access to all clinical views, but NOT sensitive data
- May “break the seal” to access patient information without an established relationship
- Access to patient notifications
- Access to Direct Secure Messaging (additional feature)

Level 3 – Reporting: Designed to obtain non-clinical information via utilization reports.

Level 4 – Front Desk: Designed to access patient information to provide administration services to their supporting organization. It is not intended to support point of care or clinical treatment.

Level 5 – HIE Administrator: Designed to support the operational nature of providing user access controls and onboarding of facility user. It is not intended to support point of care for clinical treatment.

- Access to user administration and auditing screens
- Access to Direct Secure Messaging (additional feature)

Level 6 – HIE Chief Privacy Officer: Designed to support auditing capabilities with access to usability reports and basic configurations of the system. It is not intended to support point of care for clinical treatment.

- Access all patient administration screens to manage consent
- Access to Direct Secure Messaging (additional feature)

Clinical Portal Access	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
Access to Clinical Data (including sensitive)	X					
May “break the glass” for patients who have chosen to opt-out of the IEHIE	X					
May “break the seal” to access patient information without an established relationship	X	X				
Access to patient notifications	X	X				
Direct Secure Messaging - Additional Feature	X	X			X	X
Access to Clinical Data (non-sensitive)		X				
Patient Administration – Consent Management						X
User Administration					X	

Organization Name: _____

Authorized User's Information

Level Number Requested: _____

Job Title: _____

First Name: _____

Last Name: _____

Organizational Email: _____

Facility Name: _____

Is the User a Physician? (please check) ____ Yes ____ No

External Identifier*: _____

**National Provider Identifier, if applicable.*

Supervisor's Contact Information

Job Title: _____

First Name: _____

Last Name: _____

Organizational Email: _____

Facility Name: _____

*(Access Request Form will be considered incomplete and unacceptable
without a signed attached Confidentiality Agreement)*

SUPPLEMENTAL 1: CTEN Policies for Direct Participants

101. Privacy, Security and Confidentiality of Direct Secure Mail	
Policy: 101	Version: 1.1
Date: September 29, 2015	Approved: Leo Pak

Introduction

Direct Secure Mail (DSM) is provided to providers and administrative personnel for the secure transmission of information that would otherwise require a different mode of secure transfer. The DSM method of information movement is designed to be completely secure. DSM provides organizations, providers and individuals involved in or related to the care process with a secure transport approach.

This policy addresses the need of the user (“You”) to be always mindful that information is being sent by DSM because it is (1) private, (2) requires secure transfer or (3) merits confidentiality protection. You should always consider that information being sent or received is private, secure and confidential.

Applicable Law and Regulation

For providers transferring clinical information or any information that would link the identity of a patient to the fact that the patient has a medical condition or is in treatment, several sets of laws and regulations (hereafter “rules”) apply:

1. **Federal rules** govern protected health information (“PHI”) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPPA, 45 CFR Parts 160, 162 and 164) as amended. Other federal rules govern behavioral health information including 42 CFR Part 2.
2. **State rules** add to the network of rules governing the exchange of PHI. These include the Information Practices Act (California Civil Code §1798-1798.78), California Civil Code 56.11 and 56.21, the California Welfare and Institutions Code 5328-5328.9, the Lanterman-Petris-Short Act and other California rules.

The responsibility for compliance with applicable rules falls upon the individuals (You) and organizations using DSM. DSM is merely the transport tool.

Safeguards

DSM and PHI are governed by a number of usage rules. Several are particularly important:

1. **Verified identify.** You are issued a DSM address only when You have provided identification information and your identity has been verified. Your address is specific to You individually.
2. **No sharing of DSM address.** You may not allow another person to use Your DSM address or give out Your DSM password to anyone else.

3. **Reuse of information.** Your working assumptions should be that only You can utilize information sent to you. Forwarding the information to another party or otherwise distributing it except in accord with an approved policy of Your organization is almost surely a violation of HIPAA or other federal or state rules.
4. **Behavioral health information.** The rules for the transfer of behavioral health information (substance abuse treatment, psychiatric notes) and other sensitive information such as AIDs treatment and genetic information require written consent by the patient for transfer and the data can generally not be retransferred. If You think that behavioral health information is to be moved, assure that appropriate consent has been given in accord with the policies and procedures of Your organization.
5. **Change in role.** In the event that You are moved to a new position or leave the organization, please ask your superior to terminate your DSM address. Otherwise important communications may become stranded in that inbox.
6. **Penalties.** Violations of federal and state privacy and security rules as indicated above and in the prior section are punishable by severe fines to your organization and may result in Your dismissal. It is important that You understand what data transfers are permitted and how You may use data You receive.

Applicable Policies and Procedures

You understand that in addition to your organization's policies and procedures, you are responsible for the following accompanying policies:

Policy Number	Title
102	User Identity Verification
103	CTEN* Breach Notification
104	CTEN Enterprise Security
105	CTEN Requirement to Respond
106	CTEN Duties when Submitting a Message
107	CTEN Applicability of HIPAA Regulations
108	CTEN Agreements with Participants
109	CTEN Incomplete Medical Record
1010	CTEN Direct Messaging Certificate Verification Process
1011	CTEN Use of Message Content
1012	CTEN Confidential Participant Information
1013	CTEN Safeguards
1014	CTEN Direct Secure Messaging User Setup
**CTEN* is the California Trusted Exchange Network. It relies on an agreement among HIEs called the CalDURSA or California Data Use and Reciprocal Support Agreement. The policies with the CTEN label assure that Participant Users are familiar with key provisions of the CalDURSA that apply to Transacting Message Content (moving message transactions with Direct and Exchange).	

Summary and Attestation

DSM is a tool for the secure transfer of patient information. Though it is secure, law and regulation (rules) must still allow for that transfer and the transfer must be done in accordance with permitted processes. Your organization has agreed to provide written policies and procedures for use of Direct and Exchange for transfer of PHI. Your signature on this policy indicates that You generally understand the use of DSM and agree to perform such transfers in accordance with the detailed policies of your organization and the policies listed in the above table.

Name: _____

Title: _____

Organization: _____

Signature: _____

Date: _____

102. User Identity Verification	
Policy: 102	Version: 1.1
Date: September 29, 2015	Approved: Leo Pak

Introduction

Direct Secure Mail (DSM) is supplied to providers and administrative personnel for the secure transmission of information that would otherwise require a different mode of secure transfer such as mail, fax, secure file transfer protocol, etc. The DSM method of information movement is designed to be completely secure. DSM provides organizations, providers and individuals involved in or related to the care process with a secure transport approach.

This procedure addresses the need of the Organization authorizing an individual User to have a Direct Address with the Verification of the User's Identity. A User may be a provider, staff of a provider or a person with an administrative role.

Granting Access to a User

For purposes of this Policy, an Organization which has individuals desiring access to Direct Secure Messaging ("Direct") will designate an "Access Manager." The Access Manager will be the first Direct User (person with a Direct email address) at the Organization and will be responsible for verifying the identity of other individuals applying to become Users of Direct. Verifying identity is a significant legal responsibility and lack of careful execution can have negative privacy and security results that could cause the organization to incur financial liability and negative publicity. If the Access Manager follows the process indicated below, identity verification can be performed accurately and with almost no risk.

Documentation Required to Verify Identity of a User

Attached to this Procedure is the Orion Health Declaration of Identity Template. This is for use of the organization's Access Manager in vetting the identity of users. This section describes the use of the form:

1. **Service Provider.** This is listed as Orion Health. Inland Empire HIE has a Vendor agreement with Orion Health, one of the largest providers of HIE services. Just leave the Service Provider block as it is.
2. **Organization.** This is the name and contact information for your Organization. Please provide the Access Manager's direct telephone line in the Telephone field.
3. **Applicant.** This is the name, office telephone number and home address, etc., of the person applying for a Direct address.
4. **Applicant Signature.** The form should be signed in the present of the Access Manager (called the "Trusted Agent" on page 2 of the form. The Trusted Agent signs with his/her information after verifying the information listed in "Instructions to Notary / Trusted Agent."
5. **Instruction to Notary / Trusted Agent.** The Access Manager needs to verify the User applicant based on at least one government-issued photo ID.
 - a. Passport

- b. Driver's license
- c. Military ID
- d. Permanent resident card
- e. Similar ID

If the first ID is not a government ID, a second ID is required such as

- a. Social security card
- b. Birth certificate
- c. School ID
- d. Vote's registration card

Check that the address on the government ID or other IDs match the address given in the Applicant box. If not, the applicant needs to provide a proof of address:

- a. Utility bill (telephone, gas, electric, water or Internet)
- b. Bank statement
- c. Rental agreement
- d. Government-issued document.

Attach a copy of the IDs used to the Orion form. The User signs as indicated above in the presence of the Access Manager and the Access Manager completes and signs the Trusted Agent's box.

6. **Identification #1 and #2.** Indicate what identification items are provided.
7. **Use of Notary.** If you are completing the form for the Access Manager, the first User for the Organization, the Access Manager will complete the form for him/herself and have a notary verify that the identification is attached per the instructions and then notarizes the document.

DSM Web HCO Account Request

DSM Web is a web-based secure mail solution within Orion Health™ Clinical Portal

Organization Details

Please fill out a separate form for each organization requesting access to the HIE.

Organization Name	Community Medical Centers
OID	For example, 2.16.840.1.113883.3.1 <i>A globally unique ISO identifier that consists of numbers and dots. OIDs are paths in a tree structure, with the left-most number representing the root and the right-most number representing a leaf.</i> <i>Enter the OID, if known. If an OID is not provided, Orion Health will create one using the Orion Health OID Registry.</i>
Representative	Jamie Franklin <i>The representative is an agent of the HCO, and is responsible for authorizing the Orion Health HISP to request Direct certificates on behalf of the HCO. Direct certificates facilitate the secure interstate and inter-agency sharing of electronic health information.</i>
Representative's Email Address	jfranklin@communitymedical.org
Email Domain	direct.communitymedical.HIEEmailDomain.com <i>Your organization's email domain must only contain letters. Numbers, spaces, punctuation and special characters are not permitted. For example, <u>username@direct.HCOEmailDomain.HIEEmailDomain.com</u>.</i> <i>If this domain is already in use, Orion Health will contact you for an alternative.</i>

Organization Administrator(s)

Details of up to three employees authorized to act as administrator(s) for your organization.

First Name	Richard
Middle Name	Your middle name
Last Name	Cummins
Title	Director, Technical Services Group
Email Address	rcummins@communitymedical.org

First Name	Jinyong
Middle Name	Your middle name
Last Name	Kim
Title	Mgr, Technical Services Group
Email Address	Jin.Kim@communitymedical.org

First Name	Your first name
Middle Name	Your middle name
Last Name	Your last name
Title	Your title
Email Address	User's email address for notifications

DSM Direct HCO Account Request

Organization Details

Please fill out a separate form for each organization requesting access to the HIE.

Organization Name	Name of your HCO
OID	For example, 2.16.840.1.113883.3.1 <i>A globally unique ISO identifier that consists of numbers and dots. OIDs are paths in a tree structure, with the left-most number representing the root and the right-most number representing a leaf.</i> <i>Enter the OID, if known. If an OID is not provided, Orion Health will create one using the Orion Health OID Registry.</i>
HIPAA Compliance	☐ HIPAA Covered Entity <i>A Covered Entity (CE) performs medical services on the patient and has the most trusted access to Protected Health Information (PHI).</i> ☐ HIPAA Business Associate <i>A Business Associate (BA) is someone who a CE uses for services and who needs access to the PHI of the CE's patients to perform some level of service.</i> ☐ Other HIPAA Entity <i>Health care organization that treats protected health information with the privacy and security equivalent to those required by HIPAA.</i>
Address	Street Address Address Line 2 City Postal Code State Country
Telephone	Country code - Area code - Phone number
Preferred Direct Email Domain	direct.yourDomain.HIEEmailDomain.com OR direct.yourDomain.com <i>Your organization's email domain must only contain letters. Numbers, spaces, punctuation and special characters are not permitted. For example, <u>username@direct.HCOEmailDomain.HIEEmailDomain.com</u>.</i>
Alternative Direct Email Domain	direct.yourDomain.HIEEmailDomain.com OR direct.yourDomain.com <i>In the event your preferred Direct email domain is already in use, please provide Orion Health with an alternative domain name.</i>

Organization Representative	Name of the representative <i>The representative is an agent of the HCO, and is responsible for authorizing the Orion Health HISP to request Direct certificates on behalf of the HCO. Direct certificates facilitate the secure interstate and inter-agency sharing of electronic health information.</i>
Representative's Email Address	Representative's email address for notifications

Technical Contact

The main point of contact at the HCO for any questions regarding the deployment or configuration of the XDR server and client.

Name	Name of the technical contact
Title	Title of the technical contact
Telephone	Country code - Area code - Phone number
Email Address	Corporate email address

XDR Details

The Technical Contact at the HCO should provide this information.

XDR Server URL	Public URL of the SOAP end point for the XDR server
Private Key CSR	Certificate Signing Request (CSR) of the private key that will be used to generate an SSL certificate for the XDR server and client. <i>Copy the CSR and paste it here, or upload the CSR file to the Support Tracker ticket along with this form.</i> <i>When generating your CSR, specify a key size of 2048 or higher.</i>

 ORION HEALTH™ DIRECT SECURE MESSAGING	 INLAND Empire HIE LINKING DATA TOGETHER
---	--

DIRECT IDENTITY VERIFICATION AND AUTHORIZATION

Service Provider	HISP Name: Orion Health	Telephone: +1 800 905 9151
	Address: 225 Santa Monica Boulevard, 10th Floor, Santa Monica CA 90401	Account #: 080088

Organization	Organization:	Telephone:
	Address:	
	HIPAA Compliance: ☐ HIPAA covered entity ☐ HIPAA Business Associate ☐ Other HIPAA Entity - Health-care organization that treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.	

Applicant	Name:	Telephone:
	Home Address:	Email:
	Date of Birth:	

By signing this document, I hereby agree to the attached authorization and request a Direct Certificate and declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

_____ / / , : am/pm
 Applicant Signature Date and Time

Please have a notary or trusted agent witness your signature and sign the acknowledgement on the next page. The signed form should then be returned to Orion Health by following the instructions given to you.

INSTRUCTIONS TO NOTARY/TRUSTED AGENT: Please verify the person named in this document using at least one government-issued photo ID. Examples of acceptable photo ID documents include a passport, driver's license, military ID, permanent resident card, or similar document.

If the ID is not a federal government ID, a secondary ID is required. The second ID does not have to be a government-issued ID. Examples of acceptable secondary ID documents include a social security card, birth certificate, school ID, or voter's registration card.

If the address on the ID is different from the one stated in this form, a document with the correct address must be provided. Examples of acceptable proof of address include a utility bill (telephone, gas, electric, water or Internet), bank statement, rental agreement or a government-issued document.

Attach a copy of all ID documents to this form. Make sure the information listed in the identification boxes on the first page and below match the identity documents presented during the verification process. **Notaries should sign the Notarial Acknowledgement, leaving the Trusted Agent information blank. Trusted Agents do not need to complete the Notarial Acknowledgement.**

Identification #1	Type of Document:		Photo: Y N
	Issued By:	Serial #:	
	Name on ID#1:	Expiration Date:	

Identification #2	Type of Document:		Photo: Y N
	Issued By:	Serial #:	
	Name on ID#2:	Exp. Date:	

TRUSTED AGENT'S STATEMENT (Not required if notarized)

Trusted Agent	I hereby declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that on the date indicated herein, applicant personally appeared before me, signed the foregoing document in my presence, and presented the identification listed above.		
	Name		
	Organization		
	Address		
	Telephone		Email:
Trusted Agent Signature _____ Date and Time _____ / _____ , _____ : _____ am/pm			

NOTARIAL ACKNOWLEDGMENT

STATE/Commonwealth of _____ }
COUNTY/Parish of _____ }

I hereby certify under penalty of perjury under the laws of the United States of America that at the above-indicated date and time, personally appeared before me, the above-named Applicant, who signed the foregoing document in my presence, and who presented the identification listed above, affixed hereto, which I did review for authenticity.

WITNESS my hand _____ and official seal
Notary Signs Here

Date and Time / / , : am/pm

Print Name		Organization / Employer
Telephone		Email:



AUTHORIZATION

PLEASE READ THIS AUTHORIZATION CAREFULLY BEFORE SIGNING THE ATTACHED IDENTITY VERIFICATION DOCUMENT. BY SIGNING THE IDENTITY VERIFICATION, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AUTHORIZATION, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AUTHORIZATION OR DO NOT WISH TO APPOINT ORION HEALTH AS YOUR CERTIFICATE AGENT, DO NOT SIGN THE IDENTITY VERIFICATION. IF YOU HAVE ANY QUESTIONS, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

DigiCert, Inc. (“**DigiCert**”) issues X.509 v.3 digital certificates (“**Certificates**”) to customers of the health information service provider identified on the attestation document (“**Orion Health**”). You, as the organization that will be named in a certificate, are providing this authorization to assist Orion Health in performing certain digital certificate-related duties that are normally reserved for Certificate subjects, usually an entity’s equipment, personnel, or agents. These tasks include managing keys, registering devices, and authenticating personnel with DigiCert and its Certificate systems and installing, configuring, and managing issued Certificates. Therefore, you hereby agree and authorize Orion Health and DigiCert as follows:

1. **Certificates.** Orion Health may request and approve Certificates in your name and use issued Certificates for your benefit. DigiCert may issue, refuse to issue, revoke, or restrict access to Certificates in accordance with the instructions provided by Orion Health and rely on these instructions as if originating from you.
2. **Representations.** You represent that you are a HIPAA covered entity, a HIPAA business associate, or a health-care organization that treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. You represent that you will limit your use of the digital certificate for purposes required as a HIPAA Business Associated or Non-HIPAA Healthcare Entity (HE), defined as an entity that has an appropriate healthcare-related need to exchange Direct messages and which agrees to handle protected health information with privacy and security protections that are equivalent to those required by HIPAA.
3. **Authorization.** You explicitly appoint Orion Health’s employees and agents as your agent for the purpose of requesting, using, and managing Certificates and corresponding private keys. Orion Health’s employees and agents are authorized to fulfill all obligations imposed by DigiCert with respect to the Certificate, communicate with DigiCert regarding the management of key sets and Certificates, and fulfill all roles related to Certificate issuance, such as a certificate requester, certificate approver, and contract signer (as used in the CA/Browser Forum’s Extended Validation Guidelines for SSL Certificates). You hereby authorize Orion Health and its employees to:
 - (i) Request Certificates for domains and emails owned or controlled by you or your affiliates,
 - (ii) Request Certificates naming you or your equipment, employees, agents, or contractors as the subject, and
 - (iii) Accept terms and conditions related to Certificates issued on your behalf.
4. **Trusted Agent.** In addition, you are hereby appointed as an agent of DigiCert for the purpose of collecting documentation, verifying identities, and providing identity information to DigiCert. Any information must be verified in accordance with instructions provided by DigiCert. The requirements for identity verification are set by the applicable CP and may change without notice. Therefore, DigiCert may amend the instructions at any time.

5. Documentation. For each certificate ordered by Orion Health under your authorization, DigiCert must obtain a personal attestation and a copy of all documentation necessary to verify the entity's identity. DigiCert may reuse this information in some cases. DigiCert may rely solely on the information you provide or previously provided when issuing a Certificate or may elect to perform additional verification prior to issuing a Certificate. You agree to provide, at all times, provide accurate, complete, and true information to DigiCert. If any information provided to DigiCert changes or becomes misleading or inaccurate, then you agree to promptly update the information. You consent to (i) DigiCert's public disclosure of information embedded in an issued Certificate, and (ii) DigiCert's transfer of your personal information to DigiCert's servers, which are located inside the United States. DigiCert shall follow the privacy policy posted on its website when receiving and using information from you or Orion Health. DigiCert may modify the privacy policy in its sole discretion.
6. Representation. You represent that you have the authority to execute this authorization and bind your organization (if applicable) by its terms. By submitting documentation to DigiCert, you represent to DigiCert that (i) you have verified any named individual's name, address, email address, telephone number, birthdate, and any other information required by DigiCert and in accordance with any instructions provided by DigiCert, (ii) you have examined any relied upon documents for modification or falsification and believe that the documents are legitimate and correct, and (iii) you are unaware of any information that is reasonably misleading or that could result in a misidentification of the verified entity. These representations survive termination of this appointment until all Certificates that rely on the documentation expire.
7. Duration. This authorization lasts until revoked by you, and you are responsible for all Certificates requested by Orion Health on your behalf until after DigiCert receives a clear email message revoking the authorization at legal@digicert.com. Even after revocation, all representations and obligations herein survive until all Certificates issued under this authorization expire or are revoked in accordance with DigiCert's agreement with Orion Health. DigiCert may require that you periodically renew this authorization by resubmitting a copy of this authorization to DigiCert.
8. Certificate Revocation and Termination. DigiCert will revoke any Certificate issued to Orion Health on your behalf after receiving notice from you and after verifying the legitimacy of the revocation request. DigiCert may also revoke a Certificate issued to Orion Health on your behalf for any reason and without notice.
9. Warranty Disclaimers. DIGICERT SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICES WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO SERVICES WILL BE TIMELY OR ERROR-FREE. DigiCert may modify or discontinue specific service or product offerings at any time. Nothing herein requires DigiCert to provide Certificates or other related services to you or Orion Health.
10. Limitation on Liability. YOU HEREBY WAIVE ANY RIGHT TO ANY DAMAGES RELATED TO DIGICERT'S SERVICES, INCLUDING THE ISSUANCE OR USE OF CERTIFICATES. DIGICERT IS NOT LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNATIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement were breached or proven ineffective.
11. Indemnification. To the maximum extent permitted by law, you will indemnify and defend DigiCert and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all liabilities, claims, damages, and costs (including reasonable attorney's fees) related to either DigiCert's reliance on this authorization or the use of a Certificate issued under this authorization.
12. Notices. You must send all notices (i) in writing, (ii) with delivery confirmation via first class mail, commercial overnight delivery service, facsimile transmission, email, or by hand, and (iii) addressed to DigiCert, Inc., Attn: Legal Department, 2600 West Executive Parkway, Suite 500, Lehi, Utah 84043, email: legal@digicert.com, fax: 1-866-

842-0223. DigiCert may change its address for notices by sending notice of the change to Orion Health. Orion Health is solely responsible for conveying notices to you. All notices to DigiCert are effective on receipt. DigiCert will deliver notices to you by delivering the notice to Orion Health. Notices are effective when sent to Orion Health in accordance with DigiCert's agreement with Orion Health.

13. Severability. The invalidity or unenforceability of a provision under this authorization, as determined by an arbitrator, court, or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this agreement. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.
14. Intended Beneficiaries. Orion Health and DigiCert are express and intended beneficiaries of your obligations and representations under this agreement.

103. CTEN Breach Notification	
Policy: 103	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Introduction

Breach means (1) the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting Message Content and (2) the use or disclosure of Message Content that is not for a HIPAA Permitted Purpose. The principal HIPAA permitted purposes are (1) treatment, (2) payment and (3) healthcare operations. The focus of Transacting Message Content is upon the treatment purpose.

One-Hour Breach Notification

For this Policy, a “CTEN Member” is an organization that has signed the CalDURSA and has been accepted by the California Interoperability Committee to the CTEN. Each CTEN Member agrees that within one (1) hour of discovering information that leads the CTEN Member to reasonably believe that a Breach may have occurred, it shall alert other CTEN Members whose Message Content may have been Breached and the Interoperability Committee to such information by sending an email to a dedicated e-mail address (hereinafter “Alert Email”).

- i. The Alert Email is primarily intended to alert that a Breach may have occurred. CTEN Members will use caution before relaying details of the potential Breach via e-mail.
- ii. Immediately notify other CTEN Members, who, in the judgment of the CTEN Member making the alert, may have had a Breach of Message Content or otherwise are likely affected by the Breach.
- iii. CTEN Members are strongly urged to send Breach Notifications through a secure means, where appropriate and possible (i.e., posted on the Secure Site) and labeled as Confidential Participant Information.
- iv. If, on the basis of the information that the CTEN Member has, the CTEN Member believes that it should temporarily cease exchanging Message Content with all other CTEN Members, it may undergo a service level interruption or voluntary suspension.

Twenty-Four Hour Notification of Breach Determination

As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, the CTEN Member shall provide a Notification to all CTEN Members likely impacted by the Breach and the Interoperability Committee of such Breach. The Notification should include sufficient information for the Interoperability Committee to understand the nature of the Breach. For instance, such Notification could include, to the extent available at the time of the Notification, the following information:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach (e.g. employees, Participants, service providers, unauthorized persons, etc.)
- The type of Message Content Breached

- CTEN Members likely impacted by the Breach
- Number of individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by the reporting CTEN Member to mitigate the Breach
- Current Status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

The CTEN Member shall supplement the information contained in the Notification as it becomes available and cooperate with other CTEN Members and the Interoperability Committee in accordance with Section 20(e) of the CalDURSA relating to rights in a dispute. The Notification required by this policy (Section 14.3 of CalDURSA) shall not include any PHI. If, on the basis of the Notification, a CTEN Member desires to stop Transacting Message Content with the CTEN Member that reported a Breach, it shall stop Transacting Message Content in accordance with Section 12.1(b) of the CalDURSA. If, on the basis of the notification, the Interoperability Committee determines that (i) the other Participants that have not been notified of the Breach would benefit from a summary of the Notification or (ii) a summary of the Notification to the other CTEN Members would enhance the security of the Performance and Service Specifications, it may provide, in a timely manner, a summary to such CTEN Members that does not identify any of the CTEN Members or individuals involved in the Breach.

1. Information provided by a CTEN Member in accordance with this policy (Section 14.3 of CalDURSA), except Message Content, may be “Confidential Participant Information.” Such “Confidential Participant Information” shall be treated in accordance with Section 16 of CalDURSA, Confidential Participant Information.
2. This policy shall not be deemed to supersede a CTEN Member’s obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law.
3. Compliance with this policy shall not relieve CTEN Members of any other security incident or breach reporting requirements under Applicable Law including, but not limited to consumers.

104. CTEN Enterprise Security	
Policy: 104	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Maintain Secure Environment

Each CTEN Member organization (“Member”) shall be responsible for maintaining a secure environment that supports secure Transactions. Members shall use appropriate safeguards to prevent use or disclosure of Message Content other than as permitted by applicable law and regulation and the Member organization’s policies. These include appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of Message Content.

HIPAA Implementation Specifications

Appropriate safeguards for Non-Federal Participants shall be in state law, or those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, “required” implementation specifications, and “addressable” implementation specifications to the extent that the “addressable” implementation specifications are reasonable and appropriate in the Member’s environment, or both. If an “addressable” implementation specification is not reasonable and appropriate in the Member’s environment, then the Member shall document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate.

Federal Participants

Appropriate safeguards for Federal Participants shall be those required by Applicable Federal Law related to information security.

Written Privacy and Security Policies

Each Member shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the Member’s respective Effective Date.

105. CTEN Requirement to Respond	
Policy: 105	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Duty to Respond to Treatment Messages

All CTEN Members that request, or allow their respective Participants to request, Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A CTEN Member shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged.

Response for Other Permitted Purposes

CTEN Members may, but are not required to, Transact Message Content for a Permitted Purpose other than Treatment. Nothing in this Section 12.1(a) shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.

Duty to Respond to All Treatment Messages

Each CTEN Member that requests, or allows its respective Participants to request, Message Content for Treatment shall Transact Message Content with all other CTEN Members for Treatment, in accordance with Sections 6, 12.1(a) and 14 of the CalDURSA. If a CTEN Member desires to stop Transacting Message Content with another Member based on the other Member's acts or omissions in connection with this Agreement, the CTEN Member may temporarily stop Transacting Message Content with such Member either through modification of its Access Policies or through some other mechanism, to the extent necessary to address the Member's concerns. The Participant will notify IEHIE of the cessation and the reason for it and IEHIE will investigate the problem and attempt to resolve it.

106. CTEN Duties When Submitting a Message	
Policy: 106	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Specific Duties of a CTEN Member When Submitting a Message

Whenever a CTEN Member or Participant acts as a Submitter by submitting a Message to another CTEN Member or Participant, the Submitter shall be responsible to:

1. Submit each Message in compliance with Applicable Law and applicable Policies and Procedures including representing that the Message is:
 - a. for a Permitted Purpose;
 - b. submitted by a Submitter who has the requisite authority to make such a submission;
 - c. supported by appropriate legal authority for Transacting the Message Content including, but not limited to, any consent or Authorization, if required; and
 - d. submitted to the intended Recipient.
2. Represent that assertions or statements related to the submitted Message are true and accurate;
3. Submit a copy of the Authorization, if the Submitter is requesting Message Content from another CTEN Member or Participant which requires an Authorization.
4. For Federal Participants only, in addition to complying with 1 through 3 above, ensure that Messages submitted by such Federal Participant adhere to interoperability standards adopted by the Secretary of Health and Human Services, California Data Use and Reciprocal Support Agreement FINAL – July 24, 2014, and the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS), as applicable.

107. CTEN Applicability of HIPAA Regulations	
Policy: 107	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Applicability of HIPAA Regulations

Message Content may contain protected health information (PHI). Furthermore, some, but not all, CTEN Members (“Members”) are either a Covered Entity or a Business Associate. Because the Members are limited to Transacting Message Content for only a Permitted Purpose, the Members do not intend to become each other’s Business Associate. To support the privacy, confidentiality, and security of the Message Content, each Member and its Participants agrees as follows:

- a. If the Member is a Covered Entity, the Member does, and at all times shall, comply with the HIPAA Regulations and Applicable Law to the extent applicable.
- b. If the Member is a Business Associate of a Covered Entity, the Member does, and shall at all times, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. §164.504(e)(3)(i)(A), its Memoranda of Understanding) and Applicable Law.
- c. If the Member is a Governmental Participant, the Member does, and at all times shall, comply with the applicable privacy and security laws and regulations.
- d. If the Member is neither a Covered Entity, a Business Associate nor a Governmental Participant, the Member shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations as if it were acting in the capacity of a Covered Entity or such other standards as may be determined in the future.

108. CTEN Agreements with Participants

Policy: 108

Version: 1.0

Date: September 29, 2015

Approved: Leo Pak

Enforceable Agreements

Each CTEN Member (“Member”) has valid and enforceable agreements with each of its Participants that require the Participants to, as a minimum:

1. Comply with all Applicable Law;
2. Reasonably cooperate with the Member on issues related to Transacting Message Content;
3. Transact Message Content only for a Permitted Purpose;
4. Use Message Content received from another Member or Participant in accordance with the terms and condition of the Participation Agreement, CalDURSA and Member’s Policies and Procedures;
5. As soon as reasonably practicably after determining that a Breach occurred, report such Breach to the Member; and
6. Refrain from disclosing to any other person any passwords or other security measures issued to the Participant by the Member.

For Participants who are employed by a Member or who have agreements with the Member, compliance with this Policy may be satisfied through written policies and procedures that address these items 1 through 6 so long as the Member can document that there is a written requirement that the Participant comply with the policies and procedures.

109. CTEN Incomplete Medical Record	
Policy: 109	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Medical Records and Message Content

Each CTEN Member and Participant acknowledges that Message Contact Transacted by Members and Participants shall not include the individual's full and complete medical record or history. Such Message Content will only include that data which is the subject of Message and available for exchange among CTEN Members.

1010. CTEN Direct Messaging Certificate Verification Process	
Policy: 1010	Version: 2.0
Date: September 29, 2015	Approved: Leo Pak

Inland Empire HIE (IEHIE) contracts with Orion Health for Direct services. Orion Health maintains CTEN Direct messaging certificates for itself and makes those available to IEHIE which makes them available to all Direct Participants. Under this arrangement, the primary responsibility for maintaining valid and current certificates lies with Orion Health, which automates the process as much as possible to reduce service interruptions. IEHIE can periodically check the existence and termination date of the Direct messaging certificate it is using. This policy describes that process.

The California Interoperability Committee maintains specific policies that define business process and technical requirements for each transaction pattern supported on the CTEN. A list of the Exchange Policies for the current CTEN transaction patterns can be found at <http://www.ca-hie.org/projects/cten/policies>.

Processes:

- Process 1 (**P1**): Obtain HPD and verify current organizations using DSM and XDR
- Process 2 (**P2**): Verify certificate expiration dates of Direct addresses
- Process 3 (**P3**): Download the IEHIE Trust Anchor
- Process 4 (**P4**): Verify inclusion of certificate into CTEN Trust Bundle

Required Artifacts:

- Artifact 1 (**DCVv2**): Direct_Certificate_Verification_v2.xlsx (spreadsheet)

P1 – Obtain HPD and Verify Current Organizations using DSM and XDR

Step 1: Export the Healthcare Provider Directory (HPD) as a comma-separated values (CSV) file from Orion Health DSM Web Portal. The CSV file contains the Direct addresses of every provider and shared mailbox group in IEHIE's HPD.

1. Log into DSM Web as the HIE Administrator.
2. From the menu, select **DSM ADMIN > HPD Export**.
3. In the **Modified since** field, select the date from which you want to export the HPD, then press the **Search** button.
4. Press the **Download CSV results** link to download the HPD as a CSV file.

[Image restricted due to confidential in commercial requirements]

Step 2: Using the downloaded HPD, open DCVv2 to verify that

- (a) each healthcare organization (HCO) using a Direct address is identified, adding or removing organizations as necessary;
- (b) each Direct address is preceded with "postmaster@", followed by the full Direct address.

Example: *postmaster@direct.xxxxx.inlandempirehie.com*,
where "xxxxx" is the name of the organization to which the address belongs

Note 1: Some HCOs may utilize multiple Direct addresses (DSM and XDR). A record must be maintained for each unique Direct address.

P2 – Verify Certificate Expiration Dates of Direct Addresses

Step 1: Orion Health's certificate management system automates the monitoring and notification process to ensure continuous service to all Direct users. Organization administrators are notified two months prior to the upcoming expiration and are required to confirm the organization's details for certificate extension. After confirmation, the public key of the Direct certificate may be verified outside of the Orion Health Portal by using the MaxMD (MMD) Direct Certificate Search, which can be found at <http://www.maxmddirect.com/maxmdirect-certificate-search.html>.

1. Navigate to the MMD website.
2. In the field, enter the Direct address and press **Search**.

There are two results available:

1. If certificate is not found or invalid:

No certificate found in public DNS or LDAP for address **postmaster@direct.**

No NS record found.

2. If certificate is found and valid:

✔ 1 certificate found in public **DNS** server for address **postmaster@direct.**

Step 2: If certificate is valid, locate the **Valid Date** in the **Certificate Information** tab (default tab), shown below.

Valid Date 2015-01-06 07:00:00 EST TO 2017-01-10 07:00:00 EST

1. In *DCVv2*, record the validity dates, your name, and the date of the observation.
2. Repeat steps of **P2** with each unique Direct address whenever a new Direct certificate is issued or updated.

P3 – Download the IEHIE Trust Anchor

Step 1: The presence of an organization's Trust Anchor certificate in a Trust Bundle is the sole technical indication of a Participant's participation in the CTEN and conformance with the policies and procedures of a Trust Profile. Technical testing with other Participants of the CTEN will be accomplished using a Staging Trust Bundle.

1. Navigate to the MMD website, <http://www.maxmddirect.com/maxmdirect-certificate-search.html>.
2. In the field, enter any current Direct address and press **Search with CA Chain**.
3. Scroll down to the **Certificates and CAs** section.
4. The second blue box (Depth 1) contains the public key for the IEHIE.



Certificate and CAs

Max-Depth 10

CERT Subject : C=US, ST=Ca, [redacted]
Issuer: C=US, O=Inland Empire EHR Resource Center, OU=Inland Empire Health Information Exchange, CN=Inland Empire Health Information Exchange
CA-Issuer: <http://cacerts.digicert.com/InlandEmpireHealthInformationExchange.crt> [View Openssl Text](#)
OCSP - URI: <http://ocsp.digicert.com>
Subject Key Identifier: [redacted] [View Openssl Text](#) [PEM](#) [DER](#)

Depth 1

CA Subject : C=US, O=Inland Empire EHR Resource Center, OU=Inland Empire Health Information Exchange, CN=Inland Empire Health Information Exchange
Issuer: C=US, O=Orion Health Inc., OU=Orion Health Direct Secure Messaging, CN=Orion Health Direct Secure Messaging CA
SHA256: 1E:72:D8:3E:D9:49:9C:BA:68:69:68:45:2B:E5:91:C4:88:16:EC:91:81:39:1A:5D:03:C1:F4:D3:BA:16:58:DC
Valid Date: 2014-01-08 07:00:00 EST 2024-01-08 07:00:00 EST
CA-Issuer: <http://cacerts.digicert.com/aiaOrionHealthIssuingCAs.p7c> [View Openssl Text](#)
OCSP - URI: <http://ocsp.digicert.com>
Subject Key Identifier: 0C:95:F0:47:52:DB:4B:A4:EB:E7:47:D2:89:B6:5C:D1:AF:3A:30:10 [View Openssl Text](#) [PEM](#) [DER](#)

Depth 2

CA Subject : C=US, O=Orion Health Inc., OU=Orion Health Direct Secure Messaging, CN=Orion Health Direct Secure Messaging CA
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Federated Trust CA
SHA256: A4:10:6D:A8:5F:7B:34:A6:D3:DE:37:88:4D:15:28:91:6B:84:F0:46:FF:B7:D4:AA:C5:21:11:7B:0C:69:95:F3
Valid Date: 2013-10-21 08:00:00 EDT 2023-10-23 08:00:00 EDT
CA-Issuer: <http://cacerts.digicert.com/aiaOrionHealthDirectSecureMessagingCA.p7c> [View Openssl Text](#)
OCSP - URI: <http://ocsp.digicert.com>
Subject Key Identifier: A5:6E:22:FF:39:69:3A:23:FB:89:24:17:C6:60:94:00:1A:DA:8E:9E [View Openssl Text](#) [PEM](#) [DER](#)

5. Download the DER certificate.
6. If sending the certificate to CTEN, change the .der file type to .txt or compress the file into a .zip to avoid issues with email virus scanners.

Note 2: This image shows the certificate chain of custody. The first blue box (Max-Depth 10) is the certificate for the Participant whose Direct address was searched. The green box (Depth 2) is the certificate for Orion Health DSM, with who IEHIE current contracts DSM services.

P4 – Verify Inclusion of Certificates into CTEN Trust Bundle

Step 1: Trust among CTEN Members is established using collections of digital certificates. To retrieve copies of specific trust bundles, the publication site for CTEN Trust Bundles can be found at <https://cten.ca-hie.net/bundles>.

1. Navigate to the CTEN website and locate the **CTEN Production Trust Bundles**.
2. Press **Show Bundle Details** for the **CTEN Direct Trust Bundles** group.

CTEN Direct Trust Bundle

Profile: California Trusted Exchange Network (CTEN) Direct Messaging

Policy: [CTEN-Policy-EPP-2-for-Direct-v1.0.pdf](#)

[[Show Bundle Details](#)] [[Download JSON Metadata](#)] [[Download Bundle](#)] - Last updated 31 Aug 2015 16:00 UTC

3. Verify that IEHIE is among **Participant** column. In the **Expires** column, verify that all other Participants have current Trust Anchors.

Profile:

California Trusted Exchange Network (CTEN) Direct Messaging

Distribution point:

<https://cten.ca-hie.net/bundles/CTEN-Direct-Trust-Bundle.p7b>

Valid from:

31 Aug 2015 16:00 UTC

Certificateificates:

Participant	Issuer	Expires	Serial Number
Axesson / SCHIE	DigiCert Federated Trust CA	8 Jan 2024	08 8F 6B 9D 51 E4 6E 38 2D 4D 50 F2 F3 FC F1 C8
RAIN Live Oak HIE	Live Oak DIRECT Trust Anchor	5 Mar 2023	00 8E 6E 3A 2E 6A 4A 6C F8
San Diego Health Connect	DigiCert Federated Trust CA	6 Aug 2023	09 54 76 28 F4 10 64 DB 09 50 87 10 09 50 67 3E

[[Hide](#)]

Step 2: In DCVv2, record the validity dates, your name, and the date of the observation.

1011. CTEN Use of Message Content	
Policy: 1011	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Message Content Shall Be Used Only as Indicated Below.

1. **Permitted Purpose.** CTEN Members shall only Transact Message Content for a Permitted Purpose as defined below. Each Member shall require that its Participants and Authorized Users comply with this provision.

Permitted Purpose shall mean one of the following reasons for which Participants or Authorized Users may legitimately Transact Message Content:

1. Treatment of the individual who is the subject of the Message;
2. Payment activities of the Health Care Provider for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan;
3. Health Care Operations of either
 - (a) the Submitter if the Submitter is a Covered Entity;
 - (b) a Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or
 - (c) the Recipient if (i) the Recipient is a Health Care Provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such Health Care Provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. §164.501 or health care fraud and abuse detection or compliance of such Health Care Provider, and, for Participants operating in California, in California Civil Code section 56.10;
4. Public health activities and reporting as permitted or required by Applicable Law, including the HIPAA Regulations at 45 C.F.R. §164.512(b) or 164.514(e);
5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content, provided that the purpose is not otherwise described in subsections 1-4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. “Meaningful use of certified electronic health record technology” shall have

the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102;

6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. §164.502(g) of the HIPAA Regulations and for Participants operating in California, in California Civil Code section 56.11(c); and
7. With regard to State Entities, uses and disclosures permitted by California law, including Civil Code sections 1798.24, 1798.24a and 1798.24b.

2. **Permitted Future Uses.** Subject to this Section (Permitted Future Uses) and CalDURSA Section 19.7 (Disposition of Message Content on Termination), Recipients may retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient's record retention policies and procedures. If the Recipient is a CTEN Member that is a Business Associate of its Participants, such Member may retain, use and re-disclose Message Content in accordance with Applicable Law and the agreements between the CTEN Member and its Participants.
3. **Management Uses.** The CTEN Interoperability Committee may request information from CTEN Members, and Members shall provide requested information, for the purposes listed in Section 4.3 (Grant of Authority) of the CalDURSA relating to management of CTEN. Notwithstanding the preceding sentence, in no case shall a CTEN Member be required to disclose (i) PHI to the Interoperability Committee in violation of Applicable Law or (ii) Participant Confidential Information. Any information, other than Message Content, provided by a CTEN Member to the Interoperability Committee shall be labeled as Confidential Participant Information and shall be treated as such in accordance with Section 16 (Confidential Participant Information) of the CalDURSA.

1012. CTEN Confidential Participant Information

Policy: 1012

Version: 1.0

Date: September 29, 2015

Approved: Leo Pak

Confidential Participant Information

1. **Agreement not to redisclose.** Each Receiving Party shall hold all Confidential Participant Information in confidence and agrees that it shall not, during the term or after the termination of this Participation Agreement, redisclose to any person or entity, nor use for its own business or benefit, any information obtained by it in connection with this Participation Agreement, unless such use or redisclosure is permitted by the terms of that Agreement.
2. **Conditions of redisclosure.** Confidential Participant Information may be redisclosed as required by operation of law, provided that the Receiving Party immediately notifies the Discloser of the existence, terms and circumstances surrounding such operation of law to allow the Discloser its rights to object to such disclosure. If after Discloser's objection, the Receiving Party is still required by operation of law to redisclose Discloser's Confidential Participant Information, it shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

1013. CTEN Safeguards	
Policy: 1013	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

Safeguards

In accordance with Enterprise Security, Equipment and Software, and Auditing which follow. CTEN Member (“Member”) agrees to use reasonable and appropriate administrative, physical, and technical safeguards and any Performance and Service Specifications and Operating Policies and Procedures to protect Message Content and to prevent use or disclosure of Message Content other than as permitted by IEHIE Policy 1011 (Use of Message Content).

Enterprise Security

General

Each Member shall be responsible for maintaining a secure environment that supports the operation and continued development of the Performance and Service Specifications. Participants shall use appropriate safeguards to prevent use or disclosure of Message Content other than as permitted by the Participation Agreement and including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Message Content. Appropriate safeguards for Non-Federal Participants shall be in state law, or those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, “required” implementation specifications, and “addressable” implementation specifications to the extent that the “addressable” implementation specifications are reasonable and appropriate in the Member’s environment, or both. If an “addressable” implementation specification is not reasonable and appropriate in the Member’s environment, then the Member shall document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate. Appropriate safeguards for Federal Participants shall be those required by Applicable Federal Law related to information security. Each Member shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the Member’s respective Effective Date. Member shall also be required to comply with any Performance and Service Specifications or Operating Policies and Procedures adopted by the CTEN Interoperability Committee, respectively, that define expectations for Participants with respect to enterprise security.

Malicious Software

Each Member shall ensure that it employs security controls that meet applicable industry or Federal standards so that the information and Message Content being Transacted and any method of Transacting such information and Message Content will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, “malware,” or other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Member 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 a System or any part thereof

or any hardware, software or data used by a Member in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Member shall use all commercially reasonable efforts to comply with the requirements of this Section.

Equipment and Software

Each Member shall be responsible for procuring, and assuring that its Participants have or have access to, all equipment and software necessary for it to Transact Message Content. Each Member shall ensure that all computers and electronic devices owned or leased by the Member and its Participants that will be used to Transact Message Content are properly configured, including, but not limited to, the base workstation operating system, web browser, and Internet connectivity.

Auditing

Each Member represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to the CalDURSA, for system administration, security, and other legitimate purposes. Each Member shall perform those auditing activities required by the Performance and Service Specifications.

1014. Direct Secure Messaging User Setup	
Policy: 1014	Version: 1.0
Date: September 29, 2015	Approved: Leo Pak

New User Process Description

The typical new user is set up for Direct Secure Messaging (DSM) as follows:

1. A user is only set up after the user applicant has completed the identity verification process (Policy 102, User Identification Verification). Either the IEHIE Direct Administrator or a delegated Direct Administrator in a participant organization provides the new user applicant with instructions for self-registration using a secure web link only available for administration purposes. The applicant enters personal demographics, work site, and submits the information.
2. The responsible Direct Administrator receives an email that the application is complete, logs on to the administration site, reviews the application, and if it is satisfactory (expected identity-verified person) and complete, the Administrator accepts it. The system sends the applicant an email indicating acceptance. The Administrator sends the applicant instructions to log on to the DSM user site for the first time using a username produced by the system, normally "First.Last" names and a temporary password.
3. When the user logs on for the first time, the user is asked to change the password and provided length and character variety requirements. The user is also asked to select and respond to three Challenge Questions. In the future, should the user forget the password or miss-type it three times, the user will be asked to answer the Challenge Questions. If answered correctly, the user can select a new password, which cannot repeat a prior password for six (6) changes and cannot be largely similar to a past password.
4. The system requires that a user's password be changed every ninety (90) days.