WILLIAM T FUJIOKA
Chief Executive Officer

County of Los Angeles
CHIEF EXECUTIVE OFFICE

Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
http://ceo.lacounty.gov

"To Enrich Lives Through Effective And Caring Service"

March 19, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

REQUEST TO AUTHORIZE THE DEPARTMENT OF HEALTH SERVICES TO EXECUTE THE LOS ANGELES NETWORK FOR ENHANCED SERVICES DATA EXCHANGE PARTICIPATION AGREEMENT
(ALL DISTRICTS AFFECTED)
(3 VOTES)

SUBJECT

Authorization for the Department of Health Services to participate in the Los Angeles Network for Enhanced Services Health Information Organization and to execute the Los Angeles Network for Enhanced Services Data Exchange Participation Agreement to electronically exchange health information with other providers of health care services in Los Angeles County to improve health care delivery.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Department of Health Services (DHS) to participate in the Los Angeles Network for Enhanced Services (LANES) Health Information Organization (HIO) and the Director of the Department, or his designee, to sign the LANES Data Exchange Participation Agreement (Participation Agreement), substantially similar to Attachment I, to enable DHS to participate in the LANES HIO. The Participation Agreement is effective upon execution by the parties and remains effective until terminated by either party.

2. Delegate authority to the Directors of other County departments that provide health care, including the Department of Mental Health (DMH), the Department of Public Health (DPH), the Probation Department, and the Sheriff, or their designee, to participate in the LANES HIO and to sign the Participation Agreement, substantially similar to Attachment I, with approval by County Counsel, the Chief Health Information Portability and Accountability Act (HIPAA) Privacy Officer, and the Chief

Information Security Officer, and 30 days prior notification to the Board.

3. Delegate authority to the Directors of the Departments that execute the Participation Agreement, or their designee, to execute amendments to the Participation Agreement, provided that: 1) any such amendment is necessary to improve operational efficiencies and/or provides for greater privacy and/or security protections and/or is necessary to meet a Department's operational needs; or is required to comply with new or revised legal requirements; or is necessary to effectuate the purpose of the LANES HIO; 2) approval of County Counsel, or his designee, is obtained prior to execution of any such amendment; and 3) the Director of the applicable Department notifies the Board and the Chief Executive Officer (CEO) of Participation Agreement changes in writing 30 days prior to execution of any such amendment.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The recommended actions will enable DHS to participate in the LANES HIO in order to share health information. The LANES HIO will improve health care delivery by facilitating access to and retrieval of clinical data by and among providers in Los Angeles County. The Participation Agreement sets forth the conditions by which information in the HIO may be accessed, and mandates various privacy and security standards necessary to comply with State and federal law. Execution of the Participation Agreement by DHS is required for DHS, or any other Department, to participate in and for its health information system to connect to the HIO.

The recommended actions also authorize other Departments that provide health care services, upon concurrence of the Chief HIPAA Privacy Officer, Chief Information Security Officer, and County Counsel, and with prior notice to your Board, to participate in and connect their health information systems in the future to the HIO.

The recommendation actions will also provide authority to execute amendments to the Participation Agreement so that as experience with the HIO matures and/or new information requirements or standards are imposed modifications to the Participating Agreement can be timely made.

LANES is a collaborative of health care providers and other organizations from both the public and private sector, including the County, seeking to improve health care delivery in Los Angeles County, primarily through electronic health information exchange (HIE). The vision of LANES is to provide an integrated, secure and forward looking management system that will facilitate the provision of legally permissible and timely, patient-centered and high-quality health care across the continuum of services, and the continuous quality improvement of healthcare and public health processes and outcomes. HIE capacity and capability is fundamental to achieve this vision.

On May 31, 2011, the Board authorized the Chief Executive Officer (CEO), on behalf of LANES, to execute a grant agreement to accept funds under a State Cooperative Grant Agreement with the federal Office of the National Coordinator for Health Information Technology and efforts by LANES to develop HIE capacity began in earnest. HIO's (organizations that facilitate HIE) provide the capability to electronically move clinical information between disparate health care information systems while maintaining the meaning of the information being exchanged. The HIO acts as a conduit to facilitate, to the extent legally permissible, the participants' secure and electronic exchange of protected health information (PHI) directly with each other, and each participant retains responsibility for assuring its privacy and security.

Presently, LANES remains a collaborative of public and private providers, including the County. As a

collaborative, LANES acts through Public Health Foundation Enterprises, Inc. (PHFE) as its fiscal intermediary. PHFE will execute the Participation Agreement on behalf of LANES, and LANES, PHFE, and the LANES' HIO technology vendor, will each execute required HIPAA business associate agreements to ensure that the information shared has adequate privacy and security safeguards.

The technical work of connecting DHS to the LANES HIO infrastructure is currently underway. We estimate that DHS will be connected to the system and ready to begin sharing data in mid-April 2013. LANES may implement a pilot project in order to slowly roll-out use of the system to a limited number of users at that time. For the other County departments that may connect to the LANES HIO, we do not yet have estimated timeframes for them doing so. DMH, Probation, and the Sheriff are all in the process of implementing or upgrading their respective electronic health record systems, and will not be in a position to connect to LANES until such time those efforts are completed. We will separately report any updates in this regard separately to the Board.

Implementation of Strategic Plan Goals

The recommended actions support Goal 1, Operational Effectiveness, of the County's Strategic Plan.

FISCAL IMPACT/FINANCING

There is no financial impact of signing the LANES Participation Agreement at this time. The LANES HIO development is being funded by a $1.0 million grant from the California Health and Human Services Agency. In the future, the LANES participants will need to pay fees to participate in the LANES HIO to support the ongoing annual cost of the HIO. LANES continues to work on a sustainability model in order to develop annual fees for participation in the LANES HIO. Once these annual fees are finalized, the participants can review the fees and determine if they want to continue to participate in the LANES HIO. There will be no penalty if they choose to withdraw. If they choose to continue their participation and agree to the fees, they will incur fees until such time they terminate their relationship with LANES. We will return to the Board in order to present the fees and request approval to pay the associated fees in order to continue participation in the LANES HIO.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The Health Information for Economic and Clinical Health Act (HITECH) provides a strong foundation for developing HIE relationships and business models. Together with HIPAA, these provisions reflect a balance between protecting the privacy of individuals' PHI and assuring that such health information is readily available to health care providers who need access to such information to provide health care to their patients.

The Participation Agreement provides assurances that the participants will only access health information for the purposes described in the agreement. The LANES Participation Agreement only allows access to patient information for the treatment of patients. Because the use and disclosure of health information through the HIO is for treatment, authorization by the patient is not required.

To participate in the LANES HIO, participants must sign the LANES Participating Agreement. Participants can include: 1) Health care providers such as hospitals; 2) Physicians and Physicians Groups; and 3) Other providers such as laboratories and imaging providers.

In order to ensure that all legal requirements and the County security standards were met, the LANES Participation Agreement was developed by a County workforce team that included subject

matter experts from County Counsel, CEO, the Chief Information Office (CIO), the Auditor-Controller HIPAA Compliance Unit, the County Chief Information Security Officer, DHS, and DMH.

The County workforce team's draft was reviewed and approved by the LANES Security and Privacy Policies Committee and is now being reviewed for approval by each of the LANES Board members.

The LANES Participation Agreement establishes the relationship and describes the roles and responsibilities between LANES and the Participants through the LANES HIO. Participants will act as Data Providers and/or as a Data Recipients. Data Providers submit information to the LANES HIO and Data Recipients will use the LANES HIO to obtain that information.

The Participation Agreement establishes the obligations, permitted and required uses and disclosures of PHI and defines the privacy and security requirements for each of the participants. The LANES Participation Agreement:

- Requires participants to have appropriate safeguards to prevent wrongful uses or disclosures of PHI.

- Requires participants to report to the LANES Board any known uses or disclosures not provided for in the Participation Agreement.

- Requires participants to ensure that any agents, including subcontractors, who have access to the data, agree to the same restrictions and conditions that apply to the participant.

- Requires participants to ensure that workforce members who access the HIO are trained and sign a confidentiality statement that includes, at a minimum, general use, security safeguards, acceptable use, and policies.

The LANES Participation Agreement includes the following security provisions:

- Requires participants to implement administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of the electronic patient information that it creates, receives, maintains, or transmits.

- Defines security controls that satisfy all applicable federal and State regulations and standards.

- Provides for audit and accountability capabilities that will be present to record activity related to access, creation, modification, and deletion of HIO data.

- All data stored and transmitted will be secured (e.g., encryption).

STATE AND FEDERAL REQUIREMENTS

The California Office of Health Information Integrity (CalOHII) lead a Task Group composed of diverse stakeholders that worked together to develop the Model Modular Participants Agreement (MMPA) released in October 2012. The MMPA set the State's standards for HIE. The County workforce team compared the LANES Participation Agreement to the State MMPA and revised it accordingly to ensure that the provisions were in alignment with or exceeded the State MMPA.

The LANES Participation Agreement also addresses the following federal requirements:

- HIPAA Privacy Standards that require certain entities to adopt appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

- Requirements related to individual permission required to access certain information, i.e. role-based access for authorized users.

- The HITECH Act Breach Notification Rule which requires notification of individuals and HHS of privacy breaches in certain circumstances.

The LANES Participation Agreement has been reviewed and approved by County Counsel as to form and contains those required provisions necessary to comply with State and federal law, including HIPAA. The Participation Agreement aligns with the MMPA and does not include standard County terms and conditions. The Participation Agreement provides for mutual indemnification by the parties. The Participation Agreement is effective upon execution by the parties and remains effective unless terminated by either party upon 45 days written notice.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

This action will benefit the County in its efforts to facilitate legally permissible data sharing in the Los Angeles County region and support partnerships with private providers in order to provide improved healthcare to County residents.

Respectfully submitted,

WILLIAM T FUJIOKA

Chief Executive Officer

WTF:AJ:MLM
MM:ljp

Enclosures

c: Executive Office, Board of Supervisors
County Counsel
Chief Information Officer
Health Services
Mental Health
Probation
Public Health
Sheriff

LOS ANGELES NETWORK FOR ENHANCED SERVICES

LANES

Electronic Health Information Data Exchange Participation Agreement

PARTICIPATION AGREEMENT

BY AND BETWEEN

THE LOS ANGELES NETWORK FOR ENHANCES SERVICES
("LANES")

AND

THE COUNTY OF LOS ANGELES

DEPARTMENT OF HEALTH SERVICES

FOR

ELECTRONIC HEALTH INFORMATION DATA EXCHANGE

_____, 2013

LANES

ELECTRONIC HEALTH INFORMATION DATA EXCHANGE PARTICIPATION AGREEMENT

TABLE OF CONTENTS

LANES

ELECTRONIC HEALTH INFORMATION DATA EXCHANGE PARTICIPATION AGREEMENT

This Agreement, including the Exhibits, contains the entire agreement between LANES and the Participant and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement and the Exhibits may be amended as described herein:

RECITALS

WHEREAS, Los Angeles Network for Enhanced Services ("LANES") is a collaborative organization representing a number of concerned organizations seeking to improve the health care delivery in Los Angeles County. One component of LANES is a Health Information Exchange which is operating as a Health Information Sharing Organization (HIO). LANES' HIO is organized and operated for the purpose of facilitating the secure and appropriate sharing of electronic health files and clinical data among health care providers and other participants in Southern California for treatment and care coordination, in an atmosphere of transparency and mutual trust. LANES may in the future participate in other regional and national electronic health information exchanges; and

WHEREAS, LANES provides or arranges for the provision of data transmission and related services to allow Participants to conduct searches for Patient Information, and to exchange Patient Information identified from those searches, from a federated computer system that facilitates the sharing of Patient Information among disparate Participants. LANES's services include establishing and applying standards for such exchange of Patient Information. LANES has access to and/or is responsible for maintaining some or all of such Patient Information in the performance of LANES' services. LANES also aggregates and/or maintains a repository of Patient Information; and

WHEREAS, this LANES Data Exchange Participation Agreement (the "Agreement") sets forth the terms and conditions upon which the Participant will participate in the HIO and is made and entered into as of the Effective Date set forth on the signature page hereof ("Effective Date"), by and between LANES and the participant named on the Signature Page ("Participant"), with reference to the following facts:

The Participant wishes to participate in the electronic health information exchange or HIO facilitated by LANES, in accordance with the terms and conditions of this Agreement; and

WHEREAS, the Participant shall participate in the HIO, as and to the extent described herein, and subject to and in accordance with the terms and conditions of this Agreement.

NOW THEREFORE, IN CONSIDERATION of the recitals, covenants, conditions and promises herein contained, and for other valuable consideration, the receipt and sufficiency of which the parties hereby acknowledge and LANES and the Participant hereby agree as follows:

I. APPLICABLE DOCUMENTS

Exhibits A, B, C, D, E, F and G are attached to and form a part of this Agreement. In the event of any conflict or inconsistency in the definition or interpretation of any word, responsibility, or contents or description of any task, or responsibility between the base agreement and the Exhibits, or between Exhibits, such conflict or inconsistency shall be resolved in a manner that advances the purpose and intent of this Agreement. Exhibits to this Agreement are as follows:

1. Exhibit A (Participation), attached hereto, which sets forth a general description of the Program(s) in which the Participant shall participate, and any additional terms and conditions that shall apply specifically to that participation.

2. Exhibit B (Technical and Security Specifications), attached hereto, which sets forth the technical and functional specifications with which the Participant shall comply in order to participate in the Program(s) as a Data Provider and/or Data Recipient.

3. Exhibit C (LANES Security & Privacy Policies), attached hereto, which sets forth the General Security Safeguards and Controls with which the Participant shall comply in order to participate in the Program(s).

4. Exhibit D (Participation Fees), attached hereto, which sets forth the fees and other amounts that the Participant shall pay to LANES in exchange for participation in the Program(s) on Exhibit B (Participation).

5. Exhibit E (Business Associate Agreement), attached hereto, which sets forth the terms and conditions upon which LANES may access Patient Information, as the business associate of the Participant.

6. Exhibit F (Role-based Access Matrix), attached hereto, which sets forth the roles and responsibilities of the Participants and Authorized Users.

7. Exhibit G (Matrix of Components Roles and Responsibilities), attached hereto, which identifies the components of the System.

This Agreement and the Exhibits hereto constitute the complete and exclusive statement of understanding between the parties, and supersedes all previous agreements, written or oral, and all communications between the partied relating to the subject matter of this Agreement. No change to this Agreement shall be valid unless prepared pursuant to the Amendment provision of the Agreement and signed by both parties.

II. DEFINITIONS

The meanings of all terms used in this Agreement shall be consistent with the defined terms set forth in this Section II (Definitions)

1. "Access" means the ability or the means necessary to view and read patient information by an Authorized User. Access includes the transfer of data from one Authorized User's electronic device to another Authorized User's electronic device through the Network.

2. "Administrative Safeguards" means administrative actions, and policies and procedures to manage the selection, development, and maintenance of security and privacy measures to protect electronic individually identifiable health information and to manage the conduct of the entity's workforce in relation to the protection of that information. Administrative safeguards include policies and procedures, workforce training, risk management plans, and contingency plans.

3. "Authorization" means the process used to determine whether a particular individual has the right to access information through the Network. Role-based access standards will be taken into account consistent with an individual's job function and the information required to perform his/her role.

4. "Authorized User" means an individual designated by LANES or the Participant to Access and use the Network, i.e., a natural person, who is authorized by a Participant to use the services on behalf of that Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant's medical staff. If the Participant is an individual, e.g., a physician, then that individual is both a Participant and an Authorized User.

5. "Business Associate" has the same meaning as the term "business associate" in 45.C.F.R. 160.103.

6. "CMIA" means the California Confidentiality of Medical Information Act, California Civil Code Section 56 et. seq.

7. "Covered Entity" has the same meaning as the term "covered entity" in 45 C.F.R. 160.103.

8. "LANES Data Exchange Participation Agreement" means a written agreement between LANES and a Participant, pursuant to which that Participant agrees to act as a Data Provider and/or a Data Recipient.

9. "Data" means the LANES' Participant's patient's information which is available to be exchanged for treatment and care coordination purposes.

10. "Data Elements" means those elements of patient information which the Data Provider has determined appropriate for access by the Data Recipient that reflect a core data set of the most relevant administrative, demographic, and clinical information or facts about a patient's healthcare, covering one or more healthcare encounters of the pertinent data to support the continuity of the patient's care.

11. "Data Provider" means a designated Participant that is registered to provide Patient Information electronically to the LANES search portal.

12. “Data Recipient” means a designated Participant who based on their defined role based access requirements may Use Patient Information received from the LANES’ search portal for treatment of the individual as long as the Participant either has or had a relationship with the individual who is the subject of the information.

13. "De-Identified Data" means Participant's Data which meets the standard for de-identification in 45.C.F.R. 164.514(b).

14. "Disclose" or "Disclosure” means with respect to Patient Information or Protected Health Information the release, transfer, exchange, provision of access to, or divulging in any other manner of Data outside the holding entity's internal operations or to other than its workforce.

15. “Edge Server” means a physical, virtual or hosted server, part of the LANES infrastructure, that meets the security requirements established by HIPAA and is within the participants’ (or the hosted vendors’) firewall and used as a message collection and gateway for all clinical data that the Participant is going to share. See Exhibit G (Matrix of Components Roles and Responsibilities).

16. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and the regulations promulgated thereunder at 45 CFR Parts 160 and 164.

17. “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).

18. "Individually Identifiable Health Information" has the same meaning as the term "individually identifiable health information" in 45 C.F.R. 160.103.

19. "Participant" means an individual or entity that has entered into the LANES Data Exchange Participation Agreement with LANES to act as a Data Provider and/or as a Data Recipient.

20. "Participation Agreement" means a legally binding written data exchange agreement pursuant to which a Participant has agreed to act as a Data Provider and/or as a Data Recipient in accordance with terms and conditions this Agreement.

21. “Participant’s System” means the electronic health information exchange infrastructure and/or hardware and software controlled by the Data Participant through which the Data Participant conducts its health information exchange related activities pursuant to its Data Exchange Participation Agreement.

22. “Patient Information” means any information whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, insurer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual. Patient Information shall be treated as Protected Health Information as defined in 45 C.F.R. section 160.103.

23. "Policies and Procedures" means those policies and procedures adopted by LANES to describe the terms and conditions pursuant to which the system shall be operated.

24. "Program" the electronic health information exchange operated by LANES.

25. "Proprietary 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, whether written or verbal, that are confidential in nature; provided, however, that "Proprietary Information" does not include Patient Data or 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 this Agreement;

(c) Is independently developed by any other party; and/or

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

26. "Protected Health Information" or "PHI" has the same meaning as the term "protected health information" in 45 C.F.R. 160.103.

27. “Root Server” is a physical, virtual or hosted server that meets the security requirements established by HIPAA and is within the LANES HIO (or the hosted vendors’) firewall and used as a message collection and gateway for clinical data that the Participants are going to share. See Exhibit G (Matrix of Components Roles and Responsibilities).

28. "System" means the compilation of servers, applications, databases and networking components required to facilitate LANES's health information exchange.

29. "Unsecured Protected Health Information" has the same meaning as the term Unsecured Protected Health Information in Section 13402 of Title XIII, 45 C.F.R. 164.402.

30. "Use" has the same meaning as the term use in 45.C.F.R. §160.103.

III. LANES’ RESPONSIBILITIES

1. Data Exchange Participation Agreement Required. LANES shall only permit entities who enter into Data Exchange Participation Agreements with LANES to access the System and use the services. A Participant may act as a Data Provider or as a Data Recipient, or as both. LANES may periodically enter into Data Exchange Participation Agreements with other Participants approved by LANES. All Data Exchange Participation Agreements to participate in any of the LANES Program(s) and amendments shall be subject to LANES’ approval.

2. Controlling Access to Patient Information. Except as described in this Section, LANES shall make Access to Patient Information available only to Participants and their respective Authorized Users, and only for purposes of treatment and care coordination, as defined under HIPAA, of an individual with whom the Participant healthcare provider has a patient relationship. Without limiting the foregoing, LANES shall make Access to Patient Information available only to Authorized Users, and only to the extent that each such Authorized User reasonably requires such Access in order to perform the responsibilities assigned to him or her.

3. System Availability. LANES shall exercise commercially reasonable efforts to make the Network available to Participants twenty-four (24) hours per day, seven (7) days per week, three hundred sixty five (365) days per year; provided, however, that the availability of the Network may be temporarily suspended for maintenance or unscheduled interruptions. LANES shall exercise commercially reasonable efforts to provide the Participant with advance notice of any such suspension or interruption of Network availability. Without limiting the foregoing, Participants shall be responsible for obtaining Patient Information through means other than the Network during any periods during which the Network is unavailable.

4. Compliance with Laws and Regulations. LANES shall comply with all laws and regulations applicable to its operations, including all applicable federal and State patient privacy and security laws.

5. Use and Disclosure of Patient Information. LANES shall Access, Use and/or Disclose Patient Information solely in its capacity as a "Business Associate" and otherwise as required for LANES' compliance with applicable laws and regulations and other requirements imposed or orders issued by any government agency or court with competent jurisdiction. LANES shall enter into a "business associate agreement" with each Participant, as required by HIPAA. Without limiting the generality of the foregoing, LANES shall not be or act as a Data Recipient. However, to the extent necessary, LANES shall be permitted to Access and Use Patient Information through the Network for the purposes of maintaining the Network and/or its resources and otherwise as required for the performance of LANES' responsibilities as set forth herein.

6. Privacy and Security of Patient Information. LANES shall implement reasonable safeguards to protect Patient Information from unlawful, unauthorized and/or inappropriate Access, tampering or disclosure as articulated in the LANES Privacy and Security Policies and as required by the attached Business

Associate Agreement. LANES will establish policy guidance relative to authorization, authentication, access, and audit for the Network and Participants. As appropriate to do so, LANES will continue to review and enhance its Privacy and Security policies to ensure that the Network affords maximum protection to the information that flows through the Network.

7. Responsibility for Employees and Others. LANES shall inform its employees, workforce members as defined by HIPAA, contractors and/or other agents who perform Program functions, including without limitation its Authorized Users who have Access to Patient Information, of the applicable terms and conditions of this Agreement, including without limitation responsibilities and restrictions imposed by applicable laws and regulations regarding the privacy and security of Patient Information, such as the HIPAA Rules. LANES through their fiscal intermediary, Public Health Foundation ("PHFE") shall indemnify Participants for all acts and omissions by any of its Authorized Users and other employees, contractors and other agents in connection with their performance of Program functions, including without limitation any privacy and/or security breaches, any noncompliance with the terms and conditions of the applicable Data Exchange Participation Agreement, and their Access or Use of Patient Information.

8. Notification of Data Breaches. LANES in accordance with Exhibit E (Business Associate Agreement) shall notify Participants, agencies of federal, state and/or local government, and other parties, of any breach of Patient Information made available for Access through the Network, as and to the extent required by, and within the periods of time required by, applicable laws and regulations, as described in Exhibit C (Security and Privacy Policies).

9. Training and Support. LANES shall provide end-users training and technical support to Participants in the access and use of the system.

10. Telephone and/or E-Mail Support. At all times LANES shall provide, by telephone and/or e-mail, support and assistance in resolving difficulties in accessing and using the System and the services.

11. Patient Control. Each Participant shall provide patients with the right to control their patient information in accordance with the Participant's Notice of Privacy Practices. LANES shall implement and maintain a protocol through which patients may exercise choice concerning the Use and Disclosure of their Patient Information as described in the LANES Privacy and Security

Policies, and LANES shall comply with the requirements of that protocol.

12. Reporting of Inaccurate and/or Inappropriate Patient Information. LANES shall receive reports from Participants and others regarding inaccurate and/or inappropriate Patient Information, corruption, errors and/or omissions in Patient Information. In consultation with the Data Provider that has made the affected Patient Information available through the Program, LANES shall within a reasonable period of time not to exceed five business days inform the Data Provider if any Authorized User has Accessed the Patient Information. The Data Provider will inform the Authorized User of the inaccurate and/or inappropriate Patient Information.

13. Malicious Software, Viruses and Other Threats. LANES shall exercise commercially reasonable efforts to prevent exposure through the Network of the Participant's System to (i) any program, routine, subroutine, virus, data, cancelbot, Trojan horse, worm or other malicious software or harmful component that will disrupt the proper operation of the Participant's System; (ii) any unlawful, threatening, abusive, libelous, defamatory, or otherwise objectionable information of any kind, including without limitation any transmissions constituting or encouraging conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state or federal law; or (iii) any information that violates the proprietary rights, privacy rights, or any other rights of a third party, including without limitation any patient.

14. Accounting of Disclosures. LANES shall provide Data Providers with Access to the network so that they may produce Accountings of Disclosures of Patient Information or develop and maintain a process by which LANES shall provide such accountings to or on behalf of such Data Providers, in reasonably sufficient time for Participant to timely comply with the HIPAA's, accounting of disclosures mandate.

15. Reports. LANES shall provide periodic reports to Participants as needed and determined by LANES.

16. Regulatory Access to Books and Records. LANES shall, until the expiration of six (6) years after the furnishing of Data and services pursuant to the Agreement, make available, upon written request, to the Secretary of the United States Department of Health and Human Services or the Controller of the United States, or any duly authorized representatives, or as required by the Data Provider to this Agreement, and books, documents and records that are necessary to certify the nature and extent of the cost of services

provided pursuant to this Agreement. If LANES carries out any of its duties pursuant to this Agreement through a subcontract with a value of Ten Thousand Dollars ($10,000) or more over a 12-month period with a related organization, such subcontract shall contain a provision placing the same obligations on subcontractor as this provision places on LANES.

17. Portal Access. LANES shall make available a secure Web Portal for Data Recipients and Participants and their respective Authorized Users. Authorized Users may access Patient Information through this portal.

IV. Participant's Responsibilities

1. Participation in Program. The Participant shall participate in the Program in accordance with the terms and conditions of the Participant's Data Exchange Participation Agreement.

2. Grant of Rights. The Participant may use the System and the services for the permitted uses described in Permitted Uses section, subject to the Participant's full compliance with this Agreement. LANES retains all ownership and other rights to the System, the services and all the components thereof. The Participant shall not obtain any rights to the System except for the limited rights to use the System expressly granted by this Agreement.

3. Permitted Uses. The Participant may use the System and the services only for purposes authorized by this Agreement.

4. Prohibited Uses. The Participant shall not use or permit the use of the System or the services for any prohibited use described in Exhibit C (LANES Security & Privacy Policies). Without limiting the foregoing, The Participant shall not use the System or the services for any purpose or in any manner that is prohibited by applicable federal and State laws and regulations.

5. No Services to Third Parties. Except as expressly permitted by the applicable Data Exchange Participation Agreement, the Participant 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 equivalent services to a third party.

6. Compliance with Laws and Regulations. The Participant shall comply with all federal, state and local laws, ordinances, and regulations, including HIPAA and HITECH/ARRA, as applicable to the activities it conducts pursuant to its participation in the Program.

7. Access to Patient Information for Permitted Use Only. The Participant shall Access Patient Information through the Program only as provided in this Agreement.

8. Limitations on Use of Patient Information. Any Use or Disclosure by the Participant of Patient Information obtained through the Network shall be solely in the Participant's capacity as a "covered entity" within the meaning of 45 C.F.R. § 160.103 or as a health care provider or health care facility licensed under California law. In accordance with Exhibit A (Participation) of this Agreement, the Participant shall not Use or Disclose any Patient Information to compare the performance of health care services by one or more Participants against such performance by one or more other Participants.

9. Identification of Authorized Users. The Participant shall provide LANES with a list identifying all of the Participant's Authorized Users, in accordance with the requirements of this Agreement. The Participant shall restrict Access to the system and, if applicable, use of the services, only to the Authorized Users in accord with the level of access identified in Exhibit F (Role-based Access Matrix) that the Participant has so identified to LANES. The Participant shall inform LANES in writing within two (2) business days whenever an Authorized User is added or removed.

10. Certification of Authorized Users. The Participant shall certify to LANES that each of the Participant's Authorized Users:

    (a) Has completed a privacy and security training program conducted by the Participant and the LANES end user training;

    (b) Will be permitted by the Participant to use the services and the System only as reasonably necessary for the performance of the Participant's activities as described herein;

    (c) Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized User pursuant to Passwords and Other Security Mechanisms Section (11); and

    (d) Has acknowledged in writing that the Authorized User's failure to comply with this Agreement may result in the withdrawal of privileges to use the services and the System and may constitute cause for disciplinary action by Participant and possible for civil and/or criminal penalties.

(e) When the Participant informs LANES of the removal of any Authorized User, LANES shall promptly de-activate the user name and password and/or other security measures of such individual.

(f) The Participant shall define and provide to LANES the role based access requirements for each of the Participant's Authorized Users as identified in Exhibit F (Role-based Access Matrix).

11. Responsibility for Acts of Authorized Users and Others. The Participant shall be responsible for all acts and omissions, including without limitation privacy or security breaches and/or failures to comply with the requirements of this Agreement, by the Participant's employees, work force members, contractors, agents and/or any other persons who are authorized to Access or Use the Network or Patient Information pursuant to the Participant's Data Exchange Participation Agreement, including without limitation the Participant's Authorized Users.

12. Passwords and Other Security Mechanisms. LANES shall issue a user name and password and/or other security measures, as described in Exhibit C (LANES Security & Privacy Policies), to each Authorized User that shall permit the Authorized User to Access the System and use the services. LANES shall provide each such user name and password and/or other security measures to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User.

13. 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 that Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from that Participant or any of that 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 that Participant.

(a) In particular and without limiting the foregoing, Participants that are Covered Entities shall be responsible for all acts or omissions of Participant's Business Associate(s) with respect to this Agreement and for enforcement of the provisions of Participant's business associate agreement(s). Participant's

business associate agreements shall meet the requirements of 45 C.F.R. 164.314(a).

(b) HIPAA-covered entities will be accountable for the actions of their workforce, as well as the contents and enforcement of their business associates agreements. See 45 C.F.R. §§164.530(b)(e) and 164.504(e). Covered entities will not be liable for the violations of other Participants.

14. Liability for Violations of the HIPAA Privacy and Security Rules. Participants are responsible for their own non-compliance with the Privacy Rule, as well as that of their workforce. Participant is obligated to promptly report noncompliance with the HIPAA Privacy Rule and this Agreement's terms to the LANES HIO Vendor. Where a business associate agreement (BAA) exists between a Participant and any business associate for the electronic exchange of PHI provided through the LANES HIO Vendor, the Participant's BAA must contractually obligate that the business associate to: 1) report any uses or disclosures of PHI that materially violate the agreement to the Participant; 2) be accountable for taking appropriate action to cure known noncompliance; 3) request satisfactory assurances that the business associate will adequately safeguard PHI; and, 4) if unable to do so, to terminate the business associate relationship. See 45 C.F.R. §§ 164.502 (e), 064.504(e). See also the parallel business associate requirements in the HIPAA Security Rule at 45 C.F.R. § 164.314(a).

15. Termination of Authorized Users. The Participant shall require that all of its Authorized Users use the System and the services only in accordance with this Agreement and the Policies and Procedures, including without limitation the provisions thereof governing the confidentiality, privacy and security of protected health information. The Participant shall impose appropriate sanctions against any of its workforce members who fail to act in accordance with this Agreement or the Policies and Procedures in accordance with that Participant's disciplinary policies and procedures.

16. Training. The Participant shall provide or arrange for appropriate training in the use of the Network and the requirements of this Agreement for all of the Participant's Authorized Users. The Participant shall inform its Authorized Users of the applicable terms and conditions of this Agreement and LANES Privacy and Security Policies, including without limitation responsibilities and restrictions imposed by applicable federal and State laws and regulations regarding the privacy and security of Patient Information.

17. Program Liaison; Program Team. The Participant shall designate a single individual (or a point of contact or an office) who shall be responsible for managing communications between the Participant and LANES. The Participant shall organize and maintain a Program Team in accordance with the requirements of this Agreement.

18. Access Controls. The Participant shall comply with this Agreement and the requirements contained herein for the application and administration of Access and Authentication controls upon use of the Network.

19. Audits for Unauthorized Use. The Participant shall monitor Access and use of the System and Patient Information on its behalf for the purpose of detecting unauthorized Access or use of the System or unauthorized Use of Patient Information through the Participant's connection(s) to the System. The Participant shall maintain an automated audit trail which can identify the user or system process which initiates a request for PHI or PII, or which alters PHI or PII. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If PHI or PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence. Participant shall notify LANES of any such unauthorized Access or use of the System or unauthorized Use of Patient Information in accordance with the requirements of this Agreement.

20. Participant's System. The Participant shall have the sole responsibility to obtain, install, and maintain at its own expense the Participant's Systems. LANES shall not be responsible for the Participant's inability to Access or use the System if that inability is for any reason other than the System's failure to comply with the specifications set forth in this Agreement or LANES's failure to perform its obligations under this Agreement, including without limitation any factors arising from the Participant's computing environment, software, interfaces, or hardware, or any upgrade or alteration to any of them.

21. Data Within Participant's Firewall. Participant shall be solely responsible for the control and protection of any and all data within the Participant's firewall, including without limitation Patient Information, and for the Participant's compliance with all federal and State laws and regulations.

22. Technology License Agreement. If LANES determines that it is necessary in order to obtain and or use the software and/or

hardware required to use the System, the Participant shall enter into one or more Technology License Agreement(s) in such forms as LANES requires.

23. System Availability. LANES shall exercise commercially reasonable efforts to make the Network available to Participants twenty-four (24) hours per day, seven (7) days per week, three hundred sixty five (365) days per year; provided, however, that the availability of the Network may be temporarily suspended for maintenance or unscheduled interruptions. LANES shall exercise commercially reasonable efforts to provide the Participant with advance notice of any such suspension or interruption of Network availability. Without limiting the foregoing, Participants shall be responsible for obtaining Patient Health Information through means other than the Program during any periods during which the Network is unavailable.

24. Protected Health Information

(a) Technical Safeguards. The Participant shall implement administrative physical and technical safeguards that reasonable and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that it creates, receives, maintains, or transmits.

(b) The Participant shall ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect health information.

(c) Implementation of technical safeguard's specifications also applies to certain situations in which other laws that require Participants to adhere to.

(d) Compliance with Policies and Procedures. LANES and the Participant shall comply with the standards for the confidentiality, security, and Use and Disclosure of patient health information, including without limitation Protected Health Information, described in HIPAA, and as provided in the Policies and Procedures. The Participant shall comply with such standards regardless of whether or not the Participant is a Covered Entity under HIPAA.

(e) Legal Requirements. LANES and the Participant shall comply with the requirements for the privacy, security, and Use and Disclosure of patient health information imposed

under Federal and State Laws, including but limited to HIPAA, HITECH. and CMIA.

(f) Reporting of Breaches. Participant shall report breaches in accordance with Exhibit C (LANES Security & Privacy Policies).

25. Additional Provisions Regarding Privacy and Security of Patient Information.

(a) Disclosures of De-Identified Data. LANES shall not disclose de-identified Patient Information unless and to the extent that LANES shall have obtained in advance the express authorization of the Data Provider that made that information available for Access through the System.

26. Other Obligations of the Participant.

(a) Compliance with Laws and Regulations. Without limiting any other provision of this Agreement requiring compliance with applicable laws and regulations, the Participant shall perform its roles and responsibilities hereunder in all respects in compliance with applicable federal, State, and local laws, ordinances and regulations.

27. System Security. The Participant shall implement reasonable and appropriate system security measures to prevent unauthorized Use, Access or Disclosure of Protected Health Information and other Patient Information.

28. Participant's Equipment. Except to the extent provided by the Technology License Agreement, the Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the services, and provide to LANES all information required to be provided by the Participant (Participant's Required Hardware and Software). The Participant's Required Hardware and Software shall conform to LANES's current and/or subsequently modified or agreed to 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 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.

29. 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 LANES or other Participants 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 LANES or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

30. Training. The Participant shall provide appropriate and adequate training to all of the Participant's workforce, including without limitation Authorized Users, in the use of the System and the services, the requirements of this Agreement and the Policies and Procedures, the requirements of applicable laws and regulations governing the confidentiality, privacy, Use, Disclosure, and security of Protected Health Information, and/or Patient Information including without limitation requirements imposed under and/or necessary for compliance with HIPAA.

V. LANES' Operations and Responsibilities

1. Compliance with Terms and Conditions. LANES shall require that Access to the System and the services shall be limited to Participants that have executed a Participant Agreement and to their Authorized Users.

2. Maintenance of System.

   (a) LANES shall maintain the functionality of the System and the services as described in Exhibit C (LANES Security & Privacy Policies), and shall provide such service, security, and other updates as LANES determines are appropriate from time to time.

   (b) LANES shall maintain the functionality of the System and the services as described in Exhibit B (Technical and Security Policies), and shall provide such service, security, and other updates as LANES determines are appropriate from time to time.

3. Operations Committee

(a) Organization. LANES shall form and maintain an Operations Committee, which shall act, as more specifically described in the Policies and Procedures, as a resource to LANES and its Board of Directors in the administration of LANES's program of electronic health information exchange, including the development of the Policies and Procedures and the amendment, repeal or replacement of Participation Agreement(s) and/or the Policies and Procedures.

(b) Powers. The powers of the Operations Committee shall be advisory only, and no action considered by the Operations Committee shall be taken or not taken except with the approval of LANES, acting either through its Board of Directors, management or staff.

(c) Compliance with Laws and Regulations. Without limiting any other provision of this Agreement requiring compliance with applicable laws and regulations, LANES shall perform its roles and responsibilities hereunder in all respects in compliance with applicable federal, state, and local laws, ordinances and regulations, including without limitation those provisions of HIPAA and/or HITECH.

4. Fees and Other Charges

(a) Services Fees. As payment for use of the System and the services, the Participant shall pay to LANES Service Fees as described in Exhibit D (Participation Fees).

(b) Other Charges. The Participant also shall pay LANES's charges for all goods or services that LANES provides at the Participant's request that are not specified in the Policies and Procedures in accordance with LANES's then-current Fee Schedule ("Miscellaneous Charges"). The Fee Schedule is subject to change at any time.

(c) Payment. The Participant shall pay all Service Fees and any Miscellaneous Charges within sixty (60) calendar days following the date of invoice by LANES sent to that Participant's address as shown in LANES's records or e-mailed in accordance with the Participant's instructions.

(d) Late Charges. Service Fees and Miscellaneous Charges not paid to LANES on or before the due date for those fees and charges 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 1/2%) per month on the outstanding balance, or the highest amount permitted by law, whichever is lower.

5. Suspension of Service. Failure to pay Service Fees and Miscellaneous Charges within sixty (60) calendar days following the due date for those fees and charges may result in termination of the Participant's access to the System and/or use of the services on ten (10) business days prior notice. A reconnection fee may be assessed to re-establish connection after termination due to non-payment, in accordance with LANES's then-current Fee Schedule.

6. 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 LANES's net income) that LANES 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 under this Agreement.

7. 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.

VI. **Proprietary Information**.

1. Scope of Proprietary Information. In the performance of their respective responsibilities pursuant to this Agreement, LANES and Participants may come into possession of certain Proprietary Information of the others.

2. Nondisclosure of Proprietary Information. LANES and the Participant each (i) shall keep and maintain in strict confidence all Proprietary 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 this Agreement; (ii) shall not use, reproduce, distribute or disclose any such Proprietary Information except as permitted by this Agreement; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure.

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

4. Notice of Disclosure. Notwithstanding any other provision hereof, nothing in this Section VI (Proprietary Information) shall prohibit or be deemed to prohibit a party hereto from disclosing any Proprietary 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.

VII. **Warranties and Disclaimers.**

LANES represents and warrants as follows: (i) it has the full power, capacity and authority to enter into and perform this Agreement and to make the grant of rights contained herein; (ii) its performance of this Agreement does not violate or conflict with any agreement to which LANES is a party; (iii) there is no pending or threatened litigation that would have a material adverse impact on its performance under this Agreement; and (iv) to the best of LANES's knowledge, Participants use of the Network pursuant to the terms and conditions of this Agreement shall not infringe the patent rights, copyrights or other intellectual property rights of any third party.

1. Disclaimers of Warranties. Except for the warranties set forth in Section VII, LANES provides access to the Network, Patient Information and use of documentation to the Participant "as is" and without any warranty of any kind to participants, whether express, implied or statutory. LANES does not warrant that the performance of the Network will be uninterrupted or error-free, or that all errors in the Network or Patient Information will be corrected; provided that the foregoing shall not relieve LANES from any of its express obligations set forth in this agreement. LANES hereby disclaims all implied and express warranties, conditions and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to quality, merchantability, fitness for purpose and non-infringement. In no event shall LANES or the Participant be liable to the other for any consequential, incidental, indirect, punitive, or special damages suffered by the other or any other third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions or other economic loss, directly or indirectly arising out of this agreement, the participant's use of the Network or any component thereof.

2. Any Patient Information. LANES shall not be liable for any damages arising out of or related to (i) the accuracy or completeness or inputting of Patient Information; or (ii) the acts or omissions of the Participant, whether suffered by LANES or any third party. LANES's total aggregate liability for any damages arising out of or related to this agreement will not exceed _____ except for LANES's breach of privacy, security or confidentiality obligations. LANES's total aggregate liability for any damages arising from LANES's breach of privacy, security or confidentiality obligations will not exceed _____. The existence of one or more claims shall not enlarge these limits. Each party acknowledges that the allocation of risk and the limitation of liability specified in this section will apply regardless of whether any limited or exclusive remedy specified in this agreement fails of its essential purpose.

3. Disclaimer of Responsibility. LANES accepts no responsibility for (a) the performance of the Prerequisite Systems or any other systems of the Participant, (b) the transmission of the Patient Information to or from the Network, (c) all use by the Participant and its employees, contractors or other agents of the Network, (d) the accuracy, completeness or appropriateness of Patient Information and any health care decision made in reliance, either in whole or in part, thereon; and (e) all Uses or Disclosures by the Participant of information obtained through the Network including, without limitation, Patient Information; provided however the

foregoing shall not limit LANES's responsibility for its obligations expressly set forth in this Agreement. The Participant and its employees, contractors and other agents shall be solely responsible for all decisions involving patient care, utilization management and quality management for its patients. Without limiting the generality of the foregoing, the Data Recipient shall have sole responsibility for the Use and Disclosure of Patient Information obtained through the Network, including without limitation all clinical decision-making based thereon or influenced thereby. The Network should be used as a supplement to, and not in place of, other data that is available to the Data Recipient and/or the treating health care provider in performing the above functions. The Participant shall have no recourse against LANES for any loss, damage, claim, or cost relating to or resulting from the use or mis-use of the Network by the Participant or data Accessed through the Network by the Participant; provided however the foregoing shall not limit LANES's responsibility for its obligations expressly set forth in this Agreement.

4. Non-Liability. Without limiting any other provision of this Agreement, LANES shall not be responsible for the act or omission of any Participant with respect to the use of the Network and Patient Information by Participants.

5. 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.

6. Unauthorized Access; Lost or Corrupt Data. LANES 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 that 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. LANES is not responsible for the content of any information transmitted or received through the System or the services. The Data Provider is solely responsible for the content of

all Patient Data that the Data Provider makes available pursuant to this Agreement.

7. Inaccurate Data. All data to which access is made through the System and/or the services originates from Data Providers, and not from LANES. 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. Without limiting any other provision of this Agreement, LANES 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.

8. Patient Care. Without limiting any other provision of this Agreement, the Participant and that 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. Neither the Participant nor any Authorized User shall have any recourse against, and shall waive, any claims against LANES 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.

9. Limitation of Liability. Notwithstanding anything in this Agreement to the contrary, to the maximum extent permitted by applicable laws, the aggregate liability of LANES, and LANES's officers, directors, employees, and other agents, to the Participant and the Participant's Authorized Users, regardless of theory of liability, shall be limited to the aggregate of Service Fees actually paid by that Participant in accordance with this Agreement for the six (6) month period preceding the event first giving rise to the claim.

VIII. INSURANCE AND INDEMNIFICATION

1. LANES Insurance

(a) Required Policies. LANES shall procure and maintain in effect during the term of this Agreement commercial liability insurance that will cover LANES’s liability with limits of not less than One Million Dollars ($1,000,000) per occurrence and Five Million Dollars ($5,000,000) in the aggregate.

(b) Carriers. All insurance required under this Section shall be carried by companies with a rating not lower than "A, X" by A.M. Best Company.

(c) Certificates of Insurance. On request of the Participant, LANES shall promptly provide the Participant with a certificate of insurance evidencing the aforementioned coverage, and shall notify the Participant immediately upon any cancellation, termination or restriction of any such coverage.

(d) Third Party Beneficiaries. Except as expressly provided with respect to other Participants there shall be no third party beneficiaries of this Agreement.

2. Participant's Insurance

(a) Participant's Insurance. The Participant shall obtain and maintain insurance coverage for general and professional liability with coverage limits that are reasonable and customary for a party engaged in the activities of the Participant in California. If any policy of such insurance is issued on a "claims made" basis, then upon the termination of any such policy, the Participant shall procure extended reporting ("tail") coverage for such policy for the longest extended reporting period that is commercially available.

(b) Participant's Insurance for Governmental Entity

(i) Self Insurance. Government entities may satisfy this requirement through evidence or self insurance.

3. Indemnification.

(a) LANES shall indemnify, defend, and hold the Participant and its employees, agents, subcontractors and licensors harmless from and against all liability to third parties (including reasonable attorneys' fees), injury or damage that arises from an act or omission of LANES, including, without limitation, LANES's breach of any obligation, representation, or warranty of LANES set forth herein.

(b) The Participant shall indemnify, defend, and hold LANES and other Participants, and their respective employees, agents, subcontractors, and licensors harmless from and against any and all liability to third parties (including reasonable attorney's fees), injury, or damage that arises from an act or omission of the Participant, including, without

limitation, the Participant's breach of any obligation, representation, or warranty of the Participant set forth herein. A party's indemnification obligations under this section are conditioned upon the party seeking to be indemnified: (a) giving prompt notice of the claim to the indemnifying party; (b) granting sole control of the defense or settlement of the claim or action to the indemnifying party; and (c) providing reasonable cooperation to the indemnifying party and, at the indemnifying party's request and expense, assistance in the defense or settlement of the claim; provided however, the indemnifying party shall be relieved of its indemnification obligations only to the extent failure to comply with any of the foregoing prejudices its ability to provide indemnification required hereunder. An indemnifying party may not settle any claim against the other without that other party's consent, which consent shall not be unreasonably withheld.

4. Specific Indemnities. Without limiting the generality of Section VIII, acts or omissions giving rise to the obligation to indemnify and hold harmless pursuant to Section VIII shall include, but not be limited to, (a) acts or omissions that result in a Breach of Privacy or Security or (b) a Data Provider's provision of any Patient Data through the services or System that is inaccurate, incomplete or defamatory.

5. Rules for Indemnification. Any indemnification made pursuant to this Agreement 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. A party seeking to be indemnified pursuant to this Section VIII shall make a demand for indemnification upon the Indemnifying Party promptly and within a period of time within which the Indemnifying Party is not prejudiced by lack of notice. Upon receipt of such notice, the Indemnifying Party shall, at its sole cost and expense, retain legal counsel and defend the party to be indemnified. The Indemnifying Party shall be responsible for, and have control of, such claim and any litigation arising there from, but may not settle such litigation without the express consent of the party(ies) 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.

IX. **GENERAL TERMS**

1. Each Data Exchange Participation Agreement and Business Associate Agreement set forth the entire agreement between the parties and supersede any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of such Agreement. All exhibits referred to in a Data Exchange Participation Agreement are incorporated herein by reference. If a party wishes to assign or otherwise transfer a Data Exchange Participation Agreement to anyone, such party must obtain the other's prior written consent, which shall not be unreasonably withheld. Any attempted transfer or assignment in violation of the foregoing shall be void and of no effect.

   Each Data Exchange Participation Agreement shall be binding on the parties, their successors, and permitted assigns. For any breach or threatened breach of obligations identified hereunder as subjecting a non-breaching party to irreparable harm, the non-breaching party shall be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. Data Exchange Participation Agreements shall be construed under the laws of the State of California, without regard to its conflicts of law principles. The parties hereby disclaim the application of the 1980 U.N. Convention on Contracts for the International Sale of Goods. If any provision of a Data Exchange Participation Agreement is found invalid or unenforceable by an arbitrator or a court of competent jurisdiction, the remaining portions shall remain in full force and effect. A Data Exchange Participation Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original and all of which together shall constitute.

   (a) The relationship of the parties to each Data Exchange Participation Agreement is one of independent contractors and shall not be deemed to be that of employer and employee, master and servant, principal and agent or any other relationship except that of independent contractors contracting for the purposes of that Agreement.

2. Medicare/Medicaid Participation. LANES hereby represents and warrants that neither LANES nor its principals (if applicable) are presently debarred, suspended, proposed for debarment, declared ineligible, or excluded from participation in any federally funded health care program, including Medicare and Medicaid. LANES shall immediately notify Participant of any threatened, proposed, or actual debarment, suspension or exclusion from any federally funded health care program, including Medicare and Medicaid. In

the event that LANES is debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in any federally funded health care program during the term of this Agreement, or if at any time after the effective date of this Agreement it is determined that LANES is in breach of this Section 19, this Agreement shall, as of the effective date of such action or breach, automatically terminate. LANES further understands that Participant may periodically check contracted individuals and entities against the Office of Inspector General ("OIG") and General Service Administration ("GSA") databases of Excluded Individuals and Entities and will notify LANES if it discovers a match. Participant will take reasonable measures to verify that the match is the same individual or entity before taking any action to terminate any underlying agreement(s).

3. Applicable Law. The interpretation of the Data Exchange Participation Agreements and the resolution of any disputes arising under such 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 this Agreement, the venue of such action shall be exclusively in Los Angeles County, in the State of California.

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

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

6. Force Majeure. If the performance of any material obligation under this Agreement is prevented or interfered with by a Force Majeure (any act or condition whatsoever beyond the reasonable control of and not occasioned by the fault or negligence of the affected party, including but not limited to internet brown-outs, terrorism, natural disasters, acts of God, acts of government, wars, riots, strikes and other labor disputes, fires, and floods) the party so affected shall be excused from such performance to the extent of such prevention or interference.

7. Supervening Circumstances. Neither the Participant nor LANES shall be deemed in violation of any provision of this Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other

circumstances that are not within its reasonable control. This Section 15.4 (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.

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

9. Notices. All notices required under this Agreement shall be in writing. Notices shall be deemed to have been duly made and received (i) when personally served, (ii) when delivered by commercially established courier service, (iii) ten (10) days after deposit in mail via certified mail, return receipt requested, or (iv) on delivery, when delivered by Federal Express, charges prepaid or charged to the sender's account, if delivery is confirmed by Federal Express. Notices must be delivered to the addresses specified in the applicable Data Exchange Participation Agreement, or to such other address as a party shall designate in writing from time to time. Any correctly addressed Notice that is refused.

10. Waiver. No provision of the terms and conditions of this 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.

X. Term and Termination

1. Term. The term of this Agreement (the "Term") shall commence on the date on which LANES and the Participant sign the Agreement (the "Effective Date"), and shall continue through and until the termination of this Agreement pursuant to this Section X (Term and Termination.

2. Termination Upon Cessation of Business. LANES may terminate this Agreement by providing a five (5) business day written notice to the Participant that LANES will cease to provide the services.

3. Termination with 45 calendar days Written Notice. Either LANES or the Participant may terminate this Agreement at any time, by giving not less than forty five (45) calendar days prior written notice to the other.

4. Termination Upon Material Breach. Either LANES or the Participant (the "Terminating Party") may terminate this Agreement upon the failure of the other party (the "Breaching Party") to perform a material responsibility arising out of this Agreement, and that failure continues uncured for a period of sixty (60) days after the Terminating Party has given the Breaching Party notice of that failure and requested that the Breaching Party cure that failure.

5. Termination upon Privacy or Security Breach. Without limiting the generality of the foregoing Section 4, either party may terminate this Agreement upon a failure by the other party to correct a Breach of Privacy or Security within sixty (60) days following notice thereof from the other.

6. Participant's Termination of Participation Agreement Upon Breach of Business Associate Agreement. Notwithstanding any other provision of this Section VIII to the contrary, the Participant may terminate its Data Exchange Participation Agreement based upon LANES's breach of its Business Associate Agreement with the Participant.

7. Effect of Termination. Upon any termination of this Agreement, the Participant shall cease to be a Participant in LANES's health information exchange and thereupon and thereafter neither the Participant nor its Authorized Users shall have any rights to use the System or the services. Certain provisions of this Agreement shall continue to apply to the former Participant and its Authorized Users following that termination, as described in Section 3.6 (Survival of Provisions).

8. Survival of Provisions. The following provisions of this Agreement shall survive any termination hereof: Section IV.11 (Responsibility for Acts of Authorized Users and others), Section IV.24 (Protected Health Information), Section VI (Proprietary Information), Section VII.9 (Limitation on Liability) and Section VII.3 (Indemnification).

XI. Amendments to Agreement and Policies and Procedures.

1. Amendments Required by Law. LANES may amend, repeal and replace these Terms and Conditions and/or the Policies and Procedures at any time, as required in order for LANES and/or Participants to comply with applicable laws and regulations. LANES shall endeavor to give Participants notice of such changes not less than thirty (30) days prior to the implementation of those changes. However, LANES may implement the change within a shorter period of time as LANES 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 LANES and the Participant, as of the effective date of the change.

2. Other Amendments. LANES may amend, or repeal and replace, or expand the scope of this Agreement to include, payment, operations, public health and research-related purposes at any time that LANES determines it is desirable to do so; provided, that LANES shall notify the Participant of any material changes to this Agreement or the Policies and Procedures at least forty five (45) days prior to the implementation of the Amendment.

3. Termination Based on Objection to Amendment. If an Amendment to this Agreement other than those made pursuant to "Amendments Required by Law" Section affects a material right or obligation of the Participant, and the Participant objects to that Amendment, the Participant may terminate this Agreement by giving LANES written notice within fifteen (15) days following LANES's notice of the Amendment. Such termination of this Agreement shall be effective as of the effective date of the Amendment to which the Participant objects; provided, however, that following receipt of the Participant's notice of its objection to the Amendment, LANES may decide in its discretion to refrain from implementing the Amendment to which the Participant has objected, in which event this Agreement shall not be terminated and shall continue in force and effect.

XII. **Complete Understanding**. This Agreement contains 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 this Agreement other than those contained or referenced in this Agreement. All modifications or amendments to this Agreement shall be in writing and signed by all parties.

XIII. **Effective Date.** This Agreement shall become effective upon the date of its execution by both parties (the "Effective Date").

XIV. **Term.** The term of this Agreement shall continue until it is terminated as provided in Termination of Data Exchange Participation Agreements Section of this Agreement.

SIGNATURE PAGE

IN WITNESS WHEREOF AND IN CONSIDERATION of the recitals, covenants, conditions and promises herein contained, and for other valuable consideration, the receipt and sufficiency of which the parties hereby acknowledge, LANES and the Participant have executed this Agreement as of the Effective date set forth below:

PARTICIPANT'S NAME	LANES REPRESENTATIVE
Signed: _____	Signed: _____
Name: _____	Name: _____
Title: _____	Title: _____
Effective Date: _____	Date: _____

Address for purposes of notice: [Insert name of Participant]

_____

_____

Exhibit A

Participation

The Participant shall participate in the following Program (s):

1. **Linking Program**. The Participant shall participate as a [Data Provider or Data Recipient] in LANES's ED Linking Program, a program of electronic health information exchange centered upon care in the emergency medicine departments described below. This Program is organized on a federated model, pursuant to which each Data Provider maintains its own repository of Patient Information, and makes specific Patient Information available to Data Recipients for Access through the Network upon request, by causing the transfer of that information as follows: (a) from a server dedicated to that function or from another resource within the Data Provider's systems, as selected by the Data Provider subject to approval by LANES for compliance with the Program's requirements to (b) the computer or other resource of the Data Recipient. The following emergency departments are to participate as Data Providers and/or as Data Recipients in the ED Linking Program initially:

Los Angeles County Harbor–UCLA Medical Center
Long Beach Memorial Medical Center
Miller Children's Hospital at Long Beach Memorial Medical Center
LAC+USC Medical Center
Providence Little of Company of Mary Medical Center San Pedro
Providence Little Company of Mary Medical Center Torrance

Additional emergency departments may from time to time begin to participate in the ED Linking Program, in accordance with their respective Data Exchange Participation Agreements. Emergency departments may from time to time cease to so participate, upon a termination or amendment of their Data Exchange Participation Agreements. LANES shall promptly notify the Participant of the addition or deletion of emergency departments from the ED Linking Program.

2. Urgent Care Program. The Participant shall participate as a [Data Provider or Data Recipient or Data Provider and Data Recipient] in LANES's Urgent Care Program, a program of electronic health information exchange centered upon providing critical data for patient care in regional Urgent Care centers. This Program is organized on a federated model, pursuant to which each Data Provider maintains its own repository of Patient Information, and makes specific Patient Information available for Access at participating urgent care centers through the Network upon request by causing the transfer of that information as follows: (a) from a server dedicated to that function or from another resource within the Data Provider's systems, as selected by the Data Provider subject to approval by LANES for compliance with the Program's requirements, (b) to the computer or other resource of the participating urgent care center Data Recipient. The following are participants in the Urgent Care Program initially:

Memorial HealthCare IPA (Data Provider and Data Recipient) Long Beach Memorial Medical Center (Data Provider)
Miller Children's Hospital at Long Beach Memorial Medical Center (Data Provider)
Providence Little of Company of Mary Medical Center San Pedro (Data Provider)
Providence Little Company of Mary Medical Center Torrance (Data Provider)

Additional Data Providers and/or Data Recipients may decide to participate in this agreement in accordance with their respective Data Exchange Participation Agreements which will include the Data Elements for their patients. Data Providers and Data Recipients may also decide to cease their participation, upon a termination or amendment of their Data Exchange Participation Agreements. LANES shall promptly notify the Participant of the addition or deletion of Data Providers and/or Data Recipients from the Urgent Care Program.

Exhibit B

Technical and Functional Specifications

Technical Specifications

- LANES supports a hybrid centralized/federated architecture. In the centralized model using "Root Server "all HIO-based clinical data will be located on the centralized LANES environment. In the federated model, "Edge Server" may be placed in their hosting location and connected (via secure VPN tunnel) to the central (Root) environment.

  In either case, centralized or federated, the LANES development team will do all of the interface connectivity and configuration work on the HIO platform. The participant or their clinical systems vendor will only be responsible for the participant-side connectivity work. Any associated hardware and software shall be obtain through a separate agreement.

- Edge Servers can be installed with options for physical servers or as virtual servers based on participants needs.

  - For VM-based virtual implementations, the participant will need to pre-establish a VM-based environment (typically Linux) running on Intel/AMD-based servers. The installation of the base configuration assumes 20GB, 50GB or 100GB disk space sizes and minimum memory of 512MB with larger memory allocation as required depending upon load and performance needs. Connectivity requires two (2) VPN tunnels: One for LANES technical support and one for Connectivity between the Edge Server and the LANES Root server;

  - For physical servers, the server is built by LANES technical vendor and delivered to the participant. The network connectivity is identical as the Virtual servers.

- Connectivity by participant systems to the "Edge server" (as in federated model) are across local networks typically behind firewalls, so security is supported locally as desired by the participant. LANES assumes this to be a local network connection between the participant sending systems and the Edge server.

- For participants who connect directly to the Root Server (i.e., without their own Edge Server), connectivity between participants and the "Root Server" is assumed to be a secure Web Services connection or secure VPN tunnel. Other options may be considered if it supports appropriate supportability and security.

    - For VPN Tunnels , the connectivity requires encrypted connections with appropriate authentication.
    - For Web Services, the connectivity requires encrypted connections with bi-directional credentialing.

- For Data users the LANES HIO Portal is using one of the following browsers: IE8+, Mozilla Firefox 3.5+, Safari 3+ and Google Chrome. There are currently no OS constraints if one of these browsers is being used.

Functional Specifications:

- LANES HIO has a clinical data repository that supports data exchange for HIOs, hospitals, and other clinical settings. It allows the aggregation of data from various sources to create a comprehensive longitudinal record of a patient.

- LANES HIO will provide doctors, nurses, and medical staff the ability to view patient information in near real-time at the point of care. The system will also capture the information on current visits for integration into the future consolidated patient records thereby creating a richer, more complete clinical view via. Continuity of Care Document (CCD).

- Messaging is currently for a standard version of HL7 2.x or 3.x/IHE messaging outbound from the participant (inbound to the LANES HIO). LANES HIO does not currently support outbound Clinical Summaries (CCDs) into participant EHRs. The minimum information types are ADT (admission, discharge, transfer) and Lab Results (ORU), but others will be considered if the participant can supply them, such as clinical notes (HL7 MDM). Also, if a participant can supply inbound Clinical Summaries (CCDs), they are supported. If the participant does not have any current outbound messaging then LANES has a default standard spec (HL7 2.4-based) or CDA based on the IHE specification.

- For Additional functional specifications refer to the Training Manual provided to the Data User.

Exhibit C

LANES Security & Privacy Policies

1. General Security Safeguards and Controls

Policy: LANES HIO data shall be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure:

a) LANES shall maintain a secure environment for all its systems that handle Individual data and any centralized data repositories containing Individual or Participant data, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data.

b) Participants shall maintain a secure environment for LANES HIO-related infrastructure, services, and data to support the secure and reliable operation and continued development of the HIO, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data accessed through the HIO services.

c) LANES and its Participants shall employ security controls that meet applicable federal and State standards so that the information and data being transmitted shall not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, or malware. In the absence of applicable industry standards, LANES and its Participants shall use all commercially reasonable efforts to comply with the requirements of this policy.

d) Participants shall collaborate with LANES to develop security and privacy policies, standards and procedures, and to amend, repeal, or replace provisions as necessary to support the secure operation and continued development of the HIO.

1.1 User Identification and Authentication

Policy: To prevent unauthorized access of information and maintain data integrity and quality, the LANES HIO authentication provision requires that both the identity and the authority of an entity requesting health information be verified and authenticated:

a) LANES shall implement unique user names for accessing the HIO. Usernames must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee. Passwords

are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the system. Passwords must be changed at least every (90) days, preferably every (60) days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

(i) Upper case letters (A-Z)

(ii) Lower case letters (a-z)

(iii) Arabic numerals (0-9)

(iv) Non-alphanumeric characters (punctuation symbols)

b) Participants shall locally authenticate all system Users before the User is given access to the HIO.

c) Participants shall assign each System User with access to HIO services to a specific Role as defined by the HIO.

d) Participants shall communicate and authenticate credentials. In any data exchange, the Participant shall communicate its credentials, and the HIO shall use such credentials to authenticate the Participant is an HIO Participant in good standing.

e) Participants shall include in each request for Individual data a non-reputable assertion as to the identity and role of the system User who will receive the data.

f) Participants shall maintain policies and procedures that govern Users ability to access information on or through the Participant's system and through the HIO services.

g) Participants shall have and apply appropriate sanctions against members of its workforce who fail to comply with the policies and procedures of the Participant or LANES. Participants shall document the sanctions that are applied, if any.

h) The HIO System shall uniquely identify and authenticate users (or processes action on behalf of users).

i) The HIO System shall identify and authenticate specific devices before establishing a connection.

j) The HIO System shall obscure feedback of the authentication information during the authentication process to protect the

information from possible exploitation/use by unauthorized individuals.

k) The HIO System shall verify that the user accessing the received Individual Information has a Role that is permitted to access the type of data being requested from the Sending Participant

1.2 Access Control and Authorization

Policy: Appropriate signed access agreements for individuals requiring access to HIO data and HIO information systems:

a) All persons that will be working with HIO data must sign a confidentiality statement that includes, at a minimum, General Use, Security Safeguards, Acceptable Use, and Enforcement Policies. The confidentiality statement must be signed by the workforce member prior to accessing the HIO. The confidentiality statement must be renewed annually.

b) LANES shall establish “Roles” for all Users, which define categories of Users of HIO services. These categories are based on the types of Individual data that these users need to access to perform their job functions, and the permitted purposes for such access.

c) The permitted purposes are based on each User’s job function and relationship with the Individual. HIO System Roles shall be used as community standard classifications to enable sending and receiving Participants to establish access control rules that are meaningful to each other. The HIO will initially favor simple, broad Role definitions to facilitate adoption by Participants and will refine these definitions over time.

d) Access Privileges shall be governed by the Role of the User in the Participant organization to which the clinical message is addressed. For example: A User may be the Primary Care Physician of a Individual in one clinic, authorized to view the full longitudinal health record in a message addressed to that clinic. The same User may play a specialist Role in another Participant organization where messages are filtered to display only data needed for permitted purpose.

e) LANES and its Participates shall have a documented access control policies that address purpose, scope, roles, responsibilities, management commitment, to facilitate the secure access to confidential data.

1.3 User Account Management

Policy: Establishing, activating, modifying, reviewing, disabling, and removing HIO accounts:

a) The HIO System shall automatically disable inactive accounts after 90 days.

b) The HIO System shall automatically terminate temporary and emergency accounts based upon a defined time period for each type of account.

c) The HIO System shall employ automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

d) LANES shall develop a notification process for timely termination of HIO user accounts/access.

1.4 Access Enforcement

Policy: Apply appropriate authorization control for LANES HIO access:

a) LANES and Participant HIO systems shall display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

b) LANES and Participant HIO systems shall prevent access after (5) failed logon attempts.

c) LANES and Participant HIO systems shall provide an automatic timeout, requiring re-authentication of the user session after no more than (20) minutes of inactivity.

d) LANES and Participant systems shall use role based access controls for all user authentications, enforcing the principle of least privilege.

e) All HIO data transmissions outside of LANES and Participant secure internal networks must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing can be encrypted. This requirement pertains to any type

HIO data in motion such as website access, file transfer, and E-Mail.

f) All HIO systems shall be protected by a comprehensive intrusion detection and prevention solution.

1.5 Audit and Accountability

Policy: LANES and its Participants shall implement technical processes that accurately record activity related to access, creation, modification and deletion of HIO data. LANES shall publish Implementation Guides that shall specify requirements for logging of messages pertaining to Individual data transmitted via the HIO. Implementation Guides shall contain general requirements for logging all messages to include, but not limited to:

1. Log-In Monitoring

(a) As part of log-in monitoring, LANES shall audit when a person logs onto the System or software application of the HIO. This shall include all attempted and failed logons.

(b) Log-In logs shall be reviewed by LANES periodically based upon audit criteria developed in advance. Anomalies must be documented and appropriate mitigating actions must be taken and documented.

2. Systems Logging Requirements:

a) LANES and Participant HIO systems shall be configured to create audit logs that track activities involving electronic data.

b) The scope of the systems logging shall include software application, network servers, firewalls, and other network hardware and software.

c) System logs shall be reviewed on a regular basis by LANES and Participants based upon audit criteria developed in advance. All anomalies must be documented and appropriate mitigating actions must be taken and documented.

d) System logs shall include, but not be limited to, the following types of information: data modification, creation, and deletion.

e) LANES and Participant system logs shall contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events, and provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

f) The HIO System shall provide date and time stamps for use in audit record generation. LANES shall establish a uniformed time synchronization standard for the HIO.

3. System Logs shall contain, at a minimum:

a) The identity of the Individual whose information was accessed.

b) A subset of the demographic information used to find a person should be logged to identify the subject of care.

c) The identity of the user accessing the Individual data.

d) The identity of the Participant with which the User is affiliated, and through whose system HIO services were accessed.

e) The type of Individual data or record accessed (e.g., pharmacy data, laboratory data, etc.).

f) The date and time of access.

g) The source of the Individual data (i.e., the Participant from whose system the accessed Individual data was derived).

4. Log Retention:

a) LANES and Participant system log data shall be achieved for at least (3) years after occurrence.

b) LANES and its Participants shall consider all logs to be PHI and secure them accordingly.

c) Log records shall support reporting to Individuals and other stakeholders of all disclosures of Individual data via the HIO. Future enhancements may include alerts, alarms, and analysis

5. System-wide Audit Practice:

a) System-wide audits shall be conducted at least annually as a minimum requirement.

b) System-wide audits shall provide the capability to compile audit records from multiple components throughout the HIO System into a system-wide time-correlated audit trail; and provide the capability to manage the selection of events to be audited by individual components of the system.

c) System-wide audit documentation shall be retained for a minimum of (6) years.

6. Protection of Audit Information:

a) LANES and its Participants shall protect audit information and audit tools from unauthorized access, modification, and deletion.

7. Audit Storage Capacity:

a) LANES and its Participants shall allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

8. Security Information and Event Management (SIEM):

a) LANES and its Participants shall employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities, and alert LANES security personnel of inappropriate or unusual activities with security implications:[need to define list of inappropriate or unusual activities that are to result in alerts].

b) The output from the security events monitoring shall facilitate the generation of a compliance audit findings report. Identified deficiencies shall be addressed by order of priority.

9. Data Integrity

Policy: LANES and its Participants shall take reasonable steps to ensure that HIO information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner:

a) LANES and its Participants shall protect individual health information from unauthorized alteration or destruction.

b) LANES and its Participants shall implement technical security measures to protect against unauthorized access to individual health information that is being transmitted over an electronic communications network.

c) LANES and its Participants shall implement a mechanism to provide the ability to encrypt and decrypt where appropriate, to protect individual health information.

d) LANES and its Participants shall avoid the use of proprietary encryption algorithms, unless reviewed by qualified experts outside of the vendor in question and approved by Federal guidelines. Asymmetric crypto-system keys shall be of a length that yields equivalent strength. Key length requirements shall be reviewed annually by LANES and upgraded as technology allows.

e) LANES and its Participants shall implement security measures to safeguard electronically transmitted individual health information from being improperly modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner.

f) LANES and its Participants shall develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.

10. Server, Laptop and Portable Device Control

Policy: LANES and its Participants shall take reasonable steps to ensure that individually identifiable health information is adequately safeguarded on computing devices:

a) All laptops that store HIO data either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the LANES Information Security Office.

b) Only the minimum necessary amount of HIO data required to perform necessary business functions may be copied, downloaded, or exported.

c) All electronic files that contain HIO data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

d) All servers, workstations, laptops and other systems that process and/or store HIO data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

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

f) All systems involved in accessing, storing, transporting, and protecting HIO data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

g) When no longer needed, all HIO data must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the LANES Information Security Office.

11. Physical Security

Policy: LANES and its Participants shall ensure that HIO data is used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours:

a) LANES and its Participants shall secure facilities where workers assist in the administration of HIO systems. LANES and its Participants shall ensure that these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or access

authorization; and access to premises is by official identification.

b) LANES and its Participants shall ensure that there are security guards or a monitored alarm system with or without security cameras 24 hours a day, 7 days a week where HIO data is stored or used.

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

d) HIO data in paper form must be disposed of through confidential means, such as cross cut shredding and pulverizing.

e) Visitors to areas where HIO data are contained shall be escorted and HIO data shall be kept out of sight while visitors are in the area.

12. Personnel Controls

Policy: Ensure Initial and ongoing Information Security and Privacy Awareness Training and compliance for workforce members involved in the performance and/or administration of confidential information:

a) **Employee Training**. LANES and Participant workforce members who assist in the performance of functions or activities on behalf of LANES, or access or disclose LANES HIO data must complete information privacy and security training, at least every two years, at their organization's expense. Each workforce member who receives information security and privacy training must sign a certification, indicating the member's name and the date on which the training was completed.

b) **Employee Discipline**. Appropriate sanctions must be applied against workforce members who fail to comply with security and privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

c) **Confidentiality Statement**. All persons that will be working with LANES HIO data must sign a confidentiality statement that includes, at a minimum, General Use, Security Safeguards, Acceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to LANES HIO data. The statement must be renewed annually.

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

13. Business Continuity / Disaster Recovery Controls

Policy: Ensure availability, continuation, and recovery of critical business processes for the protection of confidential information:

a) LANES and its Participants shall establish documented plans to enable continuation of critical business processes for the protection of HIO data held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Policy for more than 24 hours.

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

14. Breaches and Privacy and Security Incidents

Policy: LANES shall adhere to breach protocol terms and conditions in accordance with Exhibit D (Business Associate Agreement) of the LANES Electronic Health Information Data Exchange Participation Agreement.

Participants shall implement reasonable measures for the discovery and prompt reporting of any breach or privacy and/or security incident involving LANES HIO and the Participant's system(s), and to take the following steps:

a) Initial Notice to LANES (1) To notify LANES immediately by telephone call plus email or fax upon the discovery of a breach of unsecured HIO data in electronic media or in any other media if the HIO data was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security and/or privacy incident that involves HIO data. (2) To notify LANES within 24 hours by email or fax of the discovery of any suspected security and/or privacy incident, intrusion or unauthorized access, use or disclosure of HIO data in violation of LANES policies, or potential loss of confidential data affecting these policies. A breach shall be treated as discovered the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of the Participant.

b) Notice shall be provided to the LANES Program Contract Manager and the LANES Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic HIO data, notice shall be provided by calling the LANES Information Security Officer. Notice shall be made using the LANES' "Privacy Incident Report" form, including all information known at the time. Participant shall use the most current version of this form, which is posted on the LANES website (www.)

c) Upon discovery of a breach or suspected privacy and/or security incident, intrusion or unauthorized access, use or disclosure of LANES HIO data, Participant shall take:

    a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
    b. Any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

d) Investigation and Investigation Report. To immediately investigate such suspected security and/or privacy incident, security and/or privacy incident, breach, or unauthorized access, use or disclosure of HIO data. Within 72 hours of

the discovery, Participant shall submit an updated "Privacy Incident Report" containing the information and all other applicable information listed on the form, to the extent known at that time, to the LANES Program Contract Manager and the LANES Information Security Officer;

e) **Complete Report**. To provide a complete report of the investigation to the LANES Program Contract Manager and the LANES Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or State law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If LANES requests information in addition to that listed on the "Privacy Incident Report" form, Participant shall make reasonable efforts to provide LANES with such information. If, because of the circumstances of the incident, Participant needs more than ten (10) working days from the discovery to submit a complete report, LANES may grant a reasonable extension of time, in which case Participant shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. LANES will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

f) **Notification of Individuals**. If the cause of a breach is attributable to the Participant or its subcontractors, agents or vendors, Participant shall notify individuals of the breach or unauthorized use or disclosure when notification is required under State or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The LANES Program Contract Manager and the LANES Information Security

Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. LANES will provide its review and approval expeditiously and without unreasonable delay.

g) **Responsibility for Reporting of Breaches**. If the cause of a breach is attributable to Participant or its agents, subcontractors or vendors, Participant is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Participant shall notify the Secretary of the breach immediately upon discovery of the breach. If Participant has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to LANES in addition to Participant, Participant shall notify LANES, and LANES and Participant may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection above.

h) LANES Contact Information. To direct communications to LANES staff, the Participant shall initiate contact as indicated herein. LANES reserves the right to make changes to the contact information below by giving written notice to the Participant. Said changes shall not require an amendment to this policy.

Participants shall use the following LANES contact information:

LANES Contract Manager	LANES Privacy Officer	LANES Information Security Officer

i) Sanctions and/or Penalties. Participant understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to the Participant may result in the imposition of sanctions and/or penalties on Participant under HIPAA, the HITECH Act and the HIPAA.

Exhibit D

Participation Fees

The fee to participate in the LANES programs shall be negotiated at a later time, and the result of those negotiations will replace this exhibit. It is the intention of LANES to work with the greater Los Angeles healthcare delivery community to develop reasonable fees for the maximum number of participants to this agreement.

Exhibit E

BUSINESS ASSOCIATE AGREEMENT

Under this Agreement, LANES (“Business Associate”) provides services (“Services”) to Participant (“Covered Entity”) and Business Associate receives, has access to or creates Protected Health Information in order to provide those Services.

Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), and regulations promulgated thereunder, including the Standards for Privacy of Individually Identifiable Health Information (“Privacy Regulations”) and the Health Insurance Reform: Security Standards (“the Security Regulations”) at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164 (together, the “Privacy and Security Regulations”). The Privacy and Security Regulations require Covered Entity to enter into a contract with Business Associate ("Business Associate Agreement") in order to mandate certain protections for the privacy and security of Protected Health Information, and those Regulations prohibit the disclosure to or use of Protected Health Information by Business Associate if such a contract is not in place.

Further, pursuant to the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH Act"), effective February 17, 2010, certain provisions of the HIPAA Privacy and Security Regulations apply to Business Associates in the same manner as they apply to Covered Entity and such provisions must be incorporated into the Business Associate Agreement.

This Business Associate Agreement and the following provisions are intended to protect the privacy and provide for the security of Protected Health Information disclosed to or used by Business Associate in compliance with HIPAA's Privacy and Security Regulations and the HITECH Act, as they now exist or may hereafter be amended.

Therefore, the parties agree as follows:

DEFINITIONS

1.1. "Breach" has the same meaning as the term “breach" in 45 C.F.R. § 164.402.

1.2. “Disclose” and “Disclosure” mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate’s internal operations or to other than its employees.

1.3. “Electronic Health Record” has the same meaning as the term “electronic health record" in the HITECH Act, 42 U.S.C. section 17921. Electronic Health Record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians

and staff.

1.4. "Electronic Media" has the same meaning as the term "electronic media" in 45 C.F.R. § 160.103. Electronic Media means (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

The term "Electronic Media" draws no distinction between internal and external data, at rest (that is, in storage) as well as during transmission.

1.5. "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103. Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.6. "Individual" means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.7. "Minimum Necessary" refers to the minimum necessary standard in 45 C.F.R. § 162.502 (b) as in effect or as amended.

1.8. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164, also referred to as the Privacy Regulations.

1.9. "Protected Health Information" has the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Protected Health Information includes information that (i) relates to the past, present or future physical or mental health or condition of an Individual; the provision of health care to an Individual, or the past, present or future payment for the provision of health care to an Individual; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is received by Business Associate from or on behalf of Covered Entity, or is created by Business Associate, or is made accessible to Business Associate by Covered Entity. "Protected Health

Information" includes Electronic Health Information.

1.10. "Required By Law" means a mandate contained in law that compels an entity to make a Use or Disclosure of Protected Health Information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or any administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing benefits.

1.11. "Security Incident" means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information in, or interference with system operations of, an Information System which contains Electronic Protected Health Information. However, Security Incident does not include attempts to access an Information System when those attempts are not reasonably considered by Business Associate to constitute an actual threat to the Information System.

1.12. "Security Rule" means the Security Standards for the Protection of Electronic Health Information also referred to as the Security Regulations at 45 Code of Federal Regulations (C.F.R.) Part 160 and 164.

1.13. "Services" has the same meaning as in the body of this Agreement.

1.14. "Unsecured Protected Health Information" has the same meaning as the term "unsecured protected health information" in 45 C.F.R. § 164.402.

1.15. "Use" or "Uses" mean, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate's internal operations.

1.16. Terms used, but not otherwise defined in this Business Associate Agreement shall have the same meaning as those terms in the HIPAA Regulations and HITECH Act.

OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 Permitted Uses and Disclosures of Protected Health Information. Business Associate:

(a) shall Use and Disclose Protected Health Information only as necessary to perform the Services, and as provided in Sections 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 4.3 and 5.2 of this Agreement;

(b) shall Disclose Protected Health Information to Covered Entity upon request;

(c) may, as necessary for the proper management and administration of its business or to carry out its legal responsibilities:

(i) Use Protected Health Information; and

(ii) Disclose Protected Health Information if the Disclosure is Required by Law.

Business Associate shall not Use or Disclose Protected Health Information for any other purpose or in any manner that would constitute a violation of the Privacy Regulations or the HITECH Act if so Used or Disclosed by Covered Entity.

2.2 Prohibited Uses and Disclosures of Protected Health Information. Business Associate:

(a) shall not Use or Disclose Protected Health Information for fundraising or marketing purposes.

(b) shall not disclose Protected Health Information to a health plan for payment or health care operations purposes if the Individual has requested this special restriction and has paid out of pocket in full for the health care item or service to which the Protected Health Information solely relates.

(c) shall not directly or indirectly receive payment in exchange for Protected Health Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act. This prohibition shall not effect payment by Covered Entity to Business Associate. Covered Entity shall not provide such written consent except upon express approval of the departmental privacy officer and only to the extent permitted by law, including HIPAA and the HITECH Act.

2.3 Adequate Safeguards for Protected Health Information. Business Associate:

(a) shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information in any manner other than as permitted by this Business Associate Agreement. Business Associate agrees to limit the Use and Disclosure of Protected Health Information to the Minimum Necessary in accordance with the Privacy Regulation's minimum necessary standard as in effect or as amended.

(b) as to Electronic Protected Health Information, shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information; effective February 17, 2010, said safeguards shall be in accordance with 45 C.F.R. Sections 164.308, 164.310, and 164.312, and shall comply with the Security Rule's policies and procedure and documentation requirements.

2.4 Reporting Non-Permitted Use or Disclosure and Security Incidents and Breaches of Unsecured Protected Health Information. Business Associate:

(a) shall report to Covered Entity each Use or Disclosure of Protected Health Information that is made by Business Associate, its employees, representatives, Agents, subcontractors, or other parties under Business Associate's control with access to Protected Health Information but which is not specifically permitted by this Business Associate Agreement or otherwise required by law.

(b) shall report to Covered Entity each Security Incident of which Business Associate becomes aware.

(c) shall notify Covered Entity of each Breach by Business Associate, its employees, representatives, agents or subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Business Associate as determined in accordance with the federal common law of agency.

2.4.1 Immediate Telephonic Report. Except as provided in Section 2.4.3, notification shall be made immediately upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information by telephone call to (562) 940-3335.

2.4.2 Written Report. Except as provided in Section 2.4.3, the initial telephonic notification shall be followed by written notification made without unreasonable delay and in no event later than three (3) business days from the date of discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident, or Breach by the Business Associate to the Chief Privacy Officer at:

Participant's Chief Privacy Officer
Kenneth Hahn Hall of Administration
500 West Temple Street, Suite 525
Los Angeles, California 90012
HIPAA@auditor.lacounty.gov
(213) 974-2166

(a) The notification required by section 2.4 shall include, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, Used, or Disclosed; and

(b) the notification required by section 2.4 shall include, to the extent possible, all information required to provide notification to the Individual under 45 C.F.R. 164.404(c), including:

(i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(ii) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(iii) Any other details necessary to conduct an assessment of whether there is a risk of harm to the Individual;

(iv) Any steps Business Associate believes that the Individual could take to protect him or herself from potential harm resulting from the breach;

(v) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to the Individual, and to protect against any further Breaches; and

(vi) The name and contact information for the person most knowledge regarding the facts and circumstances of the Breach.

If Business Associate is not able to provide the information specified in section 2.3.2 (a) or (b) at the time of the notification required by section 2.4.2, Business Associate shall provide such information promptly thereafter as such information becomes available.

2.4.3 Request for Delay by Law Enforcement. Business Associate may delay the notification required by section 2.4 if a law enforcement official states to Business Associate that notification would impede a criminal investigation or

cause damage to national security. If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay notification, notice, or posting for the time period specified by the official; if the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

2.5 Mitigation of Harmful Effect. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement.

2.6 Breach Notification. Business Associate shall, to the extent Covered Entity determines that there has been a Breach of Unsecured Protected Health Information, provide Breach notification for each and every Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or subcontractors, in a manner that permits Covered Entity to comply with its obligations under Subpart D, Notification in the Case of Breach of Unsecured PHI, of the Privacy and Security Regulations, including:

(a) Notifying each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed as a result of such Breach;

(b) The notification required by paragraph (a) of this Section 2.6 shall include, to the extent possible:

(i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(ii) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(iii) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;
(iv) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and

(iv) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(v) The notification required by paragraph (a) of this section shall be written in plain language

Covered Entity, in its sole discretion, may elect to provide the notification required by this Section 2.6, and Business Associate shall reimburse Covered Entity any and all costs incurred by Covered Entity, including costs of notification, internet posting, or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information.

2.7 Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books and records relating to the Use and Disclosure of Protected Health Information available to the Secretary of the federal Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations. Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

2.8 Access to Protected Health Information. Business Associate shall, to the extent Covered Entity determines that any Protected Health Information constitutes a "designated record set" as defined by 45 C.F.R. § 164.501, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and copy that Protected Health Information. Business Associate shall provide such access for inspection of that Protected Health Information within two (2) business days after receipt of request from Covered Entity. Business Associate shall provide copies of that Protected Health Information within five (5) business days after receipt of request from Covered Entity. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act.

2.9 Amendment of Protected Health Information. Business Associate shall, to the extent Covered Entity determines that any Protected Health Information constitutes a "designated record set" as defined by 45 C.F.R. § 164.501, make any amendments to Protected Health Information that are requested by Covered Entity. Business Associate shall make such amendment within ten (10) business days after receipt of request from Covered Entity in order for Covered Entity to meet the requirements under 45 C.F.R. § 164.526.

2.10 Accounting of Disclosures. Upon Covered Entity's request, Business Associate shall provide to Covered Entity an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or subcontractors, in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and/or the HITECH Act which

requires an Accounting of Disclosures of Protected Health Information maintained in an Electronic Health Record for treatment, payment, and health care operations.

[Optional, to be used when all Uses and Disclosures permitted in order to perform the Services will be for the Covered Entity's payment or health care operations activities: However, Business Associate is not required to provide an Accounting of Disclosures that are necessary to perform the Services because such Disclosures are for either payment or health care operations purposes, or both.]

Any accounting provided by Business Associate under this Section 2.10 shall include: (a) the date of the Disclosure; (b) the name, and address if known, of the entity or person who received the Protected Health Information; (c) a brief description of the Protected Health Information disclosed; and (d) a brief statement of the purpose of the Disclosure. For each Disclosure that could require an accounting under this Section 2.10, Business Associate shall document the information specified in (a) through (d), above, and shall securely maintain the information for six (6) years from the date of the Disclosure. Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of request from Covered Entity, information collected in accordance with this Section 2.10 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act.

2.11 Indemnification. Business Associate shall indemnify, defend, and hold harmless Covered Entity, including its elected and appointed officers, employees, and agents, from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, penalties and fines (including regulatory penalties and/or fines),and expenses (including attorney and expert witness fees), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement; Business Associate's obligations under this provision extend to compliance and/or enforcement actions and/or activities, whether formal or informal, of Secretary of the federal Department of Health and Human Services and/or Office for Civil Rights.

OBLIGATION OF COVERED ENTITY

3.1 Obligation of Covered Entity. Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the use of Protected Health Information that would affect Business Associate's performance of the Services, and Business Associate shall thereafter restrict or limit its own uses and disclosures accordingly.

TERM AND TERMINATION

4.1 Term. The term of this Business Associate Agreement shall be the same as the term of this Agreement. Business Associate's obligations under Sections 2.1 (as modified by Section 4.2), 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 4.3 and 5.2 shall survive the termination or expiration of this Agreement.

4.2 Termination for Cause. In addition to and notwithstanding the termination provisions set forth in this Agreement, upon either party's knowledge of a material breach by the other party, the party with knowledge of the other party's breach shall:

(a) Provide an opportunity for the breaching party to cure the breach or end the violation and terminate this Agreement if the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party;

(b) Immediately terminate this Agreement if a party has breached a material term of this Agreement and cure is not possible; or

(c) If neither termination nor cure is feasible, report the violation to the Secretary of the federal Department of Health and Human Services.

4.3 Disposition of Protected Health Information Upon Termination or Expiration.

(a) Except as provided in paragraph (b) of this section, upon termination for any reason or expiration of this Agreement, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(b) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make infeasible. If return or destruction is infeasible, Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

MISCELLANEOUS

5.1 No Third Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

5.2 Use of Subcontractors and Agents. Business Associate shall require each of its agents and subcontractors that receive Protected Health Information from Business Associate, or create Protected Health Information for Business Associate, on behalf of Covered Entity, to execute a written agreement obligating the agent or subcontractor to comply with all the terms of this Business Associate Agreement.

5.3 Relationship to Services Agreement Provisions. In the event that a provision of this Business Associate Agreement is contrary to another provision of this Agreement, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of this Agreement.

5.4 Regulatory References. A reference in this Business Associate Agreement to a section in the Privacy or Security Regulations means the section as in effect or as amended.

5.5 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Regulations.

5.6. Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Regulations and other privacy laws governing Protected Health Information.

IN WITNESS WHEREOF, the parties hereto have executed this HIPAA Business

Associate Agreement effective as of the date stated below.

PARTICIPANT'S NAME	LANES REPRESENTATIVE
Signed: _____	Signed: _____
Name: _____	Name: _____
Title: _____	Title: _____
Effective Date: _____	Date: _____

Exhibit F

Role-based Access Matrix

Type of Participant		
User Level(s)	**Permission Level(s) (View Data)**	**Permission Level(s) (View and Print Data)**
Medical Clinic		
A B C		
Mental Health Clinic		
A B C		
Acute Care Hospital		
A B C		
Acute Care Hospital Emergency Department		
A B C		
Specialty Care Clinic		
A B C		

User Levels:
A. Physician/other licensed health care provider
B. Medical Assistants
C. All other staff

Permission Levels (view and print data):
1. T*o be defined by LANES Policy Committee*
2.
3.

Exhibit G

Matrix of Components

Environment/Server/Activity	Owner	Comments
Root Server		
Mirth Appliance (MirthConnect, MirthMatch, MirthResults, etc.)		
Hardware platform (typically VM), OS, baseline software	Mirth	Hosted by Mirth through LANES
Mirth Application Support	Mirth	Mirth Tools support
Software developed on tools	LANES	
MirthConnect		
Connectivity	LANES	Establishing minimum security requirements, validating connectivity, production security on Root server connections
	Participant	Confirming security on their end of the connection, keeping it secure and updated ongoing in Production
Message Data	LANES	Proper, secure receipt
	Participant	Reliable, accurate message structure
Message Translation	LANES	As required for consumption

Environment/Server/Activity			Owner	Comments
Root Server				
		Clinical Data Consumption	LANES/Mirth	proper filing, working with Mirth if data filing issues need resolution
	Mirth Results			
		DB Security	LANES	Hosted by Mirth through LANES
		Portal Security (LANES Portal)	LANES/Mirth	Mirth-hosted utility, should security issues arise.
			Participant	Access to portal accounts being compromised
	Initiate Connectivity			
		MPI Filing	Mirth	MPI Filing built and supported by Mirth
		Mirth/Initiate API Connection	LANES/Mirth	LANEs For network support, Mirth if API issues occur
		MPI Data	LANES	Data stored securely in LANES hosting site. Rules algorithms determined by LANES

Environment/Server/Activity			Owner	Comments
Edge Server				
	Mirth Appliance (MirthConnect, MirthMatch, MirthResults, etc.)			
		Hardware platform (typically VM), OS, baseline software	Participant	Hosted by Participant
		Mirth Application Support	Mirth	Mirth Tools support
		Software developed on tools	LANES	
	MirthConnect			
		Connectivity	LANES	Internal network connections behind the firewall
			Participant	Internal network connections behind the firewall
		Message Data	LANES	Proper, secure receipt
			Participant	Reliable, accurate message structure
		Message Translation	LANES	As required for consumption
		Clinical Data Consumption	LANES/Mirth	proper filing, working with Mirth if data filing issues need resolution
	Mirth Results			
		DB Security	Participant	Hosted in their firewall
		Portal Security (LANES Portal)	LANES/Mirth	Mirth-hosted utility, should security issues arise.
			Participant	Access to portal accounts being

Environment/Server/Activity			Owner	Comments
Edge Server				
				compromised
		Coordination with Root instance for Display	LANES	Data collection for presentation
	Initiate Connectivity			
		MPI Filing	Mirth	MPI Filing built and supported by Mirth
		Mirth/Initiate API Connection	LANES/Mirth	via Root Server
		MPI Data	LANES	Data stored securely in LANES hosting site. Rules algorithms determined by LANES