



Monterey County Board of Supervisors

168 West Alisal Street,
1st Floor
Salinas, CA 93901
831.755.5066

Board Order

Agreement No.: A-13293

Upon motion of Supervisor Phillips, seconded by Supervisor Salinas and carried by those members present, the Board of Supervisors hereby:

- a. Authorized the Director of Health or the Assistant Director of Health to execute a Health Information Exchange Provider Participation Agreement (Monterey County Provider Participants) ("Participation Agreement") with Central Coast Health Connect, LLC (CCHC), for participation in the county's Health Information Exchange (HIE) for the period of September 15, 2016 through June 30, 2018, and
- b. Authorized the Director of Health or the Assistant Director of Health to sign up to three (3) future amendments to the Participation Agreement where the total amendments do not significantly alter the scope of work, and
- c. Authorized use of CCHC's Attestation Form, pursuant to which each health care provider accessing the HIE at the Health Department or Natividad Medical Center shall attest compliance with the terms and conditions of the Participation Agreement.

PASSED AND ADOPTED on this 13th day of September 2016, by the following vote, to wit:

AYES: Supervisors Armenta, Phillips, Salinas, Parker and Potter

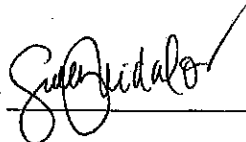
NOES: None

ABSENT: None

I, Gail T. Borkowski, Clerk of the Board of Supervisors of the County of Monterey, State of California, hereby certify that the foregoing is a true copy of an original order of said Board of Supervisors duly made and entered in the minutes thereof of Minute Book 79 for the meeting on September 13, 2016.

Dated: September 16, 2016
File ID: A 16-287

Gail T. Borkowski, Clerk of the Board of Supervisors
County of Monterey, State of California

By 
Deputy



Monterey County

168 West Alisal Street,
1st Floor
Salinas, CA 93901
831.755.5066

Board Report

Legistar File Number: A 16-287

September 13, 2016

Introduced: 8/25/2016

Current Status: Agenda Ready

Version: 1

Matter Type: BoS Agreement

TITLE:

- a. Authorize the Director of Health or the Assistant Director of Health to execute a Health Information Exchange Provider Participation Agreement (Monterey County Provider Participants) ("Participation Agreement") with Central Coast Health Connect, LLC (CCHC), for participation in the county's Health Information Exchange (HIE) for the period of September 15, 2016 through June 30, 2018, and
- b. Authorize the Director of Health or the Assistant Director of Health to approve an Attestation Form, that will require each provider accessing the HIE to attest compliance with the terms and conditions of the Participation Agreement, and
- c. Authorize the Director of Health or the Assistant Director of Health to sign up to three (3) future amendments to the Participation Agreement where the total amendments do not significantly alter the scope of work.

RECOMMENDATION:

- a. Authorize the Director of Health or the Assistant Director of Health to execute a Health Information Exchange Provider Participation Agreement (Monterey County Provider Participants) ("Participation Agreement") with Central Coast Health Connect, LLC (CCHC), for participation in the county's Health Information Exchange (HIE) for the period of September 15, 2016 through June 30, 2018, and
- b. Authorize the Director of Health or the Assistant Director of Health to approve an Attestation Form, that will require each provider accessing the HIE to attest compliance with the terms and conditions of the Participation Agreement, and
- c. Authorize the Director of Health or the Assistant Director of Health to sign up to three (3) future amendments to the Participation Agreement where the total amendments do not significantly alter the scope of work.

SUMMARY/DISCUSSION:

Central Coast Health Connect, LLC (CCHC) is a health information organization (HIO), created to oversee and facilitate a HIE, which will mobilizes healthcare information electronically across organizations within the Monterey County.

CCHC is managed by a Board of Managers and its founding members include Community Health Innovations, LLC (CHI) and Salinas Valley Memorial Hospital (SVMH). CCHC has contracted with CHI to perform day-to-day management of the HIE.

The Participation Agreement sets forth the terms of participation between the Health Department and CCHC and includes CCHC insurance requirements; general liability, errors and omissions, cyber liability and indemnification language. The Terms and Conditions are included as part of the Agreement and establish the conditions under which the Health Department will provide data and access data through CCHC's HIE. CCHC Privacy and

Security Policies and Procedures are also included as part of the Agreement and govern how CCHC will safeguard patient information and ensure compliance with patient privacy laws. These policies were developed with the participation of the Information Technology and Compliance staff and outside experts of NMC, Community Hospital of the Monterey Peninsula (CHOMP), SVMH and CHI. The provider Attestation Form is included and will be used by both the Health Department and Natividad Medical Center to ensure that all HIE authorized users providing services will comply with the terms of the Participation Agreement.

Approval of the recommended action will allow the Monterey County Health Department to become a participant in CCHC's HIE and begin securely accessing and sharing patient health data with other participating healthcare providers for the purpose of reducing health disparities, improving engagement of patients and families, improving care coordination, population and public health and improving communication between hospitals, clinics and care providers while maintaining privacy and security of patient health information.

This work supports the Monterey County Health Department 2011 - 2015 Strategic Plan initiative: Ensure access to culturally and linguistically appropriate, customer-friendly, quality health services. It also supports one or more of the ten essential public health services, specifically: 4) Mobilize community partnerships and action to identify and solve health problems, and 5) Develop policies and plans that support individual and community health efforts.


OTHER AGENCY INVOLVEMENT:

County Counsel, the Auditor-Controller and Contracts/Purchasing have reviewed and approved the Agreement. Risk has reviewed and accepts the non-standard provisions.

FINANCING:

There are no fiscal provisions included as part of this Agreement.

Prepared by: Sheena Morales, Management Analyst III, x1393

Approved by: Elsa M. Jimenez, Director of Health, x4526 

Attachments:

Central Coast Health Connect Participation Agreement is on file with the Clerk of the Board
Central Coast Health Connect Attestation Form is on file with the Clerk of the Board

ATTESTATION FORM

I, _____, hereby attest that I am a provider with _____
("Provider Participant"). I further attest that my signature below signifies my agreement to be
bound by and comply with all the terms of the Health information Exchange Provider
Participation Agreement, the Terms and Conditions for Health Information Exchange
Organization Provider Participation Agreement, and Central Coast Health Connect Security &
Privacy Policy and Procedure Manual.

Provider Name: _____

Signature: _____

Date: _____

**HEALTH INFORMATION EXCHANGE PROVIDER PARTICIPATION
AGREEMENT**

(MONTEREY COUNTY PROVIDER PARTICIPANTS)

This **HEALTH INFORMATION EXCHANGE PROVIDER PARTICIPATION AGREEMENT (Monterey County Provider Participants)**, including all of the exhibits described herein (collectively, the "Agreement") is made and entered into this 15th day of September 2016 ("Effective Date") by and between **Central Coast Health Connect LLC**, a California limited liability company with its principal place of business at 10 Ragsdale Dr. Suite 102, Monterey Ca. 93940 ("**CCHC**" or "**HIO**") and the County of Monterey, on behalf of the Health Department, with its principal place of business at 1270 Natividad Road, Salinas, CA 93906 ("**Provider Participant**").

RECITALS

A. CCHC, as a health information organization ("HIO"), seeks to facilitate the adoption of and promotion of the use of health information technology ("HIT") in the interests of quality of care, patient safety and health care efficiency, while also maintaining patient data security and privacy. In support of these objectives, CCHC is facilitating the implementation and use of a community health record and health information exchange system in Monterey County to help link, electronically, physician practices, hospitals and other health care or related entities (collectively, the Health Information Exchange" or "HIE").

B. The HIE will permit Provider Participant to contribute, as a "Data Provider", clinical patient information to such community health record which is made available to other Provider Participants of the HIE, and/or (ii) Provider Participant's Authorized Users with the ability to access such consolidated clinical records, as "Data Recipients" as further described in the Terms and Conditions for Health Information Exchange Organization Provider Participant's Agreement (the "Terms and Conditions") attached hereto as Exhibit "A".

C. CCHC, in its capacity as an HIO, facilitates collaboration among Provider Participants to establish the terms and conditions under which Patient Data may be shared, including the permissible purposes for such exchange of Patient Data and the responsibility of Provider Participants (as more particularly described in the Terms and Conditions) to all parties entering into a Provider Participation Agreement with HIO (collectively, "Provider Participants").

D. Provider Participant wishes to participate in the HIE in accordance with the terms and conditions of this Agreement;

E. This Agreement specifically applies to the environment of the HIE, and sets forth the terms and conditions that govern Provider Participant's Provider Participation in the HIE.

AGREEMENT

In consideration of the foregoing Recitals (which are incorporated herein by this reference) and the mutual covenants and agreements contained herein, the parties hereto agree as follows:

1. Provider Participation. Provider Participant shall participate in the HIE, as and to the extent described in this Agreement, and subject to and in accordance with the relevant terms of this Agreement, and all Exhibits described in Section 3 attached to this Agreement.

2. Authorized Users. Provider Participant shall identify all Authorized Users and update this information as required by Sections 4.1 and 4.2 of the Terms and Conditions using the Authorized User Form provided by HIO.

3. Incorporation of Exhibits. This Agreement hereby incorporates by reference and includes the following Exhibits attached hereto:

(a) Exhibit "A" - Terms and Conditions for Health Information Exchange Organization Provider Participant's Agreement which describes the terms and conditions with which HIO and the Provider Participant shall comply related to Provider Participation in and the operations of the HIE;

(b) Exhibit "B" - HIE Policies and Procedures, which may be amended from time to time, in accordance with this Agreement.

(c) Exhibit "C" - Business Associate Agreement, which sets forth the obligations of HIO and a business associate of Provider Participant (the "Business Associate Agreement").

(d) Exhibit "D" - Fee Schedule which sets forth any applicable Service Fee or other fee.

Notwithstanding anything to the contrary contained in this Agreement, to the extent that the terms of the Business Associate Agreement conflict with the terms of this Agreement, the terms of the Business Associate Agreement shall prevail. To the extent that the terms of the HIE Policies and Procedures conflict with the terms of this Agreement, the terms of this Agreement shall prevail.

4. Definitions. Capitalized terms that are not defined in this Agreement shall have the meanings described in the Terms and Conditions and the Business Associate Agreement.

5. Term and Termination. The term of this Agreement shall commence on the Effective Date and shall continue until it is terminated as described in the Terms and Conditions.

6. HIE Portal. Notwithstanding anything to the contrary contained in this Agreement or the Terms and Conditions, the HIE Portal will be provided by RelayHealth or such other technology vender selected by HIE.

7. Miscellaneous Provisions.

- a. Applicable Law. The interpretation of this Agreement and the Terms and Conditions and the resolution of any disputes arising thereunder 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 or the Terms and Conditions, the venue of such action shall be exclusively in Monterey County, in the State of California.
- b. Non-Assignability. No rights of the Provider Participant under this Agreement may be assigned or transferred by the Provider Participant, either voluntarily or by operation of law, without the prior written consent of HIO, which it may withhold in its sole discretion, and any attempted assignment without the prior written consent of HIO shall be null and void and of no force or effect.
- c. Subcontracting. Notwithstanding anything to the contrary contained this Agreement or the Terms and Conditions, HIO shall have the right, at its sole discretion, to select and subcontract with other persons or entities to perform any of the functions it performs or to provide any of the services it provides as an HIO.
- d. Third-Party Beneficiaries. There shall be no third-party beneficiaries of this Agreement.
- e. Supervening Circumstances. Neither the Provider Participant nor HIO 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 7(e) (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.
- f. Severability. Any provision of this Agreement or the Terms and Conditions that shall prove to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provisions of this Agreement or the Terms and Conditions, and such other provisions shall remain in full force and effect.
- g. Notices. Any and all notices required or permitted under this Agreement or the Terms and Conditions shall be sent by United States mail, overnight delivery service, or facsimile transmission to the address provided by the Provider Participant to HIO or such different addresses as a party may designate in writing. If the Provider Participant has supplied HIO with an electronic mail address, HIO may give notice by email message addressed to such address; provided that if HIO receives notice that the email message was not delivered, it shall give the notice by United States mail, overnight delivery service, or facsimile.
- h. Waiver. No provision of this Agreement or the Terms and Conditions 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.

- i. Independent Contractors. In the performance of their respective responsibilities under this Agreement, HIO and the Provider Participant are and shall be at all times acting as the independent contractor of the other, and not by virtue of this Agreement or otherwise under these Terms and Conditions acting as an employee, agent, or partner of, or joint venture with, the other.
- j. Complete Understanding. This Agreement, including the Terms and Conditions and all other Exhibits to this Agreement contains the entire agreement between HIO and Provider 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..
- k. Counterparts. This Agreement may be executed in any number of counterparts, each of which will be deemed an original as against the Provider Participant whose signature appears thereon, but all of which taken together will constitute but one and the same instrument.
- l. Amendment. This Agreement may be amended or modified only by an instrument in writing signed by the parties, except as otherwise provided by the Terms and Conditions.

[Remainder of Page Intentionally Left Blank. Signature Page to Follow]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized officer as of the date set forth above.

COUNTY OF MONTEREY

**CENTRAL COAST HEALTH
CONNECT LLC**

Printed Name: Elsa Jimenez

Printed Name: Elizabeth Lorenzi

Signature: [Handwritten Signature]

Signature: [Handwritten Signature]

Title: Director of Health

Title: VP/COO

Date: 9-27-16

Date: 08/12/16

Approved as to Fiscal Provisions:

[Handwritten Signature]
Deputy Auditor/Controller 8-23-16

~~Date~~ MANAGEMENT
COUNTY OF MONTEREY

~~APPROVED AS TO LIABILITY PROVISIONS:~~
INSURANCE LANGUAGE

[Handwritten Signature]
Risk Management
Date: 8/23/16

Approved as to Form:

[Handwritten Signature]
Deputy County Counsel
Date: 8/19/16

Contracts/Purchasing
Date:

EXHIBIT "A"

**TERMS AND CONDITIONS FOR HEALTH INFORMATION EXCHANGE
ORGANIZATION PROVIDER PARTICIPATION AGREEMENT**

[TO BE ATTACHED]

TERMS AND CONDITIONS FOR
HEALTH INFORMATION EXCHANGE ORGANIZATION
PROVIDER PARTICIPATION AGREEMENT

Section 1
INTRODUCTORY AND GENERAL PROVISIONS

1.1 Introduction. These applicable provisions of these Provider Participant Terms and Conditions for Health Information Exchange Organization Participant's Agreement ("Provider Participant Terms and Conditions") are incorporated by reference into each Health Information Exchange Organization Provider Participant's Agreement (each, a "Provider Participation Agreement") entered into by and between Central Coast Health Connect LLC ("CCHC" or "HIO"), and a Provider Participant.

1.2 Effective Date. The Effective Date of these Provider Participant Terms and Conditions is the effective date of the Provider Participation Agreement.

1.3 Nature of Organization. CCHC is a California limited liability company owned and organized by the Founding Hospital Organization Members (as defined in Section 1.5.9 below). CCHC, as a health information organization ("HIO") seeks to facilitate the adoption of and promotion of the use of health information technology ("HIT") in the interests of quality of care, patient safety and health care efficiency, while also maintaining patient data security and privacy. In support of these objectives, CCHC is facilitating the implementation and use of a community health record and health information exchange system to help link, electronically, all interested patients, physician practices, hospitals and other health care or related entities (collectively, the "Health Information Exchange" or "HIE") in a manner that complies with all applicable laws and regulations, including, without limitation those protecting the privacy and security of health information.

1.4 Description of Services. CCHC, in its capacity as an HIO facilitates collaboration and exchange of information among participants in the HIE. The Services provided by CCHC include, but are not limited to: granting rights to access a System and the related Services that allow the exchange of Patient Data between different health care facilities; establishing the terms and conditions under which Patient Data may be shared; establishing the permissible purposes for such exchange of Patient Data; overseeing privacy and security of the HIE; managing Patient opt-out requests on behalf of participants in the HIE; overseeing the type of patient accounts that are permitted to access the HIO; acting as the initial point of contact for support issues; and managing the onboarding, intake, and termination of Participants and Users.

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

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

1.5.2 "Applicable Law" means all applicable statutes, regulations, or ordinances of the state(s) or jurisdiction(s) in which the Provider Participant operates, as well as all applicable federal statutes, regulations, standards, and policy requirements.

1.5.3 "Authorized User" means an individual Participant or an individual designated to use the Services on behalf of the Provider Participant, including without limitation, an employee of the Provider Participant, a credentialed member of the Provider Participant's medical staff and/or their designated agent, and/or an affiliated clinic.

1.5.4 "Breach of Privacy or Security" is an acquisition, access, use or disclosure of Patient Data other than in compliance with these Provider Participant Terms and Conditions that pursuant to Applicable Law, including without limitation federal or state data breach notification rules, or regulations, must be reported to affected individuals and/or government officials..

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

1.5.6 "Data Provider" means a Provider Participant that is registered to provide information to HIO for use through the Services.

1.5.7 "Data Recipient" means a Provider Participant that uses the Services of the HIO to obtain health information.

1.5.8 "Effective Date" means the Effective Date of these Provider Participant Terms and Conditions specified pursuant to Section 1.2 (Effective Date).

1.5.9 "Founding Hospital Organization Members" means Community Hospital of the Monterey Peninsula and Salinas Valley Memorial Hospital.

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

1.5.11 "HITECH" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (commonly known as "ARRA"), Pub. L. No. 111-5 (February 17, 2009).gm,

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

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

1.5.14 “Participant Type” means the category(ies) of Participant to which a particular Participant is assigned by HIO based upon that Participant’s role in the health care system.

1.5.15 “Patient Data” means patient information (including but not limited to “Protected Health Information” as defined in HIPAA or “Medical Information” as defined in the CMIA) provided, or made available for exchange, by a Data Provider through HIE System and Services pursuant to Section 7.2 (Provision of Data).

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

1.5.17 “Services” means the health information exchange and related services described in Section 1.4 (Description of Services) for which the Provider Participant registers.

1.5.18 “Suspension” means the temporary discontinuance of access to the Systems or Services. During the suspension, neither the Provider Participant or its Authorized Users shall access the System or Services or be responsible for complying with the terms of this Agreement except those terms that survive termination of this Agreement in accordance with 3.10. Any voluntary suspension shall be for no longer than thirty (30) calendar days during any twelve (12) month period, unless a longer period is agreed to by the Board of Managers of CCHC.

1.5.19 “Policies and Procedures” means, collectively, the policies and procedures, for the operation and use of the System and the Services, including, without limitation, any operations manual, privacy and/or security policies, and technical specifications for the System and/or the Services. The Policies and Procedures shall be adopted by HIO and may be amended from time to time by HIO in accordance with these Provider Participant Terms and Conditions.

1.5.20 “System” means the HIE System that is made accessible to Provider Participants through their contract with HIE Vendor and their Provider Participation Agreement with HIO, as described in the Policies and Procedures.

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

1.5.22 “Unsecured Protected Health Information” means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health & Human Services (“HHS”) through guidance issued pursuant to HITECH.

1.5.23 “Unsuccessful Security Incident” means a security incident (as defined under HIPAA) that does not result in: (1) the unauthorized access, use, disclosure, modification or destruction of information; or (2) material interference with system operations in a party’s information system, including, without limitation, activity such as ping and other

broadcast attacks on that party's firewall, port scans, unsuccessful log-on attempts, denial of service and/or any combination of the foregoing, so long as no such incident results in unauthorized access, use or disclosure of electronic protected health information.

Section 2

DEVELOPMENT AND ADMINISTRATION OF PARTICIPATION AGREEMENTS

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

2.2 Relationships Between Provider Participant Terms and Conditions and Policies and Procedures.

(a) The Policies and Procedures in effect from time to time are incorporated into these Provider Participant Terms and Conditions and are attached to the Provider Participation Agreement as Exhibit "B" thereto. HIO and each Provider Participant shall be required to comply with the applicable provisions of the Policies and Procedures.

(b) HIO may exchange data with such Other HIOs that shall be identified in the Policies and Procedures, provided that such Other HIOs have agreed in their legally binding agreements with the HIO to (i) comply with all laws applicable to the Other HIO, including but not limited to HIPAA and HITECH, and to maintain and enforce appropriate policies and procedures in compliance therewith, (ii) appropriately and, in accordance with applicable industry standards, authenticate the identities and authorization of all the Other HIO's participants capable of exchanging data with or through or otherwise electronically interacting with the Other HIO's electronic systems, (iii) promptly revoke or reduce, as appropriate, the access privileges of the Other HIO's participants who no longer have a need to electronically interact with the Other HIOs electronic systems in the manner or scope permitted by the privileges; and (iv) an appropriate indemnification provision regarding the Other HIOs act or omission related to the foregoing or receipt by an HIO of an inappropriate data request from or through Other HIOs' systems, a Breach or Security Incident with respect to Patient Data, or disclosure of Proprietary and Confidential Information.

2.3 Changes to Provider Participant Terms and Conditions and Policies and Procedures. HIO may amend, repeal and replace these Provider Participant Terms and Conditions and/or the Policies and Procedures at any time, and shall give Provider Participants not less than thirty (30) days' notice of such changes prior to the implementation of such changes. However, if the change is required in order for HIO and/or Provider Participants to comply with applicable laws or regulations, HIO may implement the change within a shorter period of time as HIO determines is appropriate under the circumstances and will provide written notification to Provider Participant for the reason of the change and the effect on the HIO if the change is not implemented. Any such change to these Provider Participant Terms and Conditions and/or Policies and Procedures shall automatically be incorporated by reference into each Provider Participation Agreement, and be legally binding upon HIO and the Provider Participant, as of the effective date of the change.

2.4 Development and Administration of Provider Participation Agreements.

2.4.1 Provider Participation Agreement Required. Only persons who enter into Provider Participation Agreements with HIO or Other HIOs that have entered into legally binding agreements as described in Section 2.2 (Relationships Between Provider Participant Terms and Conditions and Policies and Procedures) shall be permitted to access the System and use the Services. A Participant may act as a Data Provider or as a Data Recipient, or as both, as described in this Section 2.4 (Development and Administration of Provider Participation Agreements). If the Provider Participant is capable of acting as a Data Provider, the Provider Participant must agree to become a Data Provider if requested to do so in writing by the HIO. A Participant may use some or all of the Services, only as specified in Participant's Provider Participation Agreement.

2.5 Change or Termination of Services. HIO may cease to participate in any Other HIO or may make any other change to the Services, or may cease providing the upon not less than ninety (90) days prior written notice to Provider Participants.

Section 3

TERM AND TERMINATION OF PARTICIPATION AGREEMENTS

3.1 Term of Provider Participation Agreements. This Provider Participation Agreement shall take effect on the date specified therein, and shall remain in force and effect until June 30, 2018 (the "Initial Term"). The term of this Provider Participation Agreement may be renewed for additional one (1) year terms (each, a "Renewal Term") following the expiration of the Initial Term or any Renewal Term upon the mutual written agreement of HIO and Provider Participant.

3.2 Participant's Suspension or Termination of Provider Participation Agreement Upon Uncured Breach. Without limiting the obligations of HIO pursuant to Section 10.1 (HIO's Performance of Obligations, Generally), a Provider Participant may suspend or terminate its Provider Participation Agreement upon HIO's failure to perform a material responsibility arising out of the Provider Participant's Provider Participation Agreement, and that failure continues uncured for a period of thirty (30) days after the Provider Participant has given HIO written notice of that failure and requested that HIO cure that failure.

3.3 Provider Participant's Suspension or Termination of Provider Participation Agreement Upon Breach of Privacy or Security. A Provider Participant may suspend or terminate its Provider Participation Agreement immediately upon a Breach of Privacy or Security, as described in Section 9.2 (Reporting of Breaches and Security Incidents), or when such Breach of Privacy or Security continues uncured for a period of thirty (30) days after the Provider Participant has given HIO written notice of that failure and requested in writing that HIO cure that breach.

3.4 Provider Participant's Suspension or Termination of Provider Participation Agreement Upon Breach of Business Associate Agreement. Notwithstanding any other provision of these Terms and Condition to the contrary, the Provider Participant may suspend or terminate its Provider Participation Agreement immediately based upon HIO's material breach of its Business Associate Agreement with the Provider Participant.

3.5 Disposition of Patient Data on Termination. At the time of suspension or termination, Data Recipient may, at its election, retain Patient Data obtained during the term of the Provider Participation Agreement in accordance with the Provider Participant Terms and Conditions, on the Data Recipient's system in compliance with the Data Recipient's document and data retention policies and procedures and Applicable Law.

3.6 HIO's Termination of Provider Participation Agreement Without Cause. Except as provided otherwise in the applicable Provider Participation Agreement, HIO may terminate any Participant's Provider Participation Agreement at any time without cause by giving not less than one hundred eighty (180) days' prior written notice to the Provider Participant.

3.7 Provider Participant's Termination of Provider Participation Agreement Without Cause. Participant may terminate this Provider Participation Agreement at any time without cause by giving not less than thirty (30) days' prior written notice to HIO.

3.8 HIO's Termination of Provider Participation Agreement Upon Uncured Breach. Without limiting the obligations of the Provider Participant pursuant to Section 5.1 (Participant's Performance of Obligations, Generally), HIO may suspend or terminate any Participant's Provider Participation Agreement upon the Provider Participant's failure to perform a material responsibility arising out of the Provider Participant's Provider Participation Agreement, and that failure continues uncured for a period of thirty (30) days after HIO has given the Provider Participant written notice of that failure and requested in writing that the Provider Participant cure that failure.

3.9 Effect of Termination of Provider Participation Agreement. Upon any termination of a Provider Participant's Provider Participation Agreement, that party shall cease to be a Provider Participant and thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services and which process is defined in the HIO's Policy and Procedures.

3.10 Payment of Fees During Term of Suspension. Provider Participant shall remain responsible for the payment of Services Fees during the terms of its suspension.

3.11 Survival of Provisions. The following provisions of the Provider Participant Terms and Conditions shall survive any termination of a Provider Participant's Provider Participation Agreement: Section 4.5 (Responsibility for Conduct of Participant and Authorized Users), Section 8 (Privacy and Security of Patient Data), Section 9 (Business Associate Agreement), Section 12 (Proprietary and Confidential Information), and Section 13.10 (Limitation of Liability)

Section 4 AUTHORIZED USERS

4.1 Identification of Authorized Users. Each Provider Participant shall provide HIO with a list in a medium and format approved by HIO identifying all the Provider Participant's Authorized Users, together with the required information described in the Policies and Procedures concerning "Required Information for Authorized Users," to enable HIO to establish a unique identifier for each Authorized User. The Provider Participant shall update such list whenever an Authorized

User is added or removed by reason of termination of employment or otherwise, in accordance with the processes described in the Policies and Procedures.

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

(a) Has completed a training program conducted by Provider Participant in accordance with Section 5.9 (Training);

(b) Will be permitted by Provider Participant to use the Services and the System only as reasonably necessary for the performance of Provider Participant's activities as the Provider Participant Type under which Participant is registered with HIO;

(c) Has agreed in writing not to disclose to any other person any passwords and/or other security measures issued to the Authorized User pursuant to Section 4.3 (Passwords and Other Security Mechanisms); (ii) to comply with Applicable Law; (iii) to reasonably cooperate with Participant and HIO on all issues related to this Provider Participation Agreement; (iv) to provide or request Patient Data only for permitted purposes; (v) to use Patient Data in accordance with the Provider Participant Terms and Conditions; and (vi) to report any Privacy or Security Breaches to Provider Participant as soon as reasonably practicable after becoming aware of an impermissible access, acquisition, use or disclosure of Patient Data or Security Incident; and

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

4.3 Passwords and Other Security Mechanisms. Based on the information provided by the Provider Participant pursuant to Section 4.1 (Identification of Authorized Users), HIO shall issue a user name and password and/or other security measure to each Authorized User that shall permit the Authorized User to access the System and use the Services. HIO shall provide each such user name and password and/or other security measure to the Provider Participant and the Provider Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Provider Participant removes an individual from its list of Authorized Users, and informs HIO of the change, pursuant to Section 4.1 (Identification of Authorized Users), HIO shall cancel the user name and password and/or other security measure of such individual with respect to the Provider Participant, and cancel and de-activate the user name and password and/or other security measure of such individual if that individual is as a result of the change no longer an Authorized User of any Participant. HIO shall ensure that such changes to access shall be made within two (2) business days of receipt of the request from Provider Participant, except in cases where a Provider Participant requests immediate termination, in which case HIO shall take immediate action and ensure that Authorized User is terminated from accessing the System and Services.

4.4 No Use by Other than Authorized Users. The Provider Participant shall restrict access to the System and, if applicable, use of the Services, only to the Authorized Users the Provider Participant has identified to HIO in accordance with Section 4.1 (Identification of Authorized Users).

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

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

Section 5

GENERAL OBLIGATIONS OF PROVIDER PARTICIPANTS

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

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

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

5.4 Patient Consent. The Provider Participant will obtain any consent or authorization that may be required by HIPAA or applicable law, prior to exchanging Patient Data with the HIO. Provider Participant will promptly notify HIO of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect HIO's use or disclosure of Protected Health Information. Provider Participant will provide such notice no later than five (5) days prior to the effective date of the change.

5.5 Patient Opt-Out. The Provider Participant shall promptly communicate all opt-out requests from patients to HIO. HIO shall communicate all opt-out requests to HIE Vendor within two (2) business days of receipt of the request from Provider Participant or patient.

5.6 Software and Hardware Provided by Provider Participant. Provider Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the Services, and provide to HIO all information required to be provided by the Provider Participant. Each Provider Participant shall be responsible for directly entering into a licensing, subscription, or other agreement with the HIE Vendor as may be required to utilize the HIE. Each Provider Participant's Required Hardware and Software shall conform to the HIE Vendor's then-current specifications. As part of the Provider Participant's obligation to provide Participant's Required Hardware and Software, the Provider Participant shall be responsible for ensuring that all the Provider 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. All costs necessary to connect and access the System will be borne by the Provider Participant.

5.7 Licenses, Subscription, and/or Other Agreements. The System may include certain third-party software, hardware, and services, which are subject to separate licenses or subscription or other agreements or may require that a Provider Participant enter into such agreements with third-party vendors. The Provider Participant shall execute such agreements as may be required for the use of such software, hardware or services. The specifications, service standards and/or warranties to be provided by the vendor or vendors of the third-party software, hardware, and services shall be described in the applicable agreements for those third-party products.

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

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

5.10 Ownership. HIO does not convey and Provider Participant does not obtain any right, title or interest in, any intellectual property rights in or to the HIO, the Services or the System by virtual of this Agreement, whether existing prior to the Effective Date, or created, developed, utilized, or provided by HIO during the Term.

Section 6 DATA RECIPIENT'S USE OF SYSTEM AND SERVICES

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

6.1 Grant of Rights to Use System and Services.

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

6.1.2 Permitted Purposes for Use of System and Services. A Data Recipient may use the System and the Services only to locate and retrieve Patient Data for purposes of treatment, payment or health care operations, as those terms are defined in HIPAA and subject to any limitations of Applicable Law. Such permitted purposes include:

- a. Treatment of the individual who is the subject of the Patient Data;
- b. Payment activities of the health care provider for the individual who is the subject of the Patient Data which includes, accessing or using Patient Data to support a claim for reimbursement submitted by a health care provider to a health plan;
- c. Health care operations of the covered entity Data Provider that is disclosing Patient Data that contains Protected Health Information;
- d. Health care operations of the covered entity Data Provider requesting Patient Data that contains Protected Health Information if (i) the Data Recipient is a health care provider who has an established Treatment relationship with the individual who is the subject of the Patient Data or is an Authorized User acting on behalf of such health care provider; and (ii) the purpose of the use is for those health care operations listed in paragraphs (1) or (2) of the definition of health care operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such health care provider.

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

6.3 Compliance With Applicable Laws. Without limiting the generality of Section 6.4 (Prohibited Uses of System and Services), the Data Recipient shall in its use of the System and the Services comply with all applicable laws and regulations, including without limitation HIPAA and the CMIA.

6.4 Prohibited Uses of System and Services. A Data Recipient shall not use or permit the use of the System or the Services for any prohibited use described in the Policies and Procedures,

which are incorporated herein by reference.

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

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

6.5 Permitted and Prohibited Uses and Disclosures of Patient Data. A Data Recipient may use and disclose Patient Data acquired through the use of the System and the Services as and to the extent permitted by law; provided, that the Provider Participant shall not use or disclose Patient Data in any manner prohibited pursuant to Section 7.5 (Limitations on Use and Disclosure of Patient Data).

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

Section 7 DATA PROVIDERS' USE OF SYSTEM AND SERVICES

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

7.1 Grant of Rights by HIO.

7.1.1 Grant by HIO. HIO grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, revocable, personal, nontransferable, limited right to have access to and to use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider's Use of System and Services), subject to the Data Provider's full compliance with the Terms and Conditions, Data Provider's Participation Agreement and any agreement between Data Provider and HIE Vendor. HIO retains all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

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

7.3 Measures to Assure Accuracy of Data.

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

7.4 Grant of License to Use Patient Data. Subject to Section 7.5 (Limitations on Use of Patient Data), the Data Provider grants to HIO a fully-paid, non-exclusive, royalty-free right and license (i) to license and/or otherwise permit others to access through the System and use all Patient Data provided by the Data Provider in accordance with the Policies and Procedures and these Provider Participant Terms and Conditions, (ii) to use such Patient Data to perform the Other Activities HIO performs pursuant to Section 10.9 (Other Activities), and (iii) to use such Patient Data to carry out HIO's duties under the Policies and Procedures and these Provider Participant Terms and Conditions for the term of the Participation Agreement.

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

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

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

7.6 Limitations on Data Provider's Provision of Patient Data. The Data Provider shall provide Patient Data only to the extent permitted by applicable law.

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

Section 8
PRIVACY AND SECURITY OF PATIENT DATA

8.1 Compliance with Policies and Procedures. HIO and each Provider Participant shall comply with the standards for privacy and security of patient health information, including without limitation, protected health information described by HIPAA and medical information described in the CMLA, as provided in the Policies and Procedures which are incorporated herein by reference.

8.2 Reporting of Breaches and Security Incidents.

8.2.1 Reporting Breaches and Security Incidents. Without limiting any Business Associate Agreement entered into pursuant to Section 9 (Business Associate Agreement), HIO and Provider Participant shall report to the other any use or disclosure of Patient Data not provided for by these Provider Participant Terms and Conditions of which HIO or Provider Participant becomes aware, any security incident (other than an Unsuccessful Security Incident) concerning electronic Patient Data accessed, used, or disclosed through the Systems or Services and any Breach of Privacy or Security. This report shall be made without unreasonable delay and in no case later than two (2) business days as provided in the Policies and Procedures.

8.2.2 Reporting Unsuccessful Security Incidents. The Provider Participant shall annually provide a report to HIO describing in summary form the nature and extent of Unsuccessful Security Incidents concerning Patient Data experienced by the Provider Participant in accessing or using the System or Services during the period covered by that report, as more specifically described in the Policies and Procedures.

8.2.3 Reports to Provider Participants. HIO shall on a monthly basis provide a report to all Provider Participants describing all Breaches of Privacy or Security of which HIO becomes aware or that are reported by Provider Participants to HIO during the prior month pursuant to Section 8.2.1 (Reporting Breaches and Security Incidents). HIO shall on an annual basis provide a report to all Provider Participants describing in summary form Unsuccessful Security Incidents reported by Provider Participants to HIO pursuant to Section 8.2.2 (Reporting Unsuccessful Security Incidents).

8.2.4. Ownership. Provider Participant does not convey and HIO does not obtain any ownership in Patient Data pursuant to the terms of the Provider Participation Agreement.

Section 9 BUSINESS ASSOCIATE AGREEMENT

The HIO is a business associate (as defined by HIPAA) of Provider Participant, and therefore shall enter into a Business Associate Agreement with that Provider Participant in the form attached as Exhibit "C" to the Provider Participation Agreement.

Section 10 HIO'S OPERATIONS AND RESPONSIBILITIES

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

10.2 Provider Participation Agreements. HIO shall require that all Provider Participants enter

into a Provider Participation Agreement to comply with the Provider Participant Terms and Conditions. HIO shall enter into Provider Participation Agreements only with those persons that satisfy the requirements for participation set forth in the Policies and Procedures.

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

10.4 Training. On an as needed basis, HIO shall provide training or training materials to each Provider Participant and/or Authorized User regarding the Provider Participant's and/or the Authorized User's rights and obligations under its Provider Participation Agreement and the Provider Participant Terms and Conditions, and the access and use of the System and Services, including such user manuals and other resources HIO determines appropriate to support the System and Services, including without limitation training for new or additional Authorized Users when added by the Provider Participant.

10.5 Telephone Support. On an as needed basis, HIO shall provide a person to answer telephone calls from patients and providers during normal business hours.

10.6 Audits and Reports. On an as needed basis, as determined by HIO, HIO (either directly or through HIE Vendor) shall provide reports, to each Provider Participant which at HIO's discretion, may include, without limitation, the following:

10.6.1 Participation Reports.

10.6.2 Usage Reports.

10.6.3 Summaries of Reports to Public Agencies.

10.6.4 Audit Trail Reports regarding any Privacy or Security breaches that involve the exchange of Patient Data through the System or Services.

10.7 Access to Patient Data. HIO shall permit access to Patient Data maintained by HIO only by Provider Participants only in compliance with the Policies and Procedures.

10.8 De-Identified Data. HIO may aggregate and de-identity or provide for the aggregation and de-identification of Patient Data exchanged through the HIE. Any de-identified data may be used only for the activities of the HIO or as otherwise agreed to in writing by Provider Participants.

10.9 Other Activities. HIO shall perform the other activities, including without limitation any additional services or functions involving the Services and/or Patient Data, as and to the extent described in the Policies and Procedures.

10.10 Compliance with Laws and Regulations. Without limiting any other provision of these Provider Participant Terms and Conditions, the Parties shall comply with all Applicable Laws.

Section 11 FEES AND CHARGES

11.1 Payment. The Provider Participant shall pay all required Service Fees and any Miscellaneous Charges in accordance with the terms of Participant's Provider Participation Agreement.

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

11.3 Suspension of Service. Failure to pay Service Fees and Miscellaneous Charges within the time-frames set forth in Participant's Provider Participation Agreement shall result in termination of the Provider Participant's access to the System and/or use of the Services on ninety (90) days' prior written notice of termination.

11.4 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 Provider Participant shall pay any tax (excluding taxes on HIO's net income) that HIO may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services provided pursuant to the Provider Participant Terms and Conditions.

11.5 Other Charges and Expenses. The Provider Participant shall be solely responsible for any other charges or expenses the Provider 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.

11.6 Non-Appropriation. To the extent that Provider Participant is required during the term of this Agreement to pay Service Fees, Miscellaneous Charges, or other charges or expenses, Provider Participant's payments to HIO under this Provider Participation Agreement are funded by local, state and federal governments. If funds from local, state and federal sources are not obtained and continued at a level sufficient to allow for Provider Participant's purchase of the indicated quantity of services, then Provider Participant may give written notice of this fact to HIO, and the obligations of the parties under this Provider Participation Agreement shall terminate immediately, or on such date thereafter, as Provider Participant may specify in its notice, unless in the meanwhile the parties enter into a written amendment modifying this Provider Participation Agreement.

Section 12 PROPRIETARY AND CONFIDENTIAL INFORMATION

12.1 Scope of Proprietary and Confidential Information. In the performance of their respective responsibilities pursuant to the Provider Participant Terms and Conditions, HIO and Provider Participants may come into possession of certain Proprietary and Confidential Information of the other. For the purposes hereof, "Proprietary and Confidential Information" means all trade secrets,

business plans, marketing plans, know-how, data, contracts, documents, scientific and medical concepts, member and customer lists, costs, financial information, profits and billings, and referral sources, existing or future services, products, operations, management, pricing, financial status, goals, strategies, objectives, and agreements of HIO or the Provider Participant, as the case may be, whether written or verbal, that are confidential in nature; provided, however, that Proprietary and Confidential Information shall not include any information that:

- (a) Is in the public domain;
- (b) Is already known or obtained by any other party other than in the course of the other party's performance pursuant to the Provider Participant Terms and Conditions, and without breach of any confidentiality, nondisclosure or other agreement by such other party;
- (c) Is independently developed by any other party; 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 the Provider Participant Terms and Conditions, or any other confidentiality or nondisclosure agreement by such other party.

12.2 Nondisclosure of Proprietary and Confidential Information. HIO and the Provider Participant each (i) shall keep and maintain in strict confidence all Proprietary and Confidential Information received from the other, or from any of the other's employees, accountants, attorneys, consultants, or other agents and representatives, in connection with the performance of their respective obligations under the Provider Participant Terms and Conditions; (ii) shall not use, reproduce, distribute or disclose any such Proprietary and Confidential Information except as permitted by the Provider Participant Terms and Conditions; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure. This provision shall not apply to information that is subject to disclosure in response to a request pursuant to the California Public Records Act. To the extent any Party is required to disclose Proprietary and Confidential Information pursuant to the California Public Records Act, a court order, subpoena or any other form of compelled disclosure, the disclosing Party must provide advance notice sufficient to allow the other party the opportunity to challenge the disclosure of information.

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

12.4 Notice of Disclosure. Notwithstanding any other provision hereof, nothing in this Section

12 (Proprietary and Confidential Information) shall prohibit or be deemed to prohibit a party hereto from disclosing any Proprietary and Confidential Information (or any other information the disclosure of which is otherwise prohibited hereunder) to the extent that such party becomes legally compelled to make such disclosure by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction, and such disclosures are expressly permitted hereunder; provided, however, that a party that has been requested or becomes legally compelled to make a disclosure otherwise prohibited hereunder by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction shall provide the other party with notice thereof within five (5) calendar days, or, if sooner, at least three (3) business days before such disclosure will be made so that the other party may seek a protective order or other appropriate remedy. In no event shall a party be deemed to be liable hereunder for compliance with any such subpoena or order of any court, administrative agency or other governmental body of competent jurisdiction.

Section 13
DISCLAIMERS, EXCLUSIONS OF WARRANTIES, LIMITATIONS OF
LIABILITY, INDEMNIFICATION, AND INSURANCE

13.1 Carrier Lines. By using the System and the Services, each Provider Participant shall acknowledge that access to the System is to be provided over various facilities and communications lines, and information will be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which are beyond HIO's control. HIO assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at user's risk and is subject to all applicable local, state, national, and international laws.

13.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Provider Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. HIO disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

13.3 Other Provider Participants. By using the System and the Services, each Provider Participant shall acknowledge that other Provider Participants have access to the System and Services, and that other parties have access to the information contained in the System through their participation in an Other HIO. Such other Provider Participants have agreed to comply with the CCHC's Policy and Procedures (attached to the Provider Participation Agreement as Exhibit "B"), concerning use of the information; however, the actions of such other parties are beyond the control of the HIO. Accordingly, HIO does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any

information on the System resulting from any Participant's actions or failures to act.

13.4 Provider Participant's Actions. The Provider 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 Provider Participant or a member of the Provider Participant's workforce.

13.5 Unauthorized Access; Lost or Corrupt Data. HIO is not responsible for unauthorized access to the Provider 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 Provider Participant is solely responsible for validating the accuracy of all output and reports and protecting the Provider Participant's data and programs from loss by implementing appropriate security measures, including routine backup procedures.

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

13.7 Patient Care. Without limiting any other provision of the Provider Participant Terms and Conditions, the Provider Participant and the Provider 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. Patient Data obtained through the System and Services is not a substitute for any Provider Participant or Authorized User, if that person/entity is a health care provider, obtaining whatever information he/she/it deems necessary, in his/her professional judgment, for the proper treatment of a patient. No Participant or Authorized User shall have any recourse against, and through the Provider Participation Agreements that apply thereto, each shall waive, any claims against HIO for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of the System and/or the Services or the data made available thereby.

13.8 Insurance. Without limiting the HIO's duty to indemnify, HIO shall maintain in effect without interruption during the term hereof policies of commercial general liability insurance with a minimum limit of \$1,000,000 per occurrence and \$2,000,000 annual aggregate, which shall include coverage for hired and non-owned vehicles; and professional errors and omissions liability insurance with \$1,000,000 per claim and \$2,000,000 annual aggregate;. All coverages, except surety, shall be issued by companies which hold rating of not less than A-VII, according to the current Best's Key Rating Guide. Failure by HIO to maintain such insurance is a default of this Agreement, which entitles Provider Participant, at its sole discretion, to terminate the Agreement

immediately. As least annually, the HIO shall review the adequacy of the insurance coverage and whether the existing coverage limits sufficiency address potential risk to the HIO.

13.9 Indemnification.

- 13.9.1 Indemnification, Generally. To the extent permitted by applicable law, HIO and Provider Participant (each, an “Indemnifying Party”) each shall defend, indemnify, and hold the other and other Provider Participants (each, an “Indemnified Party”) harmless from any liability, loss, injury, damages, or claims arising out of, or in connection with the act or omission of the Indemnifying Party (including its officers, employees, agents and subcontractors) or any of the Indemnifying Party's Authorized Users in performance of this Agreement, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Provider Participation Agreement or Business Associate Agreement, excepting only loss, injury or damage caused by the negligence or willful misconduct of personnel employed by the Indemnified Party. Indemnifying Party shall reimburse Indemnified Party for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which the Indemnifying Party is obligated to indemnify, defend and hold harmless the Indemnified Party under this Agreement.
- 13.9.2 Specific Indemnities. Notwithstanding Section 13.9.1 (Indemnification, Generally), to the extent permitted by applicable law, an Indemnifying Party shall hold Indemnified Party free of and harmless from all liability, judgments, costs, damages, claims, or demands, including any administrative costs associated with providing notice, printing and mailing costs, public relations costs, attorney fees, and costs of mitigating the harm (which may include the costs of obtaining up to one year of credit monitoring services and identity theft insurance) for affected individuals whose PHI has or may have been compromised as a result of any Breach of Privacy or Security arising out of, or in connection with the act or omission of the Indemnifying Party (including its officers, employees, agents and subcontractors) or any of the Indemnifying Party's Authorized Users.
- 13.9.3 Rules for Indemnification. Any indemnification made pursuant to this Provider Participation Agreement, the Terms and Conditions, or the Business Associate 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 Indemnified Party. In the event that a lawsuit is brought against the Indemnified Party, the Indemnifying Party shall, at its sole cost and expense, defend the Indemnified Party, if the Indemnifying Party demands indemnification by written notice given to the Indemnifying Party within a period of time wherein the Indemnifying Party is not prejudiced by lack of notice. The indemnification obligations of HIO and Provider Participant 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.

13.10 Limitation of Liability. With respect to the HIO's and Provider Participant's rights and obligations with respect to indemnification under Section 13.9 (Indemnification), HIO's liability to Provider Participant or Provider Participant's liability to HIO under the Provider Participation Agreement or these Provider Participant Terms and Conditions shall not exceed the stated aggregate limit of their then current applicable insurance coverage, provided that HIO's insurance is at all times maintained in accordance with Section 13.8 (Insurance).

Section 14

TRANSPARENCY, OVERSIGHT, ENFORCEMENT AND ACCOUNTABILITY

14.1 Transparency. HIO shall develop, implement and conduct measures to provide Provider Participants information concerning the ongoing operations of the System and the Services, including, without limitation, the efficiency, effectiveness, and security thereof, and the uses and disclosures of Patient Data made by and among Provider Participants pursuant to their use thereof, as described in the Policies and Procedures. Such measures shall include HIO's provision to Provider Participants of the reports described in Section 8.2.3 (Reports to Provider Participants).

14.2 Oversight. The HIO will prepare periodic reports to Provider Participants concerning the ongoing operations of the System and the Services, including without limitation information regarding the efficiency, effectiveness, and security thereof, and the accesses to and uses and disclosures of Patient Data made by and among Provider Participants pursuant to their use thereof, including without limitation Provider Participants' adherence to the Provider Participant Terms and Conditions and/or Policies and Procedures regarding the privacy and security of Patient Data.

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

EXHIBIT "B"

HIE POLICIES AND PROCEDURES

TO BE ATTACHED

EXHIBIT "C"

BUSINESS ASSOCIATE AGREEMENT Central Coast Health Connect LLC, a California limited liability company ("Business Associate"), and the Provider Participant identified on the Signature Page hereof ("Covered Entity"), hereby agree to the following terms and conditions of this Business Associate Agreement (the "Business Associate Agreement").

RECITALS

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

AGREEMENT

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

1. Definitions. For the purposes of this Business Associate Agreement, the term "HIPAA" means the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. Parts 160, 162 and 164), as in effect from time to time. All terms used in this Business Associate Agreement not specifically defined otherwise shall have the same definitions as given to them under HIPAA; provided, however, that the term "PHI" shall refer only to protected health information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity.
 - (a) "Breach" shall have the same meaning as "breach" as defined in 45 C.F.R. § 164.402 and shall mean the access, acquisition, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the privacy or security of the PHI; the term "breach" as used in this Business Associate Agreement shall also mean the unlawful or unauthorized access to, use or disclosure of a patient's "medical information" as defined under Cal. Civil Code § 56.05(j), for which notification is required pursuant to Cal. Health & Safety Code 1280.15.

(b) "Services" shall mean the services for or functions on behalf of Covered Entity performed by Business Associate pursuant to the Provider Participation Agreement between Covered Entity and Business Associate to which this Addendum applies.

2. Obligations of Business Associate.

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

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

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

- (i) For the proper management and administration of Business Associate [Reference: 45 C.F.R. § 164.504(e)(2)(i)(A) & 45 C.F.R. § 164.504(e)(4)(i)(A)].
- (ii) To carry out the legal *responsibilities* of Business Associate [Reference: 45 C.F.R. § 164.504(e)(4)(i)(B)].
- (iii) To provide data aggregation services relating to the health care operations of Covered Entity if and to the extent *provided* by the Provider Participation Agreement; provided that Business Associate shall not de-identify PHI except as permitted by the Terms and Conditions. [Reference: 45 C.F.R. § 164.504(e)(2)(i)(B)].

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

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

C.F.R. § 164.504(e)(4)(i)(B)] if:

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

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

(f) Reporting Unauthorized Uses and Disclosures. Business Associate shall report to Covered Entity, without unreasonable delay, and in no cases later than one (1) business day from discovery of the breach, any use or disclosure of PHI not permitted by this Business Associate Agreement of which Business Associate becomes aware, including without limitation any security incident involving electronic PHI and any breach of unsecured PHI as required by 45 C.F.R. § 164.410 [*Reference: 45 C.F.R. §§ 164.314(a)(2)(C) & 164.504(e)(2)(ii)(C)*]. Without limiting the generality of the foregoing:

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

denial of service and any combination of the above. Business Associate shall investigate each Security Incident or non-permitted access, use, or disclosure of PHI that it discovers and shall provide a summary of its investigation to Covered Entity, upon request. If Business Associate or Covered Entity determines that such Security Incident or non-permitted access, use, or disclosure constitutes a Breach, then Business Associate shall comply with the requirements of Section 2.(f)(ii) below.

(ii) Except in the event of a law enforcement delay, Business Associate shall report the information described below to Covered Entity without unreasonable delay, and in no case more than one (1) business day following discovery of a breach of unsecured PHI. Such notice shall include, to the extent possible:

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

(B) The date of the breach;

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

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

(E) Any other details necessary to complete an assessment of the risk that the PHI has been compromised. [*Reference: 45 C.F.R. §§ 164.410 & 164.404(c).*]

(iv) Business Associate shall, in consultation with the Covered Entity, mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper access, use, or disclosure, Security Incident, or Breach and in accordance with the CCHC Security & Privacy Policies and Procedures.

(v) Business Associate shall take prompt corrective action, including any action required by applicable state or federal laws and regulations relating to such Security Incident or non-permitted access, use, or disclosure and in accordance with the CCHC Security & Privacy Policies and Procedures,.

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

this Business Associate Agreement, and pursuant to which Business Associate shall obtain satisfactory assurances that the subcontractor shall appropriately safeguard that PHI [References: 45 C.F.R. § 164.308(b)(2), 45 C.F.R. § 164.314(a)(2)(i)(B) & 45 C.F.R. § 164.504(e)(2)(ii)(D)].

(h) Individuals' Access to PHI. If and to the extent that Business Associate maintains PHI in a designated record set, Business Associate shall upon request by Covered Entity make that PHI available to Covered Entity within ten (10) business days as and to the extent required for Covered Entity's compliance with its obligations to provide individuals with access to and copies of PHI pursuant to 45 C.F.R. § 164.524. If Business Associate receives an individual's request for access to PHI, Business Associate shall forward that request to Covered Entity within five (5) business days. Covered Entity shall be responsible for making all determinations regarding the granting or denial of an individual's request, and for notifying individuals thereof, and Business Associate shall not make any such determinations or notifications [Reference: 45 C.F.R. §§ 164.502(a)(4)(ii) & 164.504(e)(2)(ii)(E)].

(i) Amendments to PHI. If and to the extent that Business Associate maintains PHI in a designated record set, Business Associate shall upon request by Covered Entity make that PHI available to Covered Entity within ten (10) business days for amendment, and shall promptly incorporate any amendments to PHI directed by Covered Entity, as and to the extent required for Covered Entity's compliance with 45 C.F.R. § 164.526. If Business Associate receives an individual's request for an amendment to PHI, Business Associate shall forward that request to Covered Entity within five (5) business days. Covered Entity shall be responsible for making all determinations regarding the granting or denial of an individual's request, and for notifying individuals thereof, and Business Associate shall not make any such determinations or make any such amendments except as directed by Covered Entity [Reference: 45 C.F.R. § 164.504(e)(2)(ii)(F)].

(j) Accountings of Disclosures. Business Associate shall document disclosures of PHI as required to provide Covered Entity with information sufficient to respond to any request by an individual for an accounting of disclosures in compliance with 45 C.F.R. § 164.528, and shall provide such information to Covered Entity upon request within ten (10) business days. If Business Associate receives an individual's request for an accounting of disclosures, Business Associate shall forward that request to Covered Entity within five (5) business days. Covered Entity shall be responsible for providing all accountings of disclosures to individuals, and Business Associate shall not provide any such accountings to individuals directly [Reference: 45 C.F.R. § 164.504(e)(2)(ii)(G)].

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

(l) Books and Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the U.S. Secretary of Health & Human Services for purposes of determining Covered Entity's or Business Associate's

compliance under HIPAA [*Reference: 45 C.F.R. § 164.504(e)(2)(ii)(I)*]. Without limiting the generality of the foregoing, Business Associate shall disclose PHI when required by the U.S. Secretary of Health & Human Services under Subpart C of 45 C.F.R. Part 160 to investigate or determine Business Associate's compliance with HIPAA [*Reference: 45 C.F.R. § 164.502(a)(4)(i)*]. Business Associate shall promptly make available to Covered Entity such books, records, or other information relating to the use and disclosure of PHI for purposes of determining whether Business Associate has complied with this Business Associate Agreement or maintains adequate security safeguards, upon reasonable request by Covered Entity.

(m) Business Associate acknowledges that, as between the Business Associate and the Covered Entity, all PHI shall be and remain the sole property of the Covered Entity.

(n) Business Associate further acknowledges that it is obligated by law to comply, and represents and warrants that it shall comply, with HIPAA and the HITECH Act. Business Associate shall comply with all applicable state privacy and security laws, to the extent that such state laws are not preempted by HIPAA or the HITECH Act.

3. Covered Entity's Obligations.

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

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

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

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

4. Term and Termination.

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

(b) Termination. If Covered Entity knows of a pattern of activity or practice by Business Associate that constitutes a material breach or violation of Business Associate's obligations under HIPAA or this Business Associate Agreement, Covered Entity may (i)

immediately terminate this Business Associate Agreement and the Provider Participation if breach is incurable; or (ii) terminate this Business Associate Agreement and the Provider Participation Agreement, if feasible, subject to and in accordance with the terms and conditions of Section 3.4 of the Provider Participation Agreement after providing notice to Business Associate and a reasonable opportunity to cure the breach. [*Reference: 45 C.F.R. §§ 164.504(e)(1)(ii) & 164.504(e)(2)(iii)*].

(c) Breach Pattern of Practice by Covered Entity. If Business Associate knows of a pattern of activity or practice by Covered Entity that constitutes a material breach or a violation of Covered Entity's obligations under HIPAA or this Business Associate Agreement, Business Associate may (i) immediately terminate this Business Associate Agreement and the Provider Participation if breach is incurable; or (ii) terminate this Business Associate and the Provider Participation Agreement, if feasible, subject to and in accordance with the terms and conditions of Section 3.4 of the Provider Participation Agreement, after providing notice to Business Associate and a reasonable opportunity to cure the breach.

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

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

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

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

8. No Third Party Beneficiaries. Unless otherwise set forth herein, nothing contained herein

is intended nor shall be construed to create rights running to the benefit of third parties.

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

10. Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 4.d., 11, and 12 shall survive termination of this Addendum until such time as the PHI is returned to Covered Entity or destroyed.

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

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

IN WITNESS WHEREOF, Covered Entity and Business Associate have entered into this Agreement as of the Effective Date of the Provider Participation Agreement.

“Covered Entity”

County of Monterey

By: *Elisa Dimened* 09/27/2016
Name: *Elisa Dimened*
Title: *Director of Health*

“Business Associate”

Central Coast Health Connect LLC

By: *Elizabeth A. Lorenzi*
Name: *Elizabeth Lorenzi*
Title: *VP/CO*

RISK MANAGEMENT
COUNTY OF MONTEREY
APPROVED AS TO INDEMNITY/
INSURANCE LANGUAGE

By: *[Signature]*
Date: *8/23/16*

Reviewed as to fiscal provisions

[Signature]
Auditor/Controller
County of Monterey 8-23-16

EXHIBIT "D"

FEE SCHEDULE

Provider Participant shall have no obligation to pay any Service Fees or other fees described in Section 13 of the Terms and Conditions.

Notwithstanding the foregoing or anything else to the contrary contained in this Agreement, this Exhibit "D" may be amended upon the mutual written agreement of the parties to provide for a Service Fee or other fee or charge upon Provider Participant ("Fee Amendment"), to be effective at least thirty (30) calendar days' following such amendment, which effective date must be the first (1st) day of an upcoming month. Following the request by CCHC for a Fee Amendment, if Provider Participant does not agree to such Fee Amendment, Provider Participant may terminate this Agreement by providing CCHC with written notice of termination no later than twenty (20) calendar days following the date on which a request for a Fee Amendment is given by CCHC and the Fee Amendment shall not be effective.

8/19/16

ROUTING FORM – RQN #: 4000-2422-1 **Date:** 8/16/16

AGREEMENT **AMENDMENT** **BOARD REPORT FOR PRE-APPROVAL**

Vendor Name: CENTRAL COAST HEALTH CONNECT, LLC. (CCHC)

Title/Brief Description of Document: Participant Agreement with Monterey County Health Department for Participation in CCHC's Health Information Exchange. Term of September 15, 2016 – June 30, 2018. BOARD REPORT included for BOS Pre-Approval

Originating Dept.: 4000 - 8096 **Dept. Contact WITH Phone #:** SHEENA MORALES X1393

This Agreement or Amendment requires Board Approval: Yes No

This Agreement requires an MYA: Yes No

AGREEMENT TYPE

<input type="checkbox"/>	RQNSA – Standard Agreement	<input checked="" type="checkbox"/>	RQNNS – Non-Standard Agreement
<input type="checkbox"/>	RQNIT – ITD Standard Agreement	<input type="checkbox"/>	RQNIN – ITD Non-Standard Agreement
<input type="checkbox"/>	RQNPB – Pre-Board Standard Agreement	<input type="checkbox"/>	Non-Standard Board Agreement (Not to be tracked within RQN)
<input checked="" type="checkbox"/>	Insurance & Endorsement Current	<input checked="" type="checkbox"/>	VDR & Non-Resident State Forms Verified

ROUTING AND APPROVALS*

Each Approving Authority is requested to forward the Service Contract to the next Approving Authority in the order listed herein. Thank you.

	Approving Authority:	Approval Initials	Comments:	Date Reviewed
1st	ITD(for all ITD related contracts)		N/A	
2nd	County Counsel (required)	<i>SO</i>		8/19/2016
3rd	Risk Management (non-standard insurance and/or indemnity provisions)	<i>SM</i>	CONFIRM RISK TERMS	8/23/16
4th	Auditor-Controller (required)	<i>MS</i>	Please call PRISCA SEGOVIA 755-4939 when ready to pickup. DO NOT INTEROFFICE	8-22-16
5th	Contracts/Purchasing (required)	<i>JS</i>	INITIALED FOR ROUTING	8-24-16
	Return to Originating Department Instructions		Sheena Morales x 1393	

* In the event that one of the approving authorities has an issue with the document and will not sign, the document shall be returned immediately to the originating department's key contact person identified herein along with a brief written explanation regarding the issue. Once that issue is corrected, the originating department shall restart the routing process again from the beginning by resubmitting the document through the approval process. The original Routing Form should be included for reference.

MYA #: *



2016

Central Coast Health Connect

Security & Privacy Policy and Procedure Manual

Contents

Definitions Policy #1 4

Security & Privacy Officer Policy #2 14

HIE Portal Access Policy #3 16

HIE Portal Access Monitoring and Adherence Policy #4 19

HIE Downtime Policy #5 21

HIE Security Monitoring & Reminders Policy #6 23

HelpDesk Support Policy #7 25

Individual Authorization Policy #8 28

Restrictions by Individual Policy #9 30

Policy Revisions and Maintenance Policy #10 32

Maintaining Confidentiality Policy #11 35

Confidentiality Agreement Form for Workforce Policy #12 37

Personally Identifiable Information (PII) Policy #13 39

Uses and Disclosure Policy #14 41

Workforce and User Training Policy #15 43

De-Identification of PHI Policy #16 45

Disposal of PHI Policy #17 47

Certification Form for Disposal of PHI Policy #18 50

Malicious Software, Virus and Other Threats Policy #19 52

Disaster Recovery and Data Back-Up Plan Policy #20 54

Sanction Policy #21 56

Complaint Resolution Policy #22 58

Response to Breach and Security Incidents Policy #23 60

Firewall Policy #24 73

Auto Release of Clinical Results Policy # 25 75

Minimum Necessary Policy #26 77

Opt-Out Policy #27 79

Sensitive Health Information Policy #28 84

Patient Consent and Permissible Uses Policy #29 87

Data Exchange Between HIO to HIO Policy #30.....	90
Data Exchange Between HIO to Data Participant Policy #31.....	93
Data Exchange Between HIO to Data Provider Policy #32	97
HIE Access Termination Policy #33	98
HIE Participation Agreement Policy #34	99
Amendment of PHI Policy #35	101
Patient Record Merge Policy #36.....	103
Security Management Policy #37	105
Facility Access Control Policy #38	107
Physical Safeguards Policy – Workstation Policy #39	109
Technical Safeguards – Access Control Policy #40.....	111
Contingency Plan Policy #41	112
Master Appendix Policy #42	113

Definitions Policy #1

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to maintain a master list of policy and procedure definitions as reference for CCHC related documents.

PROCEDURE

- I. CCHC Workforce designee will routinely maintain master definition list and update as directed.

DEFINITIONS

Access	Means to cause data (i.e., Patient Information) to be viewed by an Authorized User, such as by transferring that data from one computer to another and/or by causing that data to be displayed (e.g., an Authorized User will “Access” Patient Information through the CCHC HIE); or the ability to cause data to be transferred and/or viewed as described above (e.g., a Data User will have “Access” to Patient Information through the CCHC HIE).
Administrative Safeguards	Means administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security and privacy measures to protect PHI and to manage the conduct of Users in relation to the protection of PHI. Administrative safeguards include but not limited to policies and procedures, risk management plans and workforce training.
Authentication Information	Means the method of authentication assigned to each Authorized User of CCHC by his or her Participating Organization in accordance with minimum CCHC requirements. Authentication may be based upon information known only by and unique to an Authorized User, such as a password and username.
Authorized User	Means an individual Participant or an individual designated to use CCHC HIE services on behalf of the Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant’s medical staff and/or their designated agent.

Definitions Policy #1

Breach	“Breach” shall have the same meaning as “breach” as defined in 45 C.F.R. § 164.402 and shall mean the access, acquisition, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the privacy or security of the PHI; the term “breach” as used in this Business Associate Agreement shall also mean the unlawful or unauthorized access to, use or disclosure of a patient’s “medical information” as defined under Cal. Civil Code § 56.05(j), for which notification is required pursuant to Cal. Health & Safety Code 1280.15.
Business Associate	Means a person or entity that performs a function, activity, or service to a Health Care Provider, Health Plan, Health Care Clearinghouse, or another Business Associate involving the disclosure of Protected Health Information (PHI) or Personal Demographic Information to the Business Associate. CCHC is a Business Associate to each of its Participating Organizations. Subcontractors and vendors to CCHC may be Business Associates of the CCHC.
Business Associate Agreement	Means a contract between a Covered Entity under HIPAA and a Business Associate, or between a pair of Business Associates, which obligates the Business Associate to maintain the privacy and security of Protected Health Information in accordance with the requirements of 45 C.F.R. Part 164.
Clinical Messaging	Means the exchange of Protected Health Information from one Participating Organization to another through CCHC in the form of test results or other clinical information. Test results can be generated by clinical laboratories, imaging providers, and other like providers. Other clinical information may consist of discharge summaries, consultation reports, and Patient referral data.
California Confidentiality of Medical Information Act (CMIA)	Means the California Civil Code that regulates the privacy of medical information (Cal. Civ. Code §§ 56-56.37).
Consent	Means the decision of a Patient to participate in CCHC Health Information Exchange. No affirmative action is required from a Patient to establish his or her consent. A Patient shall be deemed to have given his or her consent to participate until and unless the Patient affirmatively Opts-Out of the Health Information Exchange.
Covered Entity	Means a Health Care Provider, Health Care Clearinghouse, or a Health Plan that

Definitions Policy #1

	transmits any Protected Health Information in electronic form. A Covered Entity shall have the same meaning as such term is defined in 45 C.F.R. Part 160.
Data Provider	Means any Participant that CCHC designates as a Data Provider that is registered to provide information to CCHC HIE for use through the Services.
Data Recipient	Means a Participant that uses the Services of CCHC HIE to obtain health information.
De-identify or De-identification	Means the process of rendering Protected Health Information (PHI) into a form that does not identify a Patient, and there is no reasonable basis to believe that the information can be used to identify a Patient. In order to De-identify PHI properly, the requirements of 45 C.F.R. Part 164 shall be followed.
Dependent Account	Means a patient portal account, that is connected to an existing master or primary account, typically used for parents to view their children's health data.
Drug or Alcohol Abuse Information	Means information related to the Treatment and care of a Patient suffering from alcohol or drug abuse, or both, including any information that would specifically identify a Patient as receiving Drug or Alcohol Abuse Treatment and care. Drug or Alcohol Abuse Information shall have the same meaning as the term "Drug or Alcohol Abuse Patient records" is defined in 45 C.F.R. Part 2.
Encryption	Means a technology or methodology approved by the United States Secretary of Health and Human Services that can render Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals or entities.
E-Prescribing	Means the transmission, using electronic media, of prescription or prescription-related information between a Licensed Practitioner and a pharmacy, pharmacy benefit manager, or Health Plan, including any communication related to that prescription.
Health Care Operations	Means any of those activities identified by federal regulations at 45 C.F.R. Part 164, as may be amended, including but not limited to, quality assessment and improvement activities, case management and care coordination, reviewing the competence of Licensed Practitioners, underwriting, and business planning and management activities.

Definitions Policy #1

Health Information Exchange (HIE)	Means the Internet-based, brokered, peer-to-peer technology health information exchange platform and advanced clinical search engine that resides on servers operated by CCHC and provides electronic transfer of Protected Health Information between Participating Organizations for a permissible purpose based upon the requirements of Federal and State law.
Health Care Provider	Means a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Health care provider shall have the same meaning as such term is defined in 45 C.F.R. Part 160.
Health Information Exchange (HIE) Participation Agreement	Means a written agreement between CCHC and a Participating Organization, pursuant to which that Participant agrees to act as a Data Provider and/or a Data User and abide by all defined CCHC policies, procedures and applicable Federal and State laws. HIE Participation Agreement will also be referenced within the Policy and Procedures as HIE Participation Agreement with applicable Terms and Conditions. Terms and Conditions is an exhibit attached to the HIE Participation Agreement.
Health Information Organization (HIO)	Means a multi-stakeholder organization created to facilitate health information sharing and aggregation for treatment, payment, operations, public health and other lawful purposes.
Health Plan	Means an individual or group plan that provides, or pays the cost of medical or health services and shall have the same meaning as such term is defined in 45 C.F.R. Part 160.
Health Insurance Portability and Accountability Act (HIPAA)	Means the Health Insurance Portability and Accountability Act of 1996 and its implementing rules promulgated in 45 C.F.R. Parts 160, 162, and 164.
HIPAA Privacy Rules	Means those privacy rules described in 45 C.F.R. Part 164, Subpart E, as modified and enlarged by the Health Information Technology for Economic and Clinical Health (HITECH) Act and any other subsequent amendments.

Definitions Policy #1

HIPAA Rules	Means the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information [45 C.F.R. Parts 160 and 164] promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (“HIPAA”) of 1996, and the applicable privacy and security provisions of the American Recovery and Reinvestment Act (42 U.S.C. § 17931(a) et. seq.
HIPAA Security Rules	Means those security rules described in 45 C.F.R. Part 164, Subpart C, as modified and enlarged by the HITECH Act and any other subsequent amendments.
Health Information Technology for Economic and Clinical Health) HITECH Act	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).
Inquiry	Means a request directed by a contracted Participating Organization to CCHC for the disclosure of a Patient’s Protected Health Information for a permissible purpose.
Master Patient Index	Means the index wherein Personal Demographic Information of Patients is securely maintained by CCHC to record their decision to Opt-Out of the Health Information Exchange. For those Patients who have not elected to Opt-Out, the Master Patient Index shall be used to match such Patients with any inquiries seeking the exchange of PHI for a permissible purpose. CCHC shall maintain Personal Demographic Information regarding all potential Patients in this Master Patient Index, even if the decision is made to Opt-Out, in order to minimize the possibility of improperly matching Patients.
Mental Health Information	Means any information obtained in the course of Treatment or evaluation of any Patient suffering from a mental or behavioral disorder, including but not limited to, diagnosis and Treatment information, and any information that would specifically identify a Patient as receiving mental health services.
Minimum Necessary	Means that when requesting, using, or disclosing Protected Health Information for a permissible purpose other than Treatment or Emergency Treatment, a Covered Entity or a Business Associate shall limit Protected Health Information to the minimum amount needed to accomplish the intended purpose of the request, use, or disclosure. Minimum Necessary shall have the same meaning as such term is defined in 45 C.F.R. Part 164, Subpart E.

Definitions Policy #1

Opt-Out	Means a process under which any Patient may elect to not want to consent to the use and disclosure of his/her Protected Health Information with other Participating Organizations in the CCHC HIE.
Participant	Means an individual person or organization that is currently a party to a Participation Agreement with CCHC. When there is a policy reference to Participating Organizations (POs), it implies inclusion, as applicable to Hospitals, Physicians and Practice Staff.
Participant's System	Means the hardware and software controlled by the Participant through which the Participant conducts its health information exchange related activities.
Participant Type	Means the category(ies) of Participant to which a particular Participant is assigned by CCHC and is based upon that Participant's role in the health care system.
Patient	Means the individual whose Personal Demographic Information or Protected Health Information is subject to electronic storage and transfer by the HIE.
Patient Data	Means patient information (including but not limited to "Protected Health information" as defined in HIPAA or "Medical Information" as defined in the CMIA, or Personal Information as defined in Civil Code 1798.28, 1798.82) provided, or made available for exchange, by a Data Provider through CCHC.
Patient Notice	Means a written notice prepared and supplied to its Participating Organizations for distribution to Patients or written by Participating Organization's (and pre-reviewed by CCHC). Participating Organization may provide the Patient with an electronic version of the Patient Notice if the Patient has specifically agreed to electronic notice as permitted by the HIPAA Privacy Rules; provided that the Patient retains the right to obtain a paper copy of the Patient Notice from the Participating Organization upon request. This Patient Notice shall explain the function of CCHC; the permissible purposes for which a Patient's Protected Health Information may be shared with other Participating Organizations through the CCHC; and the types of Protected Health Information which may be shared or need authorization before sharing with other Participating Organizations (such as Sensitive Health Information).

Definitions Policy #1

Patient Information	Means all information relating to a patient that a Data Provider makes available so that Data Users may access that information through the Program.
Personal Health Record (PHR)	Means a health record that is registered by a Patient with CCHC on his or her own behalf, and utilizes an online platform sponsored by another organization. This personal health record may be developed by gathering and consolidating Protected Health Information from many sources, including Participating Organizations of CCHC HIE.
Physical Safeguards	Means the physical measures, policies, and procedures to protect the Network and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
Policies and Procedures	Means the policies and procedures adopted by CCHC using approved processes for the operation, terms and conditions to use the system and services including without limitation any operations manual, privacy and security policies, and technical specifications.
Prerequisite System	Means the technology within the Participant's firewall necessary for the Participant to access and use CCHC HIE.
Privacy Event	Means an incident that adversely affects (i) the visibility of HIO; (ii) the trust among Participants; or (iii) the legal liability of HIO or any Participant.
Privacy Officer	Means the individual named in the CCHC Privacy Officer Policy.
Program	Means any one or more programs of electronic health information exchange operated by CCHC in which a Participant agrees to participate pursuant to its HIE Participation Agreement.
Protected Health Information (PHI)	Means any information that relates to the past, present, or future physical or mental health or condition of a Patient, the provision of health care items or services to the Patient, and the past, present, or future Payment for the provision of health care items or services to a Patient. Protected Health Information also must personally identify a Patient or provide a reasonable basis to believe that the information can

Definitions Policy #1

	<p>be used to identify a Patient. Protected Health Information shall have the same meaning as such term is defined in 45 C.F.R. Part 160. HIPAA considers the following personal identifiers PHI:</p> <ul style="list-style-type: none"> A. Name B. All geographic subdivisions smaller than state of residence C. All elements of dates (except year) for dates directly related to an individual, including birth date; and all ages over 89 and all elements of dates (including year indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older D. Telephone number E. Fax number F. Electronic mail addresses G. Social security number H. Record number I. Health plan beneficiary number J. Account number K. Certificate/license number L. Vehicle identification numbers such as serial and license numbers M. Device identifiers and serial number N. Web Universal Resource Locators (URLs) O. Internet Protocol (IP) address numbers P. Biometric identifiers, including finger and voice prints Q. Full Face photographic image R. Any other unique identifier, identifying number, characteristic, or code.
Public Health Reporting	Means the exchange of Protected Health Information through CCHC HIE to a Federal or State agency for the reporting and surveillance of specified health conditions as required by law, and for the reporting of immunization data. Such reporting shall contain the minimum amount of Protected Health Information or Personal Demographic Information as is required by law.
Psychotherapy Notes	Means notes recorded by a mental Health Care Provider documenting or analyzing the contents of a conversation by a Patient during a private, group, or family counseling session, and that are separated from the rest of the Patient's medical record. Psychotherapy notes shall have the same meaning as such term is defined in 45 C.F.R. Part 164.
Security Incident	Means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations.
Sensitive Health	Means the subset of Protected Health Information involving Drug or Alcohol Abuse

Definitions Policy #1

Information (SHI)	Information, Mental Health Information, Psychotherapy Notes, Out-Of Pocket Goods and Services, any PHI subject to a disclosure restriction requested by a Patient and agreed to by a Participating Organization, or any other goods and services subject to heightened privacy and confidentiality requirements under Federal and State laws or regulations and specifically approved by CCHC.
Services	Means the health information exchange and related services provided by CCHC as described in the HIE Participation Agreement.
System	Means the HIE System that is provided by CCHC and made accessible to Participants through their contract with HIE Vendor and their Member Participation Agreement with HIO.
Technical Safeguards	Means the technology and the policy and procedures CCHC has in place to protect PHI and control access to it.
Treatment	Means the provision of health care items or services to a Patient, including direct Patient care as well as consultation, coordination, management, or Patient referral between or from one Participating Organization to another. Treatment shall have the same meaning as such term is defined in 45 C.F.R. Part 164.
Unsecured Protected Health Information or Unsecured PHI	Means Protected Health Information that has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of Encryption or other federally-approved technology or methodology specified by the Secretary of the U.S. Department of Health & Human Services (HHS) through guidance issued pursuant to HITECH. Unsecured Protected Health Information shall have the same meaning as such term is defined in 45 C.F.R. Part 164.
Unsuccessful Security Incident	Means a security incident (as defined under HIPAA) that does not result in (1) the unauthorized access, use disclosure, modification or destruction of information, or (2) material interference with system operations in a party's information system, including, without limitation, activity such as ping and other broadcast attacks on that party's firewall, port scans, unsuccessful log-on attempts, denial of service and/or any combination of the foregoing, as long as no such incident results in unauthorized access, use or disclosure of electronic protected health information.
Use	Means with respect to individually identifiable information/data and as permitted under the HIE Participation Agreement and has the same meaning as defined in 45

Definitions Policy #1

	C.F.R. § 160.103.
Workforce	Defined as employees, contractors, volunteers, trainees, or other individuals performing work for CCHC, and is under the direct control of CCHC whether or not they are paid. Workforce shall have the same meaning as such term is defined in 45 C.F.R. Part 160.
Workstation	Means an electronic computing device, for example a desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

RESOURCES

Security & Privacy Officer Policy #2

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to identify the individual(s) responsible for providing oversight and monitoring adherence to Central Coast Health Connect's (CCHC) security and privacy policies.

PROCEDURE

- I. CCHC shall designate a CCHC Security & Privacy Officer (SPO).

- II. The CCHC Security & Privacy Officer will oversee CCHC's Privacy and Security Program, including:
 - a. Developing and implementing privacy and security policies, in accordance with federal and California privacy and security requirements.
 - b. Overseeing that all Participants of the Workforce, Participating Organizations, and Business Associates who come into contact with protected health information (PHI) are properly trained.
 - c. Mitigating the effects of all disclosures that are not compliant with federal or California law or that are contrary to CCHC's Privacy Policies and Procedures.
 - d. Conducting, at least annually, a review of CCHC's provider and patient portal access procedures.
 - e. Guiding and assisting in the identification, implementation, and maintenance of privacy and security policies and procedures in coordination with CCHC's management/Executive Sponsors, CCHC Participants and legal counsel.
 - f. Reviewing all system-related information security plans in order to align security and privacy practices.
 - g. Performing initial and periodic security risk assessments and "privacy audits" and conducting ongoing compliance monitoring activities.
 - h. Complying with HIPAA, HITECH and California law on disposal of PHI.
 - i. Communicating any breach or security concerns to the applicable Privacy Officer of each Participant Organization.

- III. This list is an overview of the CCHC Security & Privacy Officer roles and responsibilities and is not meant to serve as an all-inclusive duties list.

Security & Privacy Officer Policy #2

RESOURCES

HIE Portal Access Policy #3

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to limit the potential for CCHC HIE misuse and promote patient confidentiality by only displaying the minimum functionality and information needed by the user. Access is restricted to users needing to utilize the system to fulfill their job requirements and the access authorized restricts the user from functions and information that is not needed.

This policy also provides assurance that users have received appropriate training, education and knowledge necessary to utilize CCHC HIE functions competently and professionally before access is given. All Workforce members receiving access will be further instructed in patient confidentiality, system misuse and abuse and the consequences of violations.

Additionally, the purpose of this policy is to outline the types of patient portal accounts that CCHC allows and how patients can create connections within the HIE software to view his/her medical data.

PROCEDURE

- I. Participating Organizations, Provider/Office Staff and Workforce users are responsible for ensuring pre-training is completed and attested prior to accessing CCHC HIE.
 1. RelayHealth provides an online suite of training tutorials on basic HIE functionality.
 2. All Workforce training will include patient confidentiality, and system misuse and abuse information as well as its consequences.
 3. All Participating Organizations will also ensure adherence to internal HIPAA required training per internal organization policy

- II. Patient Portal Access
 1. Patient Portal user access is restricted to use for individuals 18 years or older and does not allow for any dependent account creation.
 2. Patient Portal user invite must come directly from a Provider/Physician/Hospital. Once the user receives the Patient Portal invite, they will click the link which directs them to the Registration page.
 3. Access to CCHC HIE will be by a two-level sign-on code. The first level, a User ID, will be assigned; however the user can change this to the User's email address; the second-level will be a user selected password.

HIE Portal Access Policy #3

- a. The password will contain a minimum of eight characters and enforced for strong complex password creation logic assurance.
 - b. Keyword Dictionary system logic will aid in prevention of password with common words.
 - c. The user will be locked out after five incorrect sign-in attempts and the account will be deactivated. The user will be directed to contact RelayHealth's support to unlock their account.
 - d. Three security questions and user-specific answers will be identified. These security questions aid in user verification for password reset.
 4. Users are required to attest to review of RelayHealth's Legal Notices, which include:
 - a. Subscriber Terms of Use
 - b. Privacy Policy
 5. All support requests for Patient Portal access is provided directly by RelayHealth's HelpDesk team.
 6. Deactivation process is defined in the Termination Policy.
- III. Physician/Provider Account Access
1. CCHC's Workforce is responsible for completing and sending the applicable Practice access request form to RelayHealth Deployment Specialist for initial activation.
 - a. Coverage Group Impact (CGI) Activation Sheet – is used to add new Provider/Office Staff into the system.
 - b. RDS Activation Sheet – is used to activate Provider for results.
 2. Once activation is confirmed, CCHC's Workforce will notify user by email of their User ID and temporary password and instructions to set permanent password.
 3. Deactivation process is defined in the Termination Policy.
- IV. Participating Organization's Staff Account Access
1. Participating Organizations must request staff account access in writing – email is preferred.
 2. Prior to CCHC Workforce creating and providing that staff account, the Participating Organization must attest in writing that the specified staff members have been trained to use the RelayHealth provider portal. Provider portal training modules are available on the RelayHealth portal – see Policy 42 for links to applicable training modules.
 3. CCHC Workforce is responsible for associating the staff account with the appropriate practice/organization access.
 - a. Note that for a staff account to receive “merge” access, he/she must obtain in-person training from CCHC Workforce. See CCHC Policy # 36 – Patient Record Merge.
- V. Workforce Access
1. CCHC's Workforce is responsible for completing the appropriate user pre-registration access request form and once completed, responsible for sending to RelayHealth for initial activation or CCHC Workforce with Administrative access may set-up User ID and temporary password.
 - a. CGI Activation Sheet – is used to add new Workforce member into the system.

HIE Portal Access Policy #3

2. Once activation is confirmed, CCHC's Workforce will notify user by email of their User ID and temporary password and instructions to set permanent password.
3. Deactivation process is defined in the Termination Policy.

RESOURCES

- Reference - Maintaining Confidentiality Policy
- Reference - Minimum Necessary Policy
- Reference - Workforce and User Training Policy
- Reference - Disciplinary Action of Workforce Policy
- Reference - Termination Policy
- Appendix Reference - RelayHealth Legal Notices

HIE Portal Access Monitoring and Adherence Policy #4

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to prevent unauthorized use and disclosure of Protected Health Information (PHI) via the CCHC HIE portal and to comply with federal and state laws as well as regulations associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and California Confidentiality of Medical Information Act (CMIA).

POLICY DETAILS

This policy applies to all Authorized Users, Participating Organizations, as well as Workforce members, and contracted Business Associates.

PROCEDURE

- I. Proper access and use of PHI is required and thus audits of access and use may be performed to hold the users of the CCHC HIE accountable for their actions.
 - a. These audit requests shall be assisted by participating organizations and will:
 - i. Ensure access to and utilization of PHI in the CCHC HIE is appropriate,
 - ii. Identify inappropriate access and/or utilization,
 - iii. Facilitate monitoring of compliance with CCHC HIE organizational policy and procedures,
 - iv. Identify security breach incidents, and
 - v. Ensure preservation of any content changes to a record.
- II. CCHC's Security and Privacy Officer or designee in concert with audit frequency parameters set by CCHC's governance shall review RelayHealth's provided reports to assess system activity as well as perform an auditing review of the following but not limited to:
 - a. Security Levels – ensure Users with “full administrative access” are limited to need and function.
 - b. Inactive Accounts over 90 Days – review Users who have not logged into the system in the past 90 days to access needs.
 - c. Users Who Have Never Logged On – review Users who have never logged on to the HIE and consider revocation.
 - d. Terminated Employees - confirm User access termination due to Workforce/User engagement ending.
- III. Audits for Monitoring of Participant Organization and User Activity

HIE Portal Access Monitoring and Adherence Policy #4

- a. CCHC may conduct audits of its Participating Organizations' Users to ensure compliance for Opt-Out procedural documentation and associated system change management.

RESOURCES

- Reference - 45 C.F.R § 164.308(a)(1)

HIE Downtime Policy #5

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to assure timely and accurate notification of system scheduled and unscheduled downtime in order to maintain acceptable support levels for users of CCHC HIE. Proper notification of scheduled or unscheduled downtime of the CCHC HIE will be communicated by RelayHealth to CCHC assigned designees and Participating Organization pre-identified key liaison.

PROCEDURE

- I. Scheduled Downtime
 - a. Standard maintenance and system downtime to the CCHC HIE occurs on a weekly basis from 10pm – 2am PST.
 - b. Notification of standing maintenance system downtime is provided during training and is part of standing Participating Organization HIE Participation Agreement.
 - c. End users will not be notified of the system downtime by email as it is routine.
 - d. CCHC Website will have a standard notification message disclaimer of schedule.

RelayHealth Standard Maintenance Window	
Day(s) of the Week	Tuesday
Time	10pm – 2am PST
Frequency	Weekly

- II. Unscheduled Downtime
 - a. CCHC HIE unscheduled maintenance downtime is rare; however, if there is an unscheduled downtime, RelayHealth’s Client Engagement team will contact the following groups by email as soon as unscheduled maintenance is to occur and email when the system is available (See Reference section for Downtime Notification Contact List details):
 - i. CCHC Assigned Designee/System Administrator
 - ii. Participating Organization Pre-identified Key Liaison(s)
 - b. End users will not be notified of the system unscheduled downtime by email.

HIE Downtime Policy #5

RESOURCES

- Reference – CCHC Downtime Notification Contact List (to be developed by CCHC)

HIE Security Monitoring & Reminders Policy #6

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is for CCHC's Security & Privacy Officer to maintain watchful security monitoring of its Technology Vendors, CCHC Workforce, Participating Organizations and Authorized Users to protect CCHC HIE's Protected Health Information (PHI) and maintain compliance with HIPAA Security Administrative Safeguards. Additionally, CCHC's Security & Privacy Officer or designee will periodically provide security awareness reminders to Authorized Users to aid in security safeguard continuity measures.

PROCEDURE

- I. CCHC's Security & Privacy Officer or designee will review minimally on an annual basis, its Technology Vendor's, RelayHealth's, Security Measures Notices and applicable tools, to include but not limited to:
 - a. Audit Trail
 - b. Role-Based Usage
 - c. Encryption
 - d. Data Security
 - e. Confidentiality
 - f. Login ID and Password
 - g. Auto-Logoff
 - h. Digital Certificates
 - i. Sensitive Information
 - j. Business Partners
 - k. Disaster Recovery
 - l. Data Integrity
- II. CCHC's Security & Privacy Officer or designee will periodically issue security information and awareness reminders to CCHC Workforce, Participating Organizations and Authorized Users.
 - a. The means by which such secure reminders will be sent are as follows, but not limited to:
 - i. Meetings;
 - ii. Email reminders;
 - iii. Log-on system messages via website; or
 - iv. Letters or Newsletters

HIE Security Monitoring & Reminders Policy #6

- b. Such security reminders may include the following topics, but not limited to:
 - i. Legal and business responsibilities of CCHC HIE for protecting PHI exchanged between Participating Organizations;
 - ii. Information regarding how to use CCHC HIE services in a manner that reduces security risks, such as tools or techniques to maintain physical computer security safeguards of CCHC HIE such as the use of computer privacy screens or workstation screensavers; and/or
 - iii. General information regarding security risks and how to follow CCHC's Privacy and Security policies and procedures.
- III. CCHC Security & Privacy Officer or designee will issue security notifications within a reasonable time upon any of the following events:
 - a. Implementation by its Technology Vendor of any new security mechanisms or tools;
 - b. Enactment of significant revisions to CCHC HIE's Security & Privacy Policies and Procedures; or
 - c. Detection of threats or risks identified against CCHC HIE's services.

RESOURCES

- Reference – 45 C.F.R. § 164.308
- Reference – 45 C.F.R. § 164.306
- Reference – California Civil Code 1798 § et seq.

HelpDesk Support Policy #7

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to assure consistent levels of support and issue resolution and to maintain customer satisfaction for users of the CCHC HIE system.

POLICY DETAILS

- I. CCHC HIE will be supported primarily by its technology vendor, RelayHealth, for User support related to subscription service and technical questions for the following types of issues and during normal business hours of 8:00 am through 5:00 pm PST, Monday thru Friday.
 - a. **Critical Support Issue.** Should RelayHealth's subscription services fail to function in accordance with published specifications and User is unable to proceed without a fix to the problem or a work-around solution.
 - b. **Major Support Issue without a workaround.** Should RelayHealth's subscription services contain major functional problems against published specifications where User has no reasonable work-around, critical functionality is limited with no reasonable work-around.
 - c. **Major Support Issue with a workaround.** Should RelayHealth's subscription services contain incorrect logic, incorrect descriptions, or functional problems which the User is able to work around or where a temporary correction has been implemented (fully functional but needs improvement).
 - d. **Minor Support Issue.** Should a User experience an issue with no major functional problems against its published specifications but may contain a typographical error or similar issue.
- II. Select after hours support is available and consists of a paging protocol. After hour calls are redirected to an answering service and issues are then triaged based on severity. Only if an after hour call is deemed "critical", will a technical representative be contacted and support provided. All other non-critical requests will be managed during standard business hours.
- III. RelayHealth will track and manage all issues through their internal issue tracking system.
- IV. RelayHealth will provide regular issue reporting to CCHC Workforce on open and closed issues.
- V. Per CCHC's Opt-Out Policy, Users of the Patient Portal service will submit any Opt-out related requests directly to the Participants designated support team. Effective Q3 2015, Opt-out support calls will be centralized via CCHC support by:
 - a. Phone at 831-644-7494
 - b. Email at cchc-help@centralcoasthealthconnect.org

HelpDesk Support Policy #7

PROCEDURE

- I. User Support will be managed by RelayHealth’s HelpDesk team during normal business hours (8:00 am to 5:00 pm PST, Monday thru Friday), and Users can open a support case by phone at 866-735-2963 or email at support@relayhealth.com.
- II. RelayHealth defines support scope as outlined below.

Category	Definition	Examples
Customer Support	Issues with authentication, administration, and basic site navigation that can typically be addressed quickly with first call resolution.	Password resets Adding/removing users Basic application configuration Managing duplicate records Correcting patient merge errors
Technical Support	Issues with connectivity and transaction processing (HL7, CCD, CDA) or interface configuration.	Missing results/orders Failed transactions CSC connectivity
Production Support	Issues that result from a bug or defect in our application code resulting in the application behaving unexpectedly.	Unexpected application behaviour.
Production Incident	An incident that renders our applications and connectivity services unusable or inaccessible activating our “911” procedure.	Widespread loss of connectivity Application unavailable Mass transaction failures/delays
Provisioning Requests	Requests to add or remove providers or practices to or from any existing live interface.	RDS activation requests Interface re-configuration Interface decommissioning
Enhancements	Requests for new features or capabilities or changes to existing features that would improve the user or customer experience.	

- III. RelayHealth’s issue definition and response time goals are defined below.

Priority	Definition	Support Available	Resolution Goal
Critical	An incident that has an imminent impact on patient safety or renders the HIE applications and connectivity services unusable or inaccessible.	24x7	Less than 1 calendar day.
All Other	Issues that are impacting the ability for customers to use the HIE services and solutions as designed and documented.	8am – 5pm PST (M-F)	Less than 30 calendar days.

- IV. RelayHealth will provide routine reports to CCHC Designees and contracted Participating Organizations on open and closed issues status.

HelpDesk Support Policy #7

RESOURCES

- Reference - CCHC HIE Opt-Out Policy

Individual Authorization Policy #8

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure the methodology and validation protocols for determining which Individuals are authorized to access CCHC HIE and are compliant with HIPAA security safeguards for role-based access control (RBAC). This policy will identify how roles and functions of CCHC Workforce, Participating Organization authorized user or Individual (i.e., patient) are authorized to access CCHC HIE.

PROCEDURE

- I. CCHC will apply strict access safeguards to CCHC HIE with its Participating Organizations, Business Associates and Workforce through a verifiable and methodical process of designating approved individual Authorized Users based on roles and functions to access PHI.
- II. CCHC enforces role-based system architecture to grant access and security levels within CCHC HIE. Access rights are limited by role and functions. Examples of CCHC HIE role-based levels, but not all inclusive, include the following:
 - a. Practice Level
 - b. Provider Level
 - c. Staff Level
 - d. System Administrator
- III. CCHC will serve as the primary administrator of system access set-up and changes as defined in CCHC's HIE Portal Access Policy with its Participating Organizations and Business Associates, as well as for CCHC Workforce Authorized Users.
 - a. CCHC requires all Participating Organization and Business Associates to have executed its HIE Participation Agreement before submitting requests for Authorized users, based on role and function to CCHC Workforce.
 - i. CCHC may deny access to CCHC HIE to any Participating Organization or Business Associate until receipt of an executed HIE Participation Agreement is obtained.
 - b. CCHC requires all Participating Organizations to identify and verify its Authorized Users prior to submitting system set-up requests to CCHC Workforce.
 - c. CCHC requires all Participating Organizations to update and provide access termination requests and verification prior to submitting system request changes to CCHC Workforce in a timely manner, and as outlined in CCHC's HIE Access Termination Policy.

Individual Authorization Policy #8

- i. CCHC will maintain a log of all active users, and CCHC Workforce will start and trigger an audit to send to the participating organizations and will be conducted annually.
 - d. Participating Organizations are solely responsible for developing a process to verify and authenticate a Patient for Patient Portal access.
 - e. CCHC may request from its Participating Organizations or Business Associates with information deemed necessary to individually identify each Authorized User.
- IV. CCHC will provide Participating Organization education materials and links to website training tools to ensure compliance with all applicable Policies and Procedures for Individuals approved for CCHC HIE authorized access.
- V. Any individual member of a Participating Organization, Business Associate or CCHC Workforce who is not designated as an approved Authorized User shall not be allowed to access CCHC HIE for any purpose.

RESOURCES

- Reference – *CFR* Part 160 and Part 164, Subparts A and C
- Reference – CCHC HIE Portal Access Policy
- Reference - CCHC Workforce and User Training Policy
- Reference - CCHC HIE Access Termination Policy

Restrictions by Individual Policy #9

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to define CCHC's role in safeguarding Individuals (i.e., Patients) on their right to request restrictions on the use and disclosure of their own Protected Health Information (PHI). This policy defines how Participating Organizations (POs) and CCHC will implement required restrictions within the parameters of CCHC's HIE.

POLICY BACKGROUND

Health Insurance Portability and Accountability Act (HIPAA) Privacy Standards 45 C.F.R. 164.522 define the process by which Individuals may request restrictions on the use and disclosure of their own Protected Health Information (PHI) and Sensitive Health Information (SHI) to a Covered Entity. The right for an individual to request restrictions applies to disclosures of PHI for Treatment, Payment, Health Care operations, disclosures to persons involved in the Patient's health care or payment for health care; or disclosures to notify family members or others about the Individual's general health condition.

Covered Entities are not required to agree to requests for restrictions; however, the Covered Entity is required to have procedures in place to evaluate the request and to accept, deny and notify the individual of the request status. A Covered Entity may also accept the request for restriction with exception of providing the Individual Emergency Treatment.

CCHC is not a Covered Entity and will not accept requests for restrictions on the use and disclosure of PHI on behalf of its contracted Participating Organizations. CCHC HIE facilitates exchange of PHI of its Participating Organizations and for Permissible Purposes (References – CCHC's Patient Consent & Permissible Uses Policy & Use and Disclosure Policy).

Additionally as outlined in 45 C.F.R. 164.522, CCHC has adopted protocols for its Participating Organizations specifically regarding Sensitive Health Information (SHI) and its handling (Reference – CCHC Sensitive Health Information Policy). CCHC protocols and system configurations allow for SHI restricted information to be shared by Participating Organizations, at their option, through CCHC HIE for the Permissible Purposes of Emergency Treatment and Public Health Reporting.

If an Individual makes a request directly to CCHC to restrict the use or disclosure of PHI/SHI, CCHC will forward that request to the appropriate Participating Organization(s) within five (5) business days after receipt of the request. CCHC's Participating Organizations are responsible for researching and addressing all requests for individual restrictions and for ensuring system flagging protocols are enacted appropriately.

PROCEDURE

Restrictions by Individual Policy #9

- I. Individuals (i.e. Patients) will be educated by Participating Organizations on the various uses and disclosure of PHI and SHI and instructed how to submit requests for restriction.
 - a. Individuals shall direct all requests in writing or email and directly to the appropriate Participating Organization.
 - b. CCHC will redirect any direct requests for Individual restrictions to the appropriate Participating Organization for facilitation within five (5) business days upon initial request.
 - c. Individuals may request a modification or reversal of previously approved restricted data requests at any time in writing and for consideration with the Participating Organization to facilitate.
- II. Participating Organizations are exclusively responsible for researching and addressing all Individual requests for restrictions of PHI and SHI and maintaining compliance to all applicable Federal and State regulations.
 - a. Participating Organizations shall grant acceptance or denial of Individual restriction requests and ensure thoughtful evaluation on the restriction impact to the accuracy and integrity of the data within CCHC HIE.
 - b. Participating Organizations are responsible for informing the Individual in writing as to the request determination and any decision appeal procedures or re-instatement of previously approved restriction requests.
 - c. Participating Organizations that receive Individual restricted information shall ensure no re-disclosing of the restricted information to other third parties, with the exception of as sanctioned by law.
- III. CCHC's Security and Privacy Officer or designee will review restriction policy and request volume with its Participating Organization, at minimal, on an annual basis to ensure congruence of joint process controls.

RESOURCES

- Reference - 45 C.F.R. § 164.522
- Reference - California Civil Code 56
- Reference - CCHC Uses and Disclosure Policy
- Reference - CCHC Sensitive Health Information Policy
- Reference - CCHC Notification of Privacy
- Reference - CCHC Patient Consent & Permissible Uses

Policy Revisions and Maintenance Policy #10

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement a process for initiation of new CCHC HIE privacy and security policy and procedures requests through CCHC's established policy workflow structure as well as for modification of any previously adopted policies and procedures and corresponding forms.

POLICY GOVERNANCE BACKGROUND

As outlined in CCHC's governance plan, the Executive Committee (EC) ultimately is the decision maker for all adoption, revisions or replacement of CCHC's HIE privacy and security policies. The membership matrix, purpose, term limits and functions of the EC are defined in the CCHC governance plan. The CCHC Security and Privacy Officer or designee shall work with all sub-committees on initial requests to vet the appropriateness of all requests to assure adherence to the foundation of implementation and maintenance of secure protected health information exchange security, physical and administrative safeguards.

PROCEDURE

- IV. All requests for changes or new policies for consideration must be processed through the established CCHC HIE policy workflow structure:
 - a. CCHC Sub Committees – creation of new requests or modifications should be vetted initially by one of the following committees:
 - i. Privacy, Security & Compliance Committee
 - ii. Technology and Clinical Committee
 1. Technical Workgroup
 2. Physician Advisory & User Group
 - iii. Consumer & Education Committee
 - b. Requests made shall identify the subject of the new request or modification, the type of policy or procedure if a new request, a detailed description of why the request is needed, and any supporting impact analysis for adoption or modification.
 - c. The CCHC Security & Privacy Officer (SPO) or designee will provide an initial review for appropriateness and provide initial review feedback to the requestor within 30 business days.
 - d. Requests that are determined appropriate to proceed for EC consideration will be reviewed at designated EC policy and procedure meetings and will be co-presented by the CCHC SPO or designee and sub-committee lead.

Policy Revisions and Maintenance Policy #10

- e. The EC does have the option to review draft policies for feedback and/or decision electronically. Sample language for email review of policies and procedure is attached in the Appendix.
- f. The EC will decide on whether to approve the recommended new policy and procedure request or modification.
 - i. If approved, the EC will determine the appropriate effective date.
 - ii. If rejected or feedback for additional modification is provided by the EC, the CCHC SPO and subcommittee Chair shall be responsible for communicating to the requestor(s).
- V. The CCHC Security & Privacy Officer or designee is responsible for developing and maintaining all appropriate procedures prior to implementation.
- VI. Policies and procedures, and recordings of any change or modification decisions will be maintained in written or electronic form for the life of the policy, plus 6 years.
- VII. CCHC EC reserves the right to make amendments to the Security and Privacy policies and procedures. Notice of amendments may be provided by email, hard copy or posting the amendment, along with its effective date, on the CCHC HIE Intranet/OneDrive.
 - a. If there are material changes in policies and procedures, the affected CCHC Workforce, Participating Organization or Authorized Users must be trained on the amended policies and procedures prior to implementation.
 - b. CCHC will use its best efforts to provide notice of such new, amended or replaced policies and procedures to affected Participating Organizations or Authorized Users prior to the effective date of any such change.

RESOURCES

Maintaining Confidentiality Policy #11

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement and define procedures to protect an individual's Protected Health Information (PHI). All CCHC Workforce members and Business Associates will need to adhere and sign CCHC's confidentiality agreement.

PROCEDURE

- I. **Protection of PHI:** All Workforce members, directors, officers, contractors, and agents of CCHC HIE are responsible for protecting the privacy and security of all PHI that is received, whether orally or recorded, in the course of their work. An individual's PHI shall be protected from the moment it is received, used, stored, and eventually destroyed.
- II. **Confidentiality Agreement:** Each Workforce member, full-time employee, part-time employee, temporary employee, consultant, contracted employee, subcontractor, vendor, business associate, or agent of the CCHC HIE shall be required to sign a confidentiality agreement upon commencing work or entering into a contractual relationship with CCHC HIE.
 - a. All Workforce members, as a condition of employment, are required to sign the confidentiality agreement.
 - b. Copies of the agreement shall be maintained in the Workforce member's personnel file and a copy of the agreement will be provided to the employee.
 - c. Where required by HIPAA or California law, contractors who meet the definition of a business associate shall be required to execute a business associate agreement.
- III. **Protection of PHI - Hard Copies:** All PHI shall be maintained in a confidential manner that prevents unauthorized disclosure, either internally or to third parties. CCHC shall make all reasonable efforts to secure records containing PHI.
 - a. All PHI in hard copy form shall be kept in locked files with the number of keys limited to Workforce members whose work requires regular access to the information.
 - b. Documents containing PHI and that are deemed no longer necessary shall be destroyed in a method that induces complete destruction of the information.
- IV. **Procedure if a Breach is alleged:** All breaches of confidentiality shall be reported to the CCHC Privacy Officer.

Maintaining Confidentiality Policy #11

- a. Any Workforce member receiving an allegation of a breach of confidentiality or having knowledge or a reasonable belief that a breach of confidentiality of PHI may have occurred shall immediately notify the CCHC Privacy Officer.
- b. If it is determined that a breach of confidentiality of PHI has occurred, disciplinary action shall be taken in accordance with CCHC's disciplinary policy.
- c. The CCHC Privacy Officer shall retain documentation of all allegations that have been made and any action taken in a Master Employee HIPAA Complaint File and in the Workforce member's personnel file. A separate, secure file shall be maintained for documentation concerning violations by non-employees.

RESOURCES

- Reference – Confidentiality Agreement
- Reference – Response to Breach Policy
- Reference – Disciplinary Policy

Confidentiality Agreement Form for Workforce Policy #12

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to define the process and Workforce Confidentiality Agreement form content to be used to ensure strict confidentiality standards are adhered and potential repercussions are reviewed.

PROCEDURE

- I. CCHC's Security & Privacy Officer or designee will provide in advance to Workforce members or contracted entities, all pertinent CCHC HIE Security and Privacy policies and procedures for review before access to CCHC HIE is granted.
- II. Workforce team members will sign a Workforce Confidentiality Acknowledgement Form (content language below). A copy of the form will be provided to the Workforce member and also placed in the Workforce member's permanent employment record.
- III. It is recommended that Participating Organization's (POs) adopt this confidentiality acknowledgement process for their Workforce users.

Workforce Confidentiality Acknowledgement Form

For the Workforce Member:

I have read and understand the Central Coast Health Connect (CCHC) Confidentiality Policies on the use, collection, disclosure, storage, and destruction of Protected Health Information ("PHI").

I agree to follow the Confidentiality Policies and all related policies. I agree that, I will not reveal or disclose PHI to any person except as authorized by California and federal law. I also understand that my obligations to maintain strict confidentiality of PHI will continue after my employment or association with CCHC ends. Lastly, I understand that unauthorized use or disclosure of PHI may result in disciplinary action, which may include termination of employment or contract, the imposition of civil and criminal fines against me pursuant to California and federal laws, and reporting to any appropriate professional licensing board.

Include: Date, Employee Name, Employee Signature

Confidentiality Agreement Form for Workforce Policy #12

For the CCHC Privacy Officer, Manager or Designee:

I have discussed CCHC's Confidentiality Policies and the appropriate use, collection, disclosure, storage, and destruction of PHI with named employee or Workforce member. I have also discussed the consequences of a breach and provided an opportunity for questions.

Include: Date, CCHC Privacy Officer's Name and/or designee, and Signature

- IV. Any new or modified Confidentiality policies and procedures will require Workforce member review, acknowledgement, signed acceptance, and will be maintained in personnel files.

RESOURCES

Personally Identifiable Information (PII) Policy #13

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to establish the process to properly handle Personally Identifiable Information (PII) within CCHC's HIE and the corrective steps and consequences to be taken when a breach occurs.

POLICY BACKGROUND

- I. Personally Identifiable Information (or "PII," as used in this Policy) is information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc.
- II. The objectives of this policy is to ensure a clear definition of PII, adhere to training protocols for CCHC Workforce and Participating Organizations, and define corrective actions should there be a breach.

PROCEDURE

- I. All Personally Identifiable Information in the possession of CCHC is considered confidential unless:
 - a. The information is designated as "Directory Information" by the appropriate Data Provider; or
 - b. The Information Owner has otherwise authorized its disclosure.
- II. CCHC requires the following pieces of PII may not be collected, stored or used, except in situations where there is legitimate business need and no reasonable alternative for identification:
 - a. Social Security Number
 - b. Date of birth
 - c. Place of birth
 - d. Mother's maiden name
 - e. Credit card numbers
 - f. Bank account numbers
 - g. Income tax records, and
 - h. Driver's license numbers
- III. CCHC and Participating Organizations must ensure that their Workforce and employees understand the need to safeguard this information, and that adequate training and procedures are in place to minimize this risk. Access to such information may only be granted to authorize individuals on a "need to know basis".

Personally Identifiable Information (PII) Policy #13

- a. Additional telephone security protocols will be adopted by CCHC Workforce when taking calls from patients to ensure the appropriate identity is obtained by asking three (3) different questions to properly confirm patient PII identity. Examples of the types of question information include but are not limited to:
 - i. First Name and Last Name
 - ii. Phone Number
 - iii. Address
- IV. All breach incidents that involve PII must be reported to CCHC's Security & Privacy Officer under the same methods as defined in CCHC's Protected Health Information (PHI) Breach policies.
- V. CCHC will adhere to all applicable Federal and State laws governing improper use and disclosure of PII.

RESOURCES

- Reference – 45 CFR §155.260, Privacy and Security of PII
- Reference – 45 CFR §164.402
- Reference – California Civil Code, Section 1798.80-1798.84
- Reference – CCHC Protected Health Information and Breach Policies

Uses and Disclosure Policy #14

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to describe CCHC's role in ensuring compliance with use and disclosure of CCHC HIE's Protected Health Information (PHI) as required by Federal and State laws and regulations. Additionally, this policy will define data use and disclosure parameter as it pertains specifically for marketing or commercial purposes. This policy incorporates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements that PHI may be used or disclosed only for Permissible Purposes and should only disclose the amount of information reasonably and minimally necessary to achieve a particular purpose.

PROCEDURE

- I. All use and disclosure of PHI through CCHC HIE shall be consistent with all applicable laws.
 - a. Other permitted or required Uses and Disclosure may include but not limited to:
 - i. PHI may only be used and disclosed in accordance with the business associate agreement between CCHC and Member Participants;
 - ii. Public Health – PHI may be disclosed to an authorized public health authority for specified reasons such as to prevent or control disease, injury, or disability; to report child abuse or neglect; to report the safety or effectiveness of FDA-related products such as medication; and to notify a person at risk of contracting or spreading a communicable disease. Such reports will only be made at the request of Participant Member;

- II. Direct requests to CCHC for legal release of PHI will be handled by the CCHC Workforce Administrator with assistance from CCHC's legal counsel and they shall verify the authenticity of any subpoenas, court orders, or discovery requests for the disclosure of PHI maintained in CCHC HIE. CCHC Workforce will notify the Participating Organization of request for disclosure of information and keep a master tracking log of these requests. CCHC shall respond to these requests in an appropriate timeframe as required and outlined in HIPAA, 45 C.F.R. § 164.512 Before releasing PHI as required by law, CCHC shall perform:
 - a. Identity Verification
 - i. The identity of an individual/entity/requestor shall be verified by obtaining a written documentation, statement, or representation from the requesting entity.
 - ii. Physical presentation of a public official or agency identification badge, legal credentials, or other proof of government status if made in person shall be subject to cross-verification of the public official's identity.

Uses and Disclosure Policy #14

- b. Authority Verification
 - i. Prior to releasing PHI, CCHC shall make good faith efforts to verify the legal permission_of any entity requesting protected information to have access to the PHI.
 - c. Limited Disclosure to the Minimum Necessary
 - i. All disclosures of PHI shall be limited to the minimum amount of PHI necessary to achieve the intended purpose of the release.
- III. CCHC shall not release PHI for marketing or commercial purposes. The use of consumer information available through CCHC HIE for purposes other than Treatment, Payment or Healthcare Operations (TPO) or for any secondary uses approved by CCHC's Executive Committee is prohibited by CCHC and all Participating Organizations.
- IV. Participating Organization and Authorized Users disclosing PHI through CCHC HIE shall comply with CCHC's HIE Participation Agreement terms and conditions including enforcement and accountability protocols.
- a. The CCHC Privacy, Security & Compliance Committee (CPSCC) or Designee may either, independently or upon request of a Participant, review the uses and disclosures of Patient Data by any Participant, including without limitation the Participant's adherence to the Terms and Conditions and/or Policies and Procedures, and make recommendations to CCHC Executive Committee regarding actions to be taken with respect thereto.
 - b. Any action by the CPSCC and CCHC Executive Committee shall be taken only in accordance with the Terms and Conditions and the Policies and Procedures, and CCHC Executive Committee shall provide the Participant an opportunity to provide information regarding the matter(s) involved in any such action to CCHC Executive Committee before any action is taken.

RESOURCES

- Reference – California Civil Code 56.10
- Reference – 45 C.F.R. 164.506 & 164.508 (3)(i)
- Reference – HITECH Section 13405
- Reference - CCHC Notice of Privacy Practice Policy

Workforce and User Training Policy #15

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to establish reasonable safeguards and procedures for privacy training of protected Patient Health Information (PHI) for CCHC HIE Workforce and applicable contracted entities. Such training should be conducted as necessary and as appropriate for CCHC Workforce to carry out their duties for CCHC HIE.

PROCEDURE

- I. The establishment of a security & privacy training course tailored on role and access level for CCHC Workforce and contracted Users will be the responsibility of the CCHC Security & Privacy Officer or designee, in addition to ensuring adherence to Participating Organization's standing HIPAA Compliance Training.
- II. All members of CCHC's Workforce who come into contact with Protected Health Information (PHI) in performing their job function will be trained on the privacy laws, policies, and procedures regarding PHI. The following Workforce members will be trained.
 - a. All new CCHC Workforce members hired, will be trained during new hire orientation and before access is granted to the HIE.
 - b. All CCHC Workforce members whose duties are affected by a material change in privacy policies will be re-trained within thirty (30) days after any changes to newly adopted policies becomes effective.
 - c. Workforce members who have violated privacy laws, policies, or procedures shall be re-trained no later than thirty (30) days of the determination of the violation.
- III. A copy of documentation confirming completion of required training courses will be provided to the CCHC Workforce member and will also be kept as a permanent record of the CCHC Workforce member's employee file.
- IV. CCHC shall designate an individual or department within its organization with responsibility for training of its Workforce members regarding Federal and State laws concerning PHI and its own privacy policies. Such training may include:
 - a. Identifying appropriate personnel and assigning responsibility for privacy awareness training;
 - b. Purchasing of privacy online training tools or hire an instructor who is skilled at HIPAA privacy requirements to conduct the initial training for the CCHC Security & Privacy Officer or designee for train the trainer assistance; or

Workforce and User Training Policy #15

- c. Ensuring that current policies and procedures are reviewed periodically at staff meetings.
- V. Training shall include a detailed review of applicable policies and procedures and each trained Workforce member shall sign an acknowledgment that he or she received, read, and understands these policies. A signed acknowledgment will be provided to the Workforce member and a copy kept in their permanent employment files.
 - a. Sample Workforce Training Log should contain the following, at minimum:
 - i. Workforce Member Name
 - ii. Date of Initial Privacy Training
 - iii. Date of Additional Privacy Training
 - iv. Date Confidentiality Agreement Signed
 - v. Date Provided Access to PHI
 - vi. Date Access to PHI Terminated
 - vii. Sanctions and Disciplinary Action
- VI. **Discipline for Non-Compliance.** CCHC shall implement procedures to discipline and/or hold CCHC Workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these policies and that they comply with these policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.
- VII. **Reporting of Non-Compliance.** CCHC shall have a mechanism for, and shall encourage, all CCHC Workforce members, to report any non-compliance with these Policies to the Participant Organization. Each Participant Organization also shall establish a process for individuals whose health information is included in the CCHC HIE to report any non-compliance with these policies or concerns about improper disclosure of information about them, in concordance with current HIPAA regulations and reporting requirements.

RESOURCES

- Reference - 45 C.F.R. §164.308(a)(1)(i)

De-Identification of PHI Policy #16

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to define the permitted utilization and process when CCHC may use and disclose de-identified Protected Health Information (PHI).

POLICY DETAILS

De-identification is the process by which PHI is adapted into data that does not identify an individual/Patient. HIPAA defines de-identification of data as follows, "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." Once PHI data has been de-identified, it is considered outside the scope of Health Information Portability and Accountability Act (HIPAA), California Medical Information Act (CMIA) and other applicable privacy regulatory standards. Once health information has been de-identified, no authorization is required by an individual/patient to be used or disclosed.

PROCEDURE

- I. Participating Organizations may file requests for de-identified data to be used for efforts related to research or public health as applicable by law. As such, all requests for de-identified data are subject to evaluation and approval by the CCHC Executive Committee and the de-identified data may not be used for another purpose or sent to a third party without pre-approval by CCHC.
 - a. Potential types of research or public health efforts include, but are not limited to the following:
 - i. Health Quality Improvement
 - ii. Disease Tracking
 - iii. Public Health Threats
 - b. CCHC shall have complete discretion in evaluating any request for de-identified data from CCHC HIE and has the autonomy to deny a request for any reason. Some potential reasons for denial, but not all inclusive, include:
 - i. The rationale for the request for de-identified data is not for a legal research or public health purpose;
 - ii. There are CCHC limitations on the ability to de-identify the PHI; or
 - iii. The requesting Participant Organization does not agree with restrictions imposed by CCHC of the use of the de-identified data.
- II. Documentation of the request and subsequent CCHC leadership approval or denial of the

De-Identification of PHI Policy #16

- request will be maintained by the CCHC Security & Privacy Officer or designee.
- III. CCHC's Workforce or designee may access PHI thru CCHC's HIE to de-identify data with proper identifier removal as outlined in this policy.
- IV. CCHC Workforce or designee will ensure de-identification of an individual's health information by the removing the following identifiers as defined in 45 CFR § 164.514(b)(2)(i):
- a. Names
 - b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes
 - c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
 - d. Telephone numbers
 - e. Fax numbers
 - f. Social Security numbers
 - g. Electronic mail address
 - h. Medical record numbers
 - i. Health plan beneficiary numbers
 - j. Account numbers
 - k. Certificate/license numbers
 - l. Vehicle identifiers and serial numbers, including license plate numbers
 - m. Device identifiers and serial numbers
 - n. Web Universal Resource Locators (URLs)
 - o. Internet Protocol (IP) address numbers
 - p. Biometric identifiers, including finger and voice prints
 - q. Full face photographic images and any comparable images
 - r. Any other unique identifying number, characteristic, or code
- V. CCHC will not use or de-identify any PHI of a Patient who has elected to Opt-out of CCHC HIE.
- VI. No Participating Organization shall have the right to restrict CCHC's use or disclosure of de-identified data for the activities of the HIO.
- VII. CCHC may assign a method of record identification to re-identify the de-identified data as long as the method is not able to be translated to identify the individual and does not disclose the method for re-identification.

RESOURCES

- Reference - 45 CFR § 164.514(a)-(c)

Disposal of PHI Policy #17

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure safeguards and processes are in place for the disposal of hard and electronic media containing Protected Health Information (PHI) and are in concert with applicable Federal and State media sanitation requirements.

PROCEDURE

- I.** CCHC and its contracted Business Associates will ensure disposal or reuse of media containing PHI will be done in accordance with applicable Federal and State regulations.
- II.** Media containing PHI involved in any current or upcoming audit, investigation, or legal action should not be destroyed and the record retention limits of (7) years shall be suspended.
- III.** Media slated for disposal or reuse should be secured against inappropriate access until the disposal or reuse is certified as complete.
- IV.** CCHC's Privacy Officer or designee, shall maintain records of all disposed PHI media and those records will include at minimum:
 - a.** Date of disposal,
 - b.** Ownership and methodology of disposal,
 - c.** A statement that the PHI was disposed of in the normal course of business; and
 - d.** The signatures of the individual(s) performing and supervising the disposal.
- V.** Media containing PHI should be cleared, purged, or destroyed by the following methods:
 - a.** Hard Copy Media: Paper printouts, film, facsimile ribbons or other hard copy media shall be shredded or destroyed such that the PHI cannot be read or reconstructed.
 - b.** Electronic (or soft copy) Media: Bits and Bytes contained in hard drives, random access memory (RAM), read-only memory(ROM), disks, memory devices, phones, mobile computing devices, and other electronic media shall be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media sanitization: <http://csrc.nist.gov/>, so that PHI cannot be recovered.
 - c.** Redaction of media is excluded as a means of PHI destruction.
- VI.** CCHC's Privacy Officer or designee shall categorize the information to be disposed of, assess the platform of the medium on which it is recorded, assess the risk to confidentiality, and assuage the future plans for the media. Then, using information in Table A1 below, decide on the appropriate method for sanitization (cleared, purged, or destroyed). The selected method should be evaluated as to cost, impact, etc., and a decision should be made and approved by CCHC's Executive Committee that appropriately mitigates the risks to an unauthorized disclosure of information.

Disposal of PHI Policy #17

Table A-1 Sanitization Methods

Source: NIST Special Publication 800-88 (regarding media sanitation): <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. • <i>Disintegration, Pulverization, Melting, and Incineration.</i> These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • <i>Shredding.</i> Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm ²).

- VII.** Should CCHC contract with a vendor to provide disposal services, the HIE Participation Agreement shall provide that the vendor will establish the permitted and required uses and disclosures of information under federal and state law as outlined in the Business Associate Agreement section of the HIE Participation Agreement, and include the following:
- a. Specify the method of disposal;
 - b. Specify the timeframe between acquisition and destruction of data/media;
 - c. Establish safeguards against breaches in confidentiality protocols;
 - d. Indemnify CCHC from loss due to unauthorized disclosure, and, if appropriate, require that the contractor (Business Associate) maintain liability insurance in specified amounts at all times the Business Associate Agreement is in effect;
 - e. Comply with the destruction requirements set by Federal and State regulations; and

Disposal of PHI Policy #17

- f. Provide proof of disposal certificate.
- VIII.** The methods of disposal should be reassessed by CCHC's Security & Privacy Officer or designees as determined, based on additions or changes in current technology, best practices, and availability of economical disposal services or as additional Federal and/or State guidelines are refined.
- IX. Media Re-use:** All Electronic Media that contains PHI shall be processed in a manner to ensure such PHI is permanently removed prior to the re-use of such Electronic Media. Prior to any re-use of any Electronic Media that contains or at any time contained PHI, CCHC administrative staff shall write over or "degauss" such media to prevent recovery of PHI. If an Electronic Medium cannot be overwritten or otherwise have PHI permanently deleted, such medium must be destroyed by CCHC administrative staff. This procedure shall be regularly updated to reflect new technology relating to the deletion or erasure of information contained on Electronic Media.
- X. Accountability:** All movement or reuse of equipment and/or Electronic Media containing PHI must be recorded and maintained, and such record shall include the name of the individual to whom such equipment or media has been assigned. Such record must be retained in accordance with CCHC's record retention policy.
- XI. Data Backup and Storage:** CCHC, or its designee, shall ensure that exact copies of PHI are retrievable before the movement, replacement or reuse of equipment.
- XII.**

RESOURCES

- Reference - NIST Special Publication 800-88 (regarding media sanitation): <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
- Reference - 45 CFR 164.310(d)(2)(ii) and (ii) (regarding re-use of media)
- Reference - 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i) which ensures appropriate training for anyone involved in the disposal of PHI
- Reference - HHS HIPAA Security Series 3: Security Standards - Physical Safeguards
- Reference - CCHC Certification Form for Disposal of PHI Policy

Certification Form for Disposal of PHI Policy #18

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure by certification that entities contracted with CCHC are educated in all destruction and disposal requirements outlined in CCHC's Disposal of PHI policy and procedure. The attached certification form will be completed by CCHC's Security and Privacy Officer or designee and counter-signed by CCHC contracted vendor and/or Business Associate.

PROCEDURE

- I. The CCHC Security and Privacy Officer or designee will create, maintain, and distribute and receive the following Certification Form for Disposal of PHI within five (5) business days.
- II. Retention of the signed Certification form will be the responsibility of CCHC's Security & Privacy Officer or designee and will remain for at minimal (7) years, and beyond for any incidents under review or warranting legal action.
- III. CCHC's Security and Privacy Officer and/or Executive Committee will review the Certification Form's content for appropriate updates on a routine basis.

RESOURCES

- Reference – CCHC Disposal of PHI Policy

Certification Form for Disposal of PHI Policy #18

Appendix – CCHC Certification Form for Disposal of PHI

Facility Name

The information described below was destroyed in the normal course of business pursuant to a proper retention schedule and destruction policies and procedures.

Date of Destruction: _____ Authorized By: _____

Description of Information Sanitized: _____

Inclusive Dates Covered: _____

Method of Destruction:

Burning Shredding Pulping Demagnetizing Overwriting Pulverizing

Other: _____

Records Destroyed By: _____

Witness Signature: _____

Department Supervisor: _____

Media Reused Internally or Externally: Yes – to whom, No – confirm

Media Returned to Manufacturer: Yes – to whom, No – confirm

Other – If records are destroyed by outside firm, must confirm that a Business Associates contract exists and certificate of destruction has occurred.

Malicious Software, Virus and Other Threats Policy #19

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure safeguards are instituted for CCHC HIE's detection and reporting of malicious software that could create potential risks to the privacy and security of its Protected Health Information (PHI) in addition to the security protocols instituted by its technology partner, RelayHealth. CCHC advises all Participating Organizations, and Authorized Users to ensure similar HIPAA security precautions and practices.

PROCEDURE

- I. CCHC will make prudent efforts to protect the HIE services offered through its network and media containing PHI from malicious software and ensure strong virus protection practices, including but not limited to:
 - a. Ensure routine review of its technology vendor, RelayHealth's malicious software and virus protection protocols;
 - b. Ensure up-to-date anti-virus software is installed on all media devices and hardware used by CCHC Workforce containing PHI and have connection to the network;
 - c. Mitigate the harm of malicious software attacks by recovering PHI and other data contained on all media devices and hardware that has been attacked by malicious software;
 - d. Conduct routine virus scans of its network server and workstations and update accordingly with the most recent virus definitions;
 - e. Ensure CCHC Workforce does not bypass or disable anti-virus software installed on Workstations unless they are authorized to do so by management;
 - f. Provide periodic training and awareness to CCHC Workforce about guarding against, detecting and reporting malicious software, including but not limited to:
 - i. How to use anti-virus software
 - ii. How to report suspect malicious software incidents
 - g. Provide education to CCHC Workforce to use CCHC workstations, including email and web browsing, only for CCHC business purposes and to promptly report suspected or confirmed malicious software incidents to the CCHC Security & Privacy Officer or other designated designee.
 - h. Participating Organizations (PO) shall ensure education, training, and periodic reminders are sent to Authorized Users to promptly report suspected or confirmed malicious software incidents to their PO lead, who will report to CCHC Security & Privacy Officer or CCHC Workforce designee.

RESOURCES

Malicious Software, Virus and Other Threats Policy #19

- Reference - 45 § C.F.R. 164.308(a)(5)(ii)(B) - HIPAA Administrative Specifications regarding Security Rules

Disaster Recovery and Data Back-Up Plan Policy #20

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure the routine review of CCHC HIE technology vendor, RelayHealth's ability to create, implement and maintain safeguards of CCHC HIE's Protected Health Information (PHI) by means of established robust Disaster Recovery, Data Back Up, and Emergency Mode Operation plans. Through these plans, RelayHealth shall provide CCHC recoverable extract copies and ability to restore and recover any loss of PHI and HIE services after an emergency or disaster such as power loss, fire, natural disasters, vandalism, or security issue and to enable continuation of critical HIE processes while operating in emergency mode.

PROCEDURE

- I. CCHC HIE's Security & Privacy Officer or designee will review and monitor its technology vendor, RelayHealth's disaster recovery plan and procedures on an annual basis. Current RelayHealth Security Measures online Legal Notice as of 2014 states:
 - a. RelayHealth currently utilizes the highest levels of disaster recovery available on the market which ensures uptime by preventing outages caused by power, security, environment, fire, and natural disasters. Within these facilities, RelayHealth is able to deliver the highest levels of reliability through a number of redundant subsystems, such as multiple Internet trunks coming into from multiple sources, fully redundant power on the premises, and multiple backup generators.
- II. CCHC HIE's Security & Privacy Officer or designee, will review and monitor its technology vendor, RelayHealth's data back-up policies and procedures on an annual basis and ensure any changes, updates or plan revisions are incorporated in any applicable policies and informed to any CCHC Workforce administrative members as needed.
- III. CCHC HIE's Security & Privacy Officer or designee will review and monitor its technology vendor, RelayHealth's emergency mode operations plan and procedures on an annual basis and ensure that any changes, updates or plan revisions are incorporated in any applicable polices and informed to any CCHC Workforce administrative members as needed.
- IV. CCHC shall require its technology vendor, Relay Health, to implement procedures for periodic testing and revision of its Disaster Recovery, Data Backup, and Emergency Mode Operation plans. CCHC's technology vendor will also be required to assess the relative criticality of specific applications and data in support of other contingency plan components.
- V. CCHC will perform a periodic technical and nontechnical evaluations based initially upon the Security Standards and subsequently, in response to environmental or operational

Disaster Recovery and Data Back-Up Plan Policy #20

changes affecting the Security of PHI that establishes the extent to which the Security Policies meet the requirements of the Security Standards.

RESOURCES

- Reference - 45 C.F.R. 164.308(a)(7)(ii)(b) – Disaster Recovery
- Reference - 45 C.F.R. 164.308(a)(7)(ii)(a) - Data Back Up Plan
- Reference - 45 C.F.R. 164.308(a)(7)(ii)(c) - Emergency Mode Operation Plan
- Reference - 45 C.F.R. 164.308(a)(7)(ii)(d) - Testing and Revision Procedures
- Reference - 45 C.F.R. 164.308(a)(7)(ii)(e) - Applications and Data Criticality Analysis

Sanction Policy #21

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of the policy is to define the responsibility of each Workforce member to comply with CCHC's policies, procedures, and applicable California and Federal privacy laws and regulations. Additionally, to ensure Workforce members understand that reporting known or susceptible violations to the CCHC Security & Privacy Officer is an employment requirement.

PROCEDURE

I. Duty to Report Violations of Policies by Workforce Members

- a. It is incumbent of any Workforce member who witnesses any violations or unapproved access to Protected Health Information (PHI) or any other desecrations of CCHC's policies must immediately report the violation to the CCHC Security & Privacy Officer or Participating Organization/Provider Designee who will in turn notify the CCHC Security & Privacy Officer.
- b. Workforce members, who believe that a PHI violation has occurred, can report such violation to CCHC's Security & Privacy Officer without fear of retribution.
- c. Failure to report or alert the CCHC Security & Privacy Officer of a known or suspected violation of CCHC's PHI policies is considered a violation and may lead to disciplinary action or termination.

II. Protocols for Disciplinary Action

- a. Below are examples of actions that could lend itself to Workforce violations and lead to disciplinary action (note – said list is not all inclusive).
 - i. Looks up an individual's or relative's address for personal rather than legitimate and authorized business purposes;
 - ii. Discusses patient information in a public area;
 - iii. Leaves hard copy patient documents in a public area; and
 - iv. Demonstrates a practice of leaving a computer containing PHI unsecured.
- b. Non-compliance with CCHC's PHI policies could lead to disciplinary action or termination. The suitable level of disciplinary action will be based on the unique violation situation and its severity. Any Workforce member who is not terminated and has to comply with disciplinary action will be required to mandatory repeat review of applicable PHI and confidentiality policies and procedures.
 - i.

Sanction Policy #21

RESOURCES

Complaint Resolution Policy #22

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement a procedure for receiving, documenting, and taking appropriate and timely action with respect to privacy and operationally oriented complaints about CCHC HIE by a Participating Organization, Patient, Business Associate or Authorized User. As guided by the Office of the National Coordinator (ONC), via the HITECH act on complaint accountability protocols, this policy seeks to assure effective filing of complaints methodology and procedures for resolving complaints timely and through corrective actions.

PROCEDURE

- I. All Privacy and operationally oriented complaints by Authorized Users, Participating Organizations, Patients or Business Associates must be submitted to the CCHC's Security & Privacy Officer.
- II. Complaints will be accepted verbally but submitted in writing or electronically is preferred.
- III. CCHC's Security & Privacy Officer or designee will acknowledge receipt of complaint to the individual submitting the concern and initiate a timely review and/or investigation. If the health care information at issue was created or maintained by a Participant Organization or a Business Associate, the complaint will be forwarded to the Participant Organization or Business Associate.
- IV. The CCHC Security & Privacy Officer or designee shall determine:
 - a. Whether there has been a violation of privacy regulations or CCHC's privacy policies and determine appropriate sanctions.
 - b. What, if any, internal privacy practices need to be changed.
 - c. What, if any, additional policies need to be developed.
 - d. Who within CCHC's Workforce and/or governance structure should assist in the review.
 - e. What additional training will be provided to the person who violated the privacy regulation or policy.
 - f. When additional involvement by a Participating Organization, Business Associate, Authorized User or others with expertise is needed to review said complaint.
 - g. If the complaint involves a potential Breach of Protected Health Information (PHI), then CCHC Response to Breach Policy shall be enacted.
- V. The CCHC Security & Privacy Officer or designee shall document all complaints received by CCHC and the action taken in response to the complaint in a separate and confidentially maintained individual complaint file and keep for six (6) years.
 - a. Documentation of each complaint will be retained in written or electronic form.

Complaint Resolution Policy #22

- b. If after review and further investigation, the CCHC Security & Privacy Officer determines that the complaint cannot be verified or validated, then no further action is needed by either CCHC or CCHC's Security & Privacy Officer beyond notifying the individual that the complaint is unverifiable.
 - c. Should the complaint be verified as true, then CCHC will assuage what actions are needed to resolve the complaint, as appropriate. Actions could involve procedural modifications, system alterations, updated security efforts, sanctions, or any other measure necessary by CCHC to provide a fair and effective complaint resolution.
- VI. The CCHC Security & Privacy Officer will facilitate the response, status and actions to be taken back with the individual filing the complaint and should the proposed resolution not be deemed satisfactory, a request for further review can be made to the CCHC Executive Committee.
- VII. All complaints shall be ultimately resolved by CCHC within six (6) months from receipt of the complaint; however, CCHC shall do its best to resolve within 60 days.
- VIII. Individual's also have the right to file a complaint to the federal Office of Civil Rights about possible violations of federal health privacy laws within 180 days of when the individual knew or should have known an act or omission of the complaint occurred, unless this time limit is waived by the DHHS Secretary.

Office for Civil Rights, Region IX
U.S. Department of Health and Human Services (DHHS)
50 United Nations Plaza, Room 322
San Francisco, CA 94102
Phone: 415-437-8310
Fax: 415-437-8329

RESOURCES

- Reference – CCHC Response to Breach Policy
- Reference - 78 Fed. Reg. at 5578-79 (to be codified at 45 C.F.R. §§ 160.306(c), 160.308)
- Reference – 45 C.F.R. § 160.306, 45 C.F.R. 164.520(b)(vi)

Response to Breach and Security Incidents Policy #23

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to outline the actions to be taken by Central Coast Health Connect (CCHC) in response to a suspected breach of Protected Health Information (PHI), Security Incident, or Privacy Event involving CCHC HIE. The notification process, identification, reporting, investigation, and response to a suspected Breach or Security Incident will be in compliance with the HIPAA Breach Notification and applicable state or federal law. CCHC and its Technology Vendors, Participating Organizations, Workforce and Authorized Users will strive to prevent any Breach of health records either electronically or otherwise, and will implement Privacy and Security measures to protect the confidentiality of the information contained within CCHC HIE.

POLICY DETAILS

- I. CCHC will abide by all applicable Federal and State regulations pertaining to the privacy and security of Protected Health Information (PHI).
- II. CCHC's Workforce, Technology Vendors, Participating Organizations and Authorized Users have an obligation to report any suspected Breaches, Security Incidents, or Privacy Events of CCHC HIE to CCHC's Security & Privacy Officer.
- III. Federal and State laws require a notification to be made if there is a Breach of Unsecured Protected Health Information, Medical Information, or Personal Information. Investigation and reporting of such Breaches will be in accordance with the procedures outlined below.

PROCEDURE

- I. Participating Organizations who encounter a suspected Breach shall follow the process outlined below.
 - a. Any CCHC Participating Organization ("PO") who becomes aware of any suspected Breach or Security Incident disclosed through CCHC HIE or any Privacy Event must contact CCHC and/or CCHC's Security & Privacy Officer without unreasonable delay, and in no case more than (1) business day after discovery. If a suspected Breach or Security Incident is involved, the PO will include enough baseline information in the CCHC Breach Risk Assessment Form for CCHC to begin initial investigation and assist CCHC as needed in the review.
 - b. When a Participating Organization identifies a PHI breach, the attached HIE Participant Breach Notification form should be completed by the Participating Organization and emailed to CCHC-Help@CentralCoastHealthConnect.org

Response to Breach and Security Incidents Policy #23

- II. If CCHC encounters a suspected Breach, it shall follow the process outlined below::
- a. CCHC Security & Privacy Officer or designee will maintain an internal incident reporting log and process designed to identify, internally report, investigate and resolve the suspected Breaches or Security Incident.
 - b. CCHC's Security & Privacy Officer or designee will notify the "Breach/Disclosure Task Force" immediately after discovering a suspected Breach or Security Incident.
 - i. Additionally, the CCHC Security & Privacy Officer must notify CCHC's "Privacy, Security & Compliance Committee" members, and convene the "Breach/Disclosure Task Force" in order to begin investigation.
 - c. CCHC shall report the information described below to Participating Organization without unreasonable delay, and in no case more than one (1) business day following CCHC's discovery of a suspected Breach of Security Incident. Such notice shall include, to the extent possible:
 - i. The identification of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the breach;
 - ii. The date of the breach;
 - iii. The date of the discovery of the breach;
 - iv. A description of the types of unsecured PHI that were involved;
 - v. Any other details relevant to an assessment of the risk that the PHI has been compromised.
 - d. CCHC shall investigate each Security Incident or suspected Breach that it discovers and consult the Breach/Disclosure Task Force to make the following determinations:
 - i. Whether a Breach occurred,
 - ii. The scope and severity of the breach, if it occurred (i.e., the number and identities of individuals whose PHI may have been breached, the severity of the security breach),
 - iii. If possible, the individual(s) that caused or contributed to the breach, and
 - iv. Whether notification is required.
 - e. CCHC's Security & Privacy Officer shall provide a summary of its investigation to Breach/Disclosure Task Force and the Participating Organization. If the Breach/Disclosure Task Force determines that such Security Incident or suspected Breach constitutes an actual Breach, then CCHC shall comply with the requirements below.
 - f. The CCHC Security & Privacy Officer or designee will take the following steps, in consultation with the Breach/Disclosure Task Force:
 - i. Develop a Mitigation Plan to reduce any chance that a similar breach recurs and to ensure all appropriate notifications are facilitated. The Mitigation Plan should identify the response to the Breach including:
 1. Identify the cause of or contributing factor(s) of the security breach and identification of the corrective action.
 2. Assess whether the breach was intentional or accidental and the corresponding action items resulting from the assessment.

Response to Breach and Security Incidents Policy #23

3. Review and correct where appropriate, any policy or procedure that directly caused or contributed to the breach of confidentiality.
 4. Study the physical, technical and procedural safeguards and ensure appropriate counter-measures, such as monitoring systems for patterns of suspicious behavior that can be taken by CCHC.
 5. Work with its Technology Vendor, RelayHealth to correct any issues with respect to technical safeguards, if appropriate.
 6. CCHC shall take prompt corrective action, including any action required by applicable state or federal laws and regulations relating to such Security Incident or Breach.
- g. In addition, CCHC shall report to Participating Organization on a regular and periodic basis the ongoing existence and occurrence of Unsuccessful Security Incidents that are reported to CCHC or for which it becomes aware.

III. Notification:

- a. Notification delay is provisional if law enforcement officials inform the Participating Organization or CCHC that the notification, notice, or posting timing could impede the criminal investigation or cause damage to national security, and in those unique situations timing may be delayed for a specified period documented by the law enforcement official and be compliant with 45 C.F.R., Part 164.412 Subpart D.
- b. Participating Organizations involved in the Breach, through their workforce being partially a cause of the breach, or data from their organizations being affected in the breach, are responsible for reporting the incident to affected individuals, the CDPH, HHS, state attorney generals, or any other regulatory body as may be required by HIPAA, California Health & Safety Code 1280.15, or California Civil Code 1798.29 or 1798.82, as applicable.
- c. CCHC and affected Participating Organizations will meet and confer in good faith before notifying affected individuals and/or regulatory bodies regarding any suspected or actual Breach, and shall comply with applicable privacy laws regarding the need for, nature of, and content of any notification.
- d. Participating Organization's Privacy Officer is responsible for reporting to the CDPH, HHS, state attorney general, or other regulatory body as required by law. CCHC shall cooperate with the affected Participating Organization's Privacy Officer in order to assist him/her with the investigation or the provision of any information needed to report the Breach to any required parties. Even if only one organization is involved, that organization is still responsible for the initial reporting of a potential breach to the CCHC Security & Privacy Officer, so the CCHC Breach/Disclosure Task Force can be notified and a full investigation can be completed to confirm only one organization is truly involved.

RESOURCES

- Reference – 45 C.F.R § 164.400-41 – HIPAA Breach Notification Rule

Response to Breach and Security Incidents Policy #23

- Reference – 45 C.F.R § 164.412 Subpart D – HIPAA Law Enforcement Delay
- Reference – 45 C.F.R § 164.408 – Instructions for Submitting Notice of Breach to Secretary
- Reference - HITECH Omnibus FR, 78 FR 5566, January 25, 2013
- Reference – HITECT Act, Section 13407
- Reference – CCHC Breach Notification Form Policy
- Reference – CCHC Breach Risk Assessment Form Policy

Response to Breach and Security Incidents Policy #23

CCHC HIE Breach Notification Form

To be completed by the entity who identified the PHI breach.

Brief description of information disclosed (provide copies of information disclosed)	
Date disclosure occurred	
Date of disclosure awareness	
How you (your department) became aware of the disclosure (including name(s) of individuals notified)	
Name, medical record, and account number of patient(s) whose information was disclosed	
Address for patient whose information was disclosed	
Name of intended recipient	
Name of actual recipient	
Actions taken to retrieve/remove misdirected information	
How did the disclosure occur?	
Actions taken to prevent recurrence (includes counseling, discipline and procedure changes as appropriate)	
Individual, department, or facility responsible for the disclosure (include staff name, title, department or phone number of other facility)	

Response to Breach and Security Incidents Policy #23

Additional information	
Name of individual completing this form	

Time critical document

Please submit via Secure E-mail: CCHC-Help@CentralCoastHealthConnect.org

Phone: 831-644-7494

Response to Breach and Security Incidents Policy #23

CCHC HIE Breach Risk Assessment Form

This worksheet must be completed by the CCHC SPO or designee for each possible breach of Protected Health Information (PHI) and sent to the affected Participating Organization's Privacy Officer within 24 hours of receiving an HIE Participant Breach Notification form.

Date(s) of breach of PHI _____
Date breach detected _____

Submitter Contact Information

Full Name: _____

Organization: _____

Address: _____

Phone: _____

Email: _____

Incident Background

1. Was protected health information (PHI) involved?

- Yes, PHI was involved. *Continue to Question 2.*
- No, PHI was not involved. No breach reporting required under HIPAA.
Describe the information involved:

2. Was the PHI unsecured? (*"Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance, such as encryption or destruction. The guidance can be found on the DHHS website at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.)*)

- Yes, PHI was unsecured. *Continue to Question 3.*
- No, PHI was secured. No breach reporting required under HIPAA.
Describe the PHI (for example, was it verbal, paper, or electronic? Encrypted or password protected, other?):

Response to Breach and Security Incidents Policy #23

3. Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule? *(Providers should keep in mind that a violation of the “minimum necessary” standard is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. Providers may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule.)*

Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. *Continue to Question 4.*

No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

Describe who acquired, accessed, used and/or disclosed the PHI, whether the person(s) was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed:

4. Does an exception apply? Check any box below that applies:

Exception A.

A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

(i) Was made in good faith; and

(ii) Was within the course and scope of authority; and

(iii) Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce” includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether or not they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

Exception B.

A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

Exception C.

A breach does not include disclosure of PHI where the provider or business associate has a good faith belief that the unauthorized person who received it would not reasonably have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse

Response to Breach and Security Incidents Policy #23

mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.

- Yes, an exception applies. No breach reporting required under HIPAA.
- No, an exception does not apply. *Continue to Question 5.*

5. Risk assessment. An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL of the factors listed below.)

Factor A. Consider the nature and extent of the PHI involved, including the types of identifiers (and the likelihood of re-identification if the PHI is de-identified). *(Consider whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, STD, cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interests. Hospitals should also determine whether there is a likelihood that the PHI could be re-identified (if the PHI is de-identified) based on the context and the ability to link the information with other available information.)*

Describe the PHI involved, including identifiers and likelihood of re-identification (if the PHI is de-identified):

Consider whether PHI could be used in a manner adverse to the patient(s) or to further the unauthorized person's interests:

Factor B. Consider the unauthorized person who used or received the PHI. *(This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information - for example, is the person a covered entity required to comply with HIPAA, or a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.)*

Response to Breach and Security Incidents Policy #23

Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified):

Factor C. Consider whether the PHI was actually acquired or viewed. *(If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.)*

Describe whether the PHI was actually acquired or viewed (attach report from a computer forensic analyst, if one was obtained):

Factor D. Consider the extent to which the risk to the PHI has been mitigated — for example, as by obtaining the recipient’s satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) has been completely returned, or has been/will be destroyed. *(Hospitals should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results in terms of the risk to PHI. For example, a hospital may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)*

Describe risk mitigation steps taken:

Factor E. Describe any other relevant factors (write “none” if appropriate):

Based on the factors noted above, is there a low probability that the PHI has been compromised?

- Yes (there is a low probability), thus **No** breach reporting required under HIPAA.
- No (there is not a low probability; there is a higher probability) thus breach reporting is required under HIPAA.

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether reporting is required under federal law (HIPAA). State laws require notification of a breach as defined in state law regardless of the results of this risk assessment. (See “IV. State Law:

Response to Breach and Security Incidents Policy #23

Breach of Unencrypted Computerized Data in Any California Business” on page 12.2, and “V. State Law: Breach in a Licensed Health Care Facility” on page 12.4, for information regarding notification under state law.) A provider may also have reporting obligations pursuant to a business associate agreement or other contract.

Signature of person completing this form: _____

Title: _____

Date: _____

Response to Breach and Security Incidents Policy #23

CCHC HIE Individual Breach Notification Form

*To be printed on letterhead and filled out by CCHC SPO or designee
Used only if Breach involves the information of multiple Participating Organizations
Final Draft of Letter Must be Approved by all affected Participating Organizations*

To: Add Individual Name

Address: Add Individual's Address

Date:

RE: *Individual Breach Notice*

Dear _____,

We take the privacy and security of your information very seriously. Regrettably, we are writing to inform you of a breach of your Protected Health Information (PHI) [or Personal Information] contained in the Central Coast Health Connect (CCHC) Health Information Exchange (HIE).

Description of Occurrence:

Type of PHI (Protected Health Information) Involved:

Actions Taken & Undergoing to Investigate, Mitigate and Protect against any further Breaches:

Suggested Steps for Personal Protection:

[Please note that the steps for personal protection will be customized for each notification, depending on the nature and extent of information disclosed, and applicable federal and state regulatory requirements]

We recommend that you immediately take the following Fraud Alert steps outlined below.

1. Call one of the three major credit bureaus listed below to place a "Fraud Alert" on your credit report. This can help prevent anyone from opening additional accounts in your name. Once the credit bureau confirms your Fraud Alert, the other two credit bureaus will automatically place alerts on your credit report.
 - a. Equifax: 1-800-525-2685; www.equifax.com
 - b. Experian: 1-888-397-3742; www.experian.com
 - c. Transunion: 1-800-680-7289; www.transunion.com
2. Order your credit reports from all three bureaus. When you set up a Fraud Alert, you can also receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts or activities that are not yours.
3. Monitor your credit reports carefully. Even with Fraud Alerts on your credit bureau accounts, we recommend that you continue to monitor your credit reports to ensure no one has opened an account using your personal information.

Response to Breach and Security Incidents Policy #23

Again, we are committed to a thorough investigation of the breach of PHI. Our contact information is below for your reference as well.

For More Information at CCHC:

Add Telephone: _____

Add Email: _____

Add Address: _____

Add CCHC Website: _____

Sincerely,

[insert name, title and organization]

Firewall Policy #24

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is for CCHC to monitor data security protection and safeguards by its technology vendor with firm firewall capabilities to aid in prevention of breach of Protected Health Information (PHI) in CCHC HIE. As defined by the National Institute of Standards & Technology (NIST), “Firewalls are devices or a program that control the flow of network traffic between networks or hosts that employ differing security postures.” Attention to Firewall guidelines are also needed by CCHC’s Participating Organizations and Workforce to ensure Authorized Users have proper protection.

PROCEDURE

- I. CCHC Security & Privacy Officer or designee will check minimally on an annual basis, on its technology vendor’s Firewall specific policy and procedures to ensure safeguards are in place that follow guidelines from the National Institute of Standards & Technology (NIST) as highlighted below and/or security tenets proposed by the Health Insurance Portability and Accountability Act (HIPAA).
 - a. Firewall policies need to define how an organization’s firewalls will handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types.
 - b. Routine risk analysis should be conducted to develop a list of the types of traffic that must be secured—including which types of traffic can traverse a firewall under what circumstances.
 - c. Generally, all inbound and outbound traffic not expressly permitted by the firewall policy should be blocked. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the network.
- II. CCHC’s technology vendor, RelayHealth, ensures through vigilant adoption, implementation and monitoring of their firewall security measures to take all reasonable measures to secure data on its servers and in their data center. RelayHealth’s data center is both physically and electronically secured. Servers are isolated from the Internet by using a firewall which is both a hardware and software system that blocks access by unauthorized parties. Per RelayHealth’s Network Security plan specific to firewall safeguards:

Firewall Policy #24

- a. All production and staging activities are isolated within the datacenter. Customer integration environments are secured behind the firewall. Each environment has separate role-based access controls (RBAC).
 - b. RelayHealth uses redundant best-of-breed firewalls at various layers in the RelayHealth architecture to protect the network from the outside world. Access lists are used on the front-end routers to prevent any spoofing of internal IP addresses as well as to filter maligned packets and private network access attempts.
 - c. RelayHealth's highly restrictive firewall policy explicitly defines inbound traffic. Only a handful of IP addresses are exposed to the outside Internet. The redundant firewall configuration blocks all inbound network traffic except for filtered http, https, SMTP, SFTP and DNS traffic. All 'allow' rule sets are established on a per-server basis and are not used as global rules for all systems.
 - d. All RelayHealth security devices have redundancy. All dedicated firewalls are active fail-over clustered. The management VPN-Firewalls are active failover clustered and can maintain management access in the event of a single VPN server failure. Requisite authentication servers are configured in a high availability cluster to remove single points of failure.
- III. CCHC's Workforce and Participating Organizations shall ensure firewall protections safeguards are internally maintained and monitored and ensure any known disabling of protection hardware or software by Workforce members or Authorized Users are potential grounds for disciplinary action or User access suspension.

RESOURCES

- Reference - NIST SP 800-41, Guidelines on Firewalls and Firewall Policy
- Reference – 45 C.F.R. **§164.308(a)(5)(ii)(B)**
- **Reference – RelayHealth Network Security Plan**

Auto Release of Clinical Results Policy #25

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to establish the procedures and guidelines for Participating Organizations associated with CCHC HIE's waiting period as it pertains to automatic release of clinical data through its Patient Portal. The release of results through HIE's has been guided by regulations issued under the Clinical Laboratory Improvement Amendment (CLIA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and HIPAA mega rule of 2013 affecting radiologist, and Federal and State guidelines.

POLICY BACKGROUND

CCHC and its technology partner vendor RelayHealth have adopted Health Insurance Portability and Accountability Act (HIPAA) privacy rule safeguards to exchange secure healthcare information through CCHC HIE's patient-physician communications patient portal solution. Physicians may deliver diagnostic results, preventive care advice and other healthcare information securely to their patient's through this tool.

In an effort to support the sensitive nature of Clinical data initial communication, CCHC has adopted policy standards to ensure there is an automatic "delay" in CCHC HIE posting of Clinical data (i.e., laboratory tests, radiology images and transcribed reports), for both abnormal and normal readings to allow Physician's adequate time to communicate directly first with their patients before results are posted in the Patient Portal.

PROCEDURE

- I. CCHC Security and Privacy Officer or Designee shall provide review to newly contracted Participating Organizations to ensure the waiting period triggers within CCHC HIE for Clinical data release protocols are clear. Participating Organizations shall be responsible for developing adequate Patient and Provider education materials on the Use and Disclosure of Clinical data.
- II. CCHC HIE's contracted entities shall adhere to the system set-up protocols for Clinical data as follows:
 - a. All Participating Organizations may choose to auto release "normal" or "abnormal" clinical results to a Patient via CCHC HIE immediately upon receipt of result (i.e. zero day delay) but must release the result no later than a seven (7) day delay.
 - b. All Participating Organizations must exclude Sensitive Health Information (SHI) from auto-releasing to the patient's online record (i.e. the patient's view), per CCHC Policy #28 Sensitive Health Information.

Auto Release of Clinical Results Policy #25

- III. CCHC Participating Organizations shall also adhere to electronic posting restrictions outlined in CCHC's Sensitive Health Information Policy as well as California law explicit prohibition against sharing the following test results electronically with a patient:
- a. HIV antibody tests,
 - b. Tests indicating a presence of antigens indicating a hepatitis infection,
 - c. Toxicology results documenting the abuse use of drugs,
 - d. Test results relating to routinely processed tissues, including skin biopsies, Pap smear tests and other cytology, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy,
 - e. Any information specifically relating to the patient's participation in outpatient treatment with a psychotherapist, specifically psychotherapy notes, and
 - f. Any information that discloses results of at test for a genetic characteristic or provides identifying characteristics of the person to whom the test results apply.

RESOURCES

- Reference – 42 CFR 493, 45 CFR Part 164, 42 CFR 496.6 (k)(i)
- Reference – California Health and Safety Code, Section 123148
- Reference – California Health and Safety Code, Section 123148 (f)
- Reference – 78 FR 14793
- Reference – CCHC Policy # 32 Sensitive Health Information Policy

Minimum Necessary Policy #26

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure that limited use, disclosure and restrictions of information requests of Protected Health Information (PHI) by all CCHC Workforce members and other contracted Users is available to the minimum amount of information necessary to accomplish their job duties or intended purpose of such information.

POLICY DETAILS

I. Policy Background

- a. "Minimum Necessary" is founded from the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Privacy Rules set forth at 45 C.F.R. Part 164.502 (b). The concept of Minimum Necessary is that when requesting, using, or disclosing PHI, a Covered Entity under HIPAA or a Business Associate must make reasonable efforts to limit the amount of PHI to the Minimum Necessary to accomplish the intended purpose. Compliance is applicable to CCHC's HIE and its Participating Organizations.
- b. The Minimum Necessary rule should work in tandem with CCHC's User Authorization procedures and defined role based access security controls within the HIE. Workforce members and Participating organizations may be limited in their access to PHI to the Minimum Necessary based upon their role and the need of said data within their job functions or duties.

II. Uses

- a. CCHC will identify:
 - i. The persons or classes of persons in its Workforce who need access to PHI to carry out their job functions and/or duties;
 - ii. The categories or types of PHI needed; and
 - iii. The conditions appropriate to such access.
- b. Workforce members' access to PHI shall be solely on a "need to know" basis.
- c. Workforce members' use or disclosure of PHI shall be limited to that PHI needed to perform job responsibilities and duties.

III. Non-Routine Requests and Disclosures

- a. Non-routine requests for, and disclosures of, PHI shall be reviewed by the CCHC Privacy Officer, individually, or by his/her designee. CCHC shall develop and implement criteria designed to limit its requests for PHI to the minimum necessary to satisfy the request of the intended purpose.

Minimum Necessary Policy #26

- b. CCHC shall rely on a Participant's request for PHI as the minimum necessary for the intended disclosure. Additionally, should a Participating Organization submit an inquiry for the permissible purpose of treatment or *emergency* treatment, a Participating Organization will not be subject to the Minimum Necessary rule.
 - c. Disclosures by Workforce Members or Participating Organizations shall contain the minimum amount of PHI as necessary for the intended purpose of the disclosure.
- IV. **Information Systems.** All information systems will be designed, in accordance with CCHC's available resources, to meet the minimum necessary provisions of HIPAA. This is to be accomplished by removing identifiers and removing data fields not necessary to performing the primary purpose of the use or disclosure.

PROCEDURE

- I. The CCHC Security & Privacy Officer or designee will determine Workforce member access to PHI based on job duties and/or functions and will document in the individual's personnel file. Determination of access will be based on:
 - a. Employees or classes of employees who need access to PHI to carry out their daily functions.
 - b. For each class of employee, the category or categories of PHI to which access is needed.
- II. In general, PHI used internally at CCHC may be used by CCHC personnel to facilitate exchange of information between Participants for treatment, payment or other healthcare operations of CCHC Participants. PHI may not be released outside of CCHC unless it is to:
 - a. A Business Associate with whom CCHC has a Business Associate Agreement or a Participant of the CCHC HIE via the HIE Participation Agreement; or
 - b. As otherwise may be required by law.

RESOURCE

Opt-Out Policy #27

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to describe how individuals will be informed on the uses and disclosure of Protected Health Information (PHI) through CCHC's HIE and how they have the ability to change their participation status (i.e., Opt-Out or Opt Back-In).

PROCEDURE

- I. CCHC HIE is structured to automatically include all PHI provided by contracted Participating Organizations unless an individual requests to Opt-Out. After Opting-Out, an individual may also request to Opt Back-In at any time into CCHC HIE, thus allowing inclusion of their PHI.
- II. If an individual elects to Opt-Out of CCHC HIE, PHI will not be shared except to the ordering Provider. Limited information that is required to be reported to healthcare providers under the law will continue to be directly transmitted to the required recipient in accordance with any mandatory Federal or State laws or regulations.
- III. Participating Organizations are required to educate and inform individuals of the use and disclosures of PHI within CCHC HIE and the ability for an individual to choose, at any time, to Opt-Out.
- IV. Participating Organizations shall make good faith efforts to educate all individuals in advance or at time of registration of the use and disclosure of PHI and Opt-Out or Opt Back-In protocols.
 - a. CCHC will provide Participating Organizations sample template Patient Education and Opt-Forms to model and/or use (see attached Appendix) as well as CCHC Workforce will maintain these materials on the CCHC main website.
 - b. Participating Organizations are encouraged to create education and Opt-Out materials in both English and Spanish.
 - c. Participating Organizations may customize the Patient Education or informational materials as long as CCHC Workforce reviews in advance for input and approval and CCHC does not incur any liabilities as result of modifications.
 - d. Participating Organizations shall include provide information about individuals' participation in CCHC HIE in their Notice of Privacy Practices.
 - e. Participating Organizations shall ensure to the individual that election to Opt-Out does not hinder any provision of care or coverage, meaning that a Participating Organization will not withhold care or coverage from an individual based on election to Opt-Out of CCHC HIE.
- V. Should an individual decide to Opt-Out there are various methods to make the necessary request. Individuals may request the Opt-Out form from their Participating Organization,

Opt-Out Policy #27

- contact CCHC directly by help desk phone or email via CCHC's website.
- a. Once CCHC Workforce receives the Opt-Out form, facilitation may take up to five (5) business days to complete.
 - i. CCHC Workforce shall notify the individual that the Opt-Out task is complete if an email address has been provided; in all other cases, CCHC will notify the Participating Organization who shall notify the individual in writing that the change in the individual's participation has been processed.
 - b. In the event an individual calls CCHC's help support number directly for Opt-Out assistance, CCHC Workforce will implement verification protocols to ensure individual authentication before proceeding with Opt-Out.
 - c. In situations when an individual does not present at registration physically, such as when a lab is sent by courier, the Participating Organization shall mail a hard copy of the patient education materials. If the mail is returned to sender (i.e., due to a bad address), then the Participating Organization shall send Opt-Out requests for those individuals to CCHC since education information was undeliverable.
 - d. Should an individual who has Opted-Out, elect to Opt Back-In, then the individual may contact the Participating Organization or CCHC Workforce by mail or email for consideration and processing.
- VI. Individuals cannot Opt-Out of disclosures for public health activities, except as provided by applicable laws and individuals may not Opt-Out of other disclosures required by law (i.e., court orders).
- VII. CCHC Workforce will keep all Opt-Out and Opt Back-In documentation for seven (7) years.

RESOURCES

- Reference - 45 C.F.R. §§ 164.506(b), 164.522(a), and 164.524
- Reference - California's Confidentiality of Medical Information Act (CMIA—Cal. Civ. Code §§ 56 et. seq.)
- Appendix Reference – CCHC Opt Out Patient Education Materials Appendix Reference
- Appendix Reference – CCHC Opt Out Form
- Appendix Reference – CCHC Website Instructions to Opt-Out

Opt-Out Policy #27

Appendix – CCHC Opt Out Patient Education Materials

Your Guide to Understanding Central Coast Health Connect

A Health Information Exchange for Monterey County

What is Central Coast Health Connect (CCHC)?

CCHC is a community health information exchange (HIE), a system established to help patients and healthcare providers securely share health information electronically. An HIE helps to ensure that only you and the caregivers you authorize — including doctors, hospitals, and labs — have secure, instant access to vital medical information necessary to provide you the best care possible.

Why is it important to participate in CCHC?

Many people see multiple care providers, often in separate locations. The information about their care, such as doctors' office visits, prescriptions, lab tests, and imaging, historically has also been kept separate. That fragmentation can lead to unnecessary duplication of services and increased safety risks. To increase safety, efficiency, and collaboration, leading-edge organizations are implementing health information exchanges to link patients and their care providers and close the information gaps. When you and your healthcare providers participate in CCHC, your healthcare teams can securely access and share pertinent medical information, enhancing their ability to make the best decisions for your care.

How is my information secure?

Protecting privacy is a top priority in the CCHC system. Access to patient data is strictly regulated and state and federal privacy laws and policies are strictly followed and enforced. CCHC understands that patient privacy is essential, and we make every effort to ensure patient data is securely managed.

What if I don't want to participate in CCHC?

If you don't want to participate in CCHC, you may choose to opt out. It is also important to understand that **opting out prevents the sharing of your information through CCHC between providers**. If they choose, your doctor and other care providers will still be able to use the electronic health information exchange to have your lab results, radiology reports, and other data sent directly to them; previously, they may have received this information by fax, mail, or other electronic communication.

If you still choose to opt out, please e-mail cchc-help@centralcoasthealthconnect.org or call (831) 644-7494 to leave a message and a staff member will contact you.

To learn more about Central Coast Health Connect, please call (831) 644-7494 or visit www.CentralCoastHealthConnect.org and click on the link on the bottom of the page.

Appendix – CCHC Website Instructions to Opt-Out

Opt-Out Policy #27

What if I don't want to participate in CCHC?

If you don't want to participate in CCHC, you may choose to opt out. It is important to understand that opting out prevents the sharing of your information through CCHC between providers.

Please note, your doctors and other care providers will still be able to use the electronic health information exchange to have lab results, radiology reports, and other data sent directly to them if they are the ordering or participating provider; previously, they may have received this information by fax, mail, or other electronic communication.

If you still choose to opt out, please download the below form, fill out, sign and send according to the instructions on the document. If you have any questions please leave a voice mail at (831) 644-7494, a representative will return your call. You may also email cchc-help@centralcoasthealthconnect.org.

Opt-Out Policy #27

Appendix - CCHC Opt Out Form

This form is for patients who do not wish to participate in Community Hospital of the Monterey Peninsula's electronic health information exchange, known as Central Coast Health Connect (CCHC).

A health information exchange (HIE) is a way of sharing your health information among participating doctors' offices, hospitals, labs, radiology centers, and other healthcare providers through secure, electronic means. This gives participating caregivers the most recent information available from your other caregivers when they are making decisions about your care. If you opt out of participating in CCHC, your doctor and other care providers will still be able to use the system to have your lab results, radiology reports, and other data sent to them; previously, they may have received this information by fax, mail, or other electronic communication. Choosing to opt out only restricts the sharing of information between providers. When applicable, in accordance with laws, the required reporting of infectious diseases to public health officials will also occur through the HIE, even if you opt out.

To opt out of HIE complete this form; it is not necessary to complete a form for each provider. If you do not live in Monterey County, but still receive care in Monterey County, you should complete this form to opt out. If you wish to reverse your decision, you may opt back in at any time by calling (831) 644-7494. Please note: Opt-out requests will be processed within (5) business days.

Mail signed and completed form to: CCHC Administrator, 10 Ragsdale Drive, Suite 102, Monterey, CA 93940
Or scan and e-mail signed form to cchc-help@centralcoasthealthconnect.org or fax to (831) 644-7451.

INFORMATION OF PATIENT OPTING OUT (please print clearly)

Hospital Name _____
 Patient Name _____
 Address _____ City _____ State _____ Zip Code _____
 Primary Phone Number _____ Secondary Phone Number _____
 E-mail Address _____
 Date of Birth _____ Sex: Male or Female _____
 Reason for opting out (optional) _____

If this form is signed by someone other than the person above, the person signing the form hereby certifies that he/she is acting as:
 Parent _____ Legal Guardian _____ Other (specify relationship) _____

Contact information for individual completing this form if other than patient:
 Printed Name _____ Phone Number _____
 Patient Information _____
 Printed Name _____
 Signature _____ Date _____

Sensitive Health Information Policy #28

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to require compliance with certain categories of Protected Health Information (PHI) referred to as Sensitive Health Information (SHI) that is protected from routine disclosure through CCHC HIE and requires patient consent. Sensitive Health Information shall comply with use, disclosure, authorization and confidentiality requirements defined by Federal and State laws and regulations.

POLICY DETAIL

- I. Federal and State laws outline Security and Privacy requirements regarding disclosures of certain categories of Protected Health Information (PHI) that might be considered private or sensitive to a Patient. These particular laws are intended to ensure Patient confidence and require firm compliance. This higher level PHI is referred to as Sensitive Health Information (SHI). Depending upon the Permissible Purpose for which SHI is being inquired, the law may require that a Patient authorize, in writing the release of SHI specifics. SHI that requires written authorized Patient release will not be disclosed through CCHC HIE.
- II. Per the Department of Health and Human Services Federal Register Vol. 79, No. 25 and its Final Rule dated 2/6/2014, the stated amendment to the Clinical Laboratory Improvement Amendment (CLIA) of 1988, CCHC recognizes the following:
 - a. Upon the request of a patient, laboratories subject to CLIA may provide the patient with completed test reports.
 - b. Laboratories have 30 days to comply with the patient request.
 - c. The Final Rule does not differentiate 'Sensitive' versus 'non-Sensitive' test results.
 - d. There are limited exceptions where a licensed health care professional (HCP) has determined that access requested is likely to endanger the life or physical safety of the individual or another person.
 - e. This Final Rule 'preempts' more restrictive state laws.
- III. Per California Health and Safety Code 123148, CCHC recognizes the following categories as Sensitive Health Information:
 - a. HIV antibody tests,
 - b. Tests indicating a presence of antigens indicating a hepatitis infection,
 - c. Toxicology results documenting the abuse use of drugs, and
 - d. Test results relating to routinely processed tissues, including skin biopsies, Pap smear tests and other cytology, products of conception, and bone marrow aspirations for morphological evaluation (if they reveal a malignancy).

Sensitive Health Information Policy #28

- IV. Per California Civil Code 56.104, CCHC also recognizes the following as Sensitive Health Information:
 - a. Any information specifically relating to the patient's participation in outpatient treatment with a psychotherapist, specifically psychotherapy notes
- V. Per California Civil Code 56.17, CCHC also recognizes the following as Sensitive Health Information:
 - a. Any information that discloses results of at test for a genetic characteristic or provides identifying characteristics of the person to whom the test results apply.
- VI. Per California Welfare & Institutions Code Section 5328, CCHC also recognizes the following as Sensitive Health Information:

All information and records obtained in the course of providing services under Division 4 (commencing with Section 4000), Division 4.1 (commencing with Section 4400), Division 4.5 (commencing with Section 4500), Division 5 (commencing with Section 5000), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7100) of the Lanterman-Petris-Short Act, to either voluntary or involuntary recipients of services.

PROCEDURE

- I. Participating Organizations (POs):
 - a. POs shall exclude the following information from being 'auto-released' to the patient's online record (i.e. released to the patient's view on the patient portal) see CCHC Policy #25 on Auto Releasing of Clinical Results for additional information:
 - i. HIV antibody tests,
 - ii. Tests indicating a presence of antigens indicating a hepatitis infection,
 - iii. Toxicology results documenting the abuse use of drugs,
 - iv. Test results relating to routinely processed tissues, including skin biopsies, Pap smear tests and other cytology, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy,
 - v. Any information specifically relating to the patient's participation in outpatient treatment with a psychotherapist, specifically psychotherapy notes, and
 - vi. Any information that discloses results of at test for a genetic characteristic or provides identifying characteristics of the person to whom the test results apply.
 - b. The above list of Sensitive Health Information is a minimum requirement. It is acceptable for Data Providers, who may find it necessary or legally required to do so, to exclude additional data.
- II. CCHC:
 - a. CCHC will share SHI in response to an Inquiry from a PO only if the Patient has elected not to Opt-Out, and it is for a Permissible Purpose that is authorized by law without a Patient's signed authorization.

Sensitive Health Information Policy #28

- b. Any disclosure of SHI through the HIE must also provide a written warning that prohibits re-disclosure of the SHI by the receiving organization except as maybe authorized by law.

RESOURCES

- Reference – CCHC Policy #25 Auto-Release of Clinical Results
- Reference - California Civil Code 56.104
- Reference - California Health and Safety Code 123148
- Reference - California Civil Code 56.17
- Reference - Department of Health and Human Services Federal Register Vol. 79, No. 25

Patient Consent and Permissible Uses Policy #29

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to define the Permissible Purposes for which Protected Health Information (PHI) may be disclosed through the HIE from one Participating Organization to another. Without a Permissible Purpose, no authorization for information exchange will be permitted. Additionally, the policy's purpose is to enhance Patient and Provider confidence in the overall exchange process, and minimize potential for misuse of PHI, by establishing clear definitions and appropriate access and disclosure limits on what constitutes Permissible Purpose.

POLICY DETAILS

- I. As guided by the Office of the National Coordinator for Health Information Technology there is the strong need for appropriate limits on the collection, use and disclosure of PHI by CCHC HIE. CCHC shall establish limitations with Participating Organizations to ensure the PHI will only be disclosed for a Permissible Purpose.
- II. Permissible Purposes for which PHI may currently be disclosed through CCHC HIE are as follows:
 - a. Treatment
 - b. Payment Activities
 - c. Healthcare operations
 - d. Emergency Treatment
 - e. Public Health Reporting
- III. The scope of each of these Permissible Purposes under CCHC HIE is defined below.
 - a. **Treatment:** The Permissible Purpose of Treatment allows the exchange of PHI from one Participating Organization through the HIE in response to an inquiry from another Participating Organization. Treatment means the provision of health care items or services to a Patient. The provision of health care items or services may include direct Patient care as well as the consultation, coordination, management, or referral of a Patient between or from one Participating Organization to another. Treatment shall be limited to the provision of health care items or services to the Patient who is the subject of the information (except in the case of mother/infant). A disclosure for the Permissible Purpose of Treatment may occur through the HIE only if the Patient has not elected to Opt-Out.
 - b. **Payment Activities:** The Permissible Purpose of Payment Activities allows the exchange of PHI to support a claim for reimbursement submitted by a health care provider to a health plan.

Patient Consent and Permissible Uses Policy #29

- c. Healthcare Operations: The Permissible Purpose of Healthcare operations allows the exchange of PHI to from the HIE to the Participating Organization to support the health care operations of that Participating Organization.
- d. Emergency Treatment: The Permissible Purpose of Emergency Treatment allows for the exchange of PHI from one Participating Organization through the HIE in response to an inquiry from another Participating Organization. Emergency Treatment means the provision of health care items or services to a Patient suffering from a condition which poses an immediate threat to the health of the Patient (for example, death or serious impairment to one or more bodily systems, organs, or parts) and which requires immediate medical intervention. Emergency Treatment is a distinct subset of Treatment. A disclosure of the Permissible Purpose of Emergency Treatment may occur through CCHC HIE only if the Patient has not elected to Opt-Out.
- e. Public Health Reporting: The Permissible Purpose of Public Health Reporting allows for the exchange of PHI from a Participating Organization to a state or federal agency through the HIE for the reporting and surveillance of specific health conditions identified under and required or authorized by state or federal law, and for the reporting of immunization data. All reports for the Permissible Purpose of Public Health Reporting must comply with the requirements established by the agency that receives the report. Such reporting must contain only the Minimum Necessary of PHI as authorized for the specific reporting purpose. A disclosure for the Permissible Purpose of Public Health Reporting may be undertaken regardless of whether a Patient decides to Opt-Out of CCHC HIE.

PROCEDURE

- I. Patient
 - a. A Patient who has not Opted-Out shall be deemed to have given his/her consent to participate in CCHC HIE, and his/her PHI may be exchanged for the Permissible Purposes of Treatment, Emergency Treatment and Public Health Reporting.
 - b. The PHI of a Patient who has Opted-Out of CCHC HIE shall not be exchanged for any Permissible Purposes except for Public Health Reporting. However, PHI will still be sent to and viewable by anyone who ordered, dictated or was copied on the Patient's result and/or report for any Permissible Purposes except Public Health Reporting.
- II. Participating Organization
 - a. Each inquiry seeking a Patient's PHI through CCHC HIE must be limited to Permissible Purposes. All inquiries must be submitted electronically.
 - b. When submitting an inquiry, a Participating Organization must certify electronically to CCHC HIE that it has an existing Treatment relationship to the Patient sufficient to justify the Permissible Purpose of Treatment or Emergency Treatment.
 - c. Any PHI obtained as a result of said inquiry must be used only for the Permissible Purpose for which it was intended and be limited to the PHI of the Patient who is the subject of the inquiry (except in the case of mother/infant).

Patient Consent and Permissible Uses Policy #29

- d. Participating Organizations seeking the exchange of Sensitive Health Information must comply with CCHC Sensitive Health Information Policy and Procedures and as needed, must obtain the specific written consent of the Patient.
- III. CCHC
- a. If a Patient has not Opted-Out, CCHC HIE will share PHI in response to an inquiry from a Participating Organization once electronic certification that an existing treatment relationship to the Patient sufficient to justify the Permissible Purposes of Treatment or Emergency Treatment has been received by CCHC.
- b. CCHC requires all inquiries for the exchange of Sensitive Health Information are in compliance with the Sensitive Health Information policies and procedures.
- c. CCHC may determine to de-identify PHI, and may use said de-identified data for any public health or research purpose approved by the CCHC Executive Committee.
- d. Nothing stated in this policy or procedure will preclude CCHC from using and disclosing PHI as necessary to permit the ongoing operation, maintenance and repair of its HIE, provided, that third party vendors involved in operation, maintenance and repair must enter into a Model Modular Participant Agreement with CCHC. The purpose of this provision is to ensure that CCHC may undertake uses and disclosures necessary to establish and maintain connectivity with Participating Organizations, and to perform necessary repair functions.
- e. PHI may not be used or disclosed for marketing purposes without the prior written consent of an affected Patient.

RESOURCES

- Reference – 45 C.F.R § 160-163
- Reference – 45 C.F.R § 164.506
- Reference – California Civil Code § 56, et seq.
- Reference – California Civil Code Sections 1798.29 and 1798.82
- Reference – CCHC Sensitive Health Information Policy

Data Exchange Between HIO to HIO Policy #30

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure that Health Information Organizations (HIOs) external to CCHC and its participants, with which CCHC will be exchanging Personal Health Information (PHI) adhere to similar policies and procedures, have similar safeguards in place – technical, administrative, and otherwise – to ensure that information and the exchange of information is occurring in a secure and safe environment with appropriate protocols in place.

POLICY DETAILS

- I. CCHC and the Health Information Organization agree to follow and adhere to all federal and state laws applicable to the governance and protection of Protected Health Information (PHI).
- II. CCHC and the external HIE agree not to use PHI for purposes of marketing.
- III. The burden of safely and securely providing and accessing this PHI is the equal burden of CCHC and the HIO external to CCHC. Therefore both CCHC and the external HIO share in this responsibility of ensuring security of patient information, equally.
- IV. CCHC and the external HIO will conform to current and generally accepted industry-wide standards and practices relating to meeting privacy and security regulations.
- V. CCHC and the external HIO will maintain sufficient standards and safeguards and ensure that proper procedures are in place to ensure that the security and privacy of patient health care information is maintained whether this data is received through CCHC, the external HIO, or any other HIO that either organization will be exchanging patient health information.
- VI. Both CCHC and the external HIOs may be participating on or signatories to HealtheWay, the Data Use Reciprocal Support Agreement (DURSA), the California Enhanced DURSA (CAE-DURSA), the National Association for Trusted Exchange (NATE), or similar certifying agency(ies) or their successor organizations.
- VII. Any modifications made by HealtheWay, the Data Use Reciprocal Support Agreement (DURSA), the California Enhanced DURSA (CAE-DURSA), the National Association for Trusted Exchange (NATE), or similar certifying agency(ies) or their successor organizations that will result either in CCHC or the external HIO to become non-compliant, partially-compliant, or any other status other than fully compliant with these respective certifying organizations may, depending on the modifications made, result in the immediate cessation of access and exchange of patient information between CCHC and the external HIO.
- VIII. CCHC and the external HIO will execute an agreement to share information.

Data Exchange Between HIO to HIO Policy #30

- IX. No fees will be charged by CCHC to the external HIO for providing patient health care information contained within the CCHC HIE.
- X. No fees will be charged by the external HIO to CCHC for accesses patient health care information contained within the external HIO's HIE.
- XI. Audit logs must be maintained by CCHC and the external HIO.
- XII. Audit logs must be made available for viewing and reporting purposes within (7) days upon written request by either CCHC or the external HIO.
- XIII. CCHC shall not access or provide access to a patient's Protected Health Information if the patient has opt-ed out or revoked their consent authorizing CCHC or the external HIE to access such Protected Health Information.
- XIV. Consent shall not be required for CCHC or the external HIO to access Protected Health Information provided that:
 - a. CCHC and the external HIO comply with existing federal and state laws and regulations requiring patient consent for emergencies, or
 - b. CCHC or the external HIO have an opt-out policy for patient participation on the HIE, therefore, by default the patient information is accessible, unless specific access is denied by the patient to access their data through the appropriate opt-out process currently in place by CCHC or the external HIO.
- XV. If CCHC or the external HIO is permitted to disclose Protected Health Information to a government agency for purposes of public health reporting, including monitoring disease trends, conducting outbreak investigations, responding to public health emergencies, assessing the comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms, without patient consent under applicable state and federal laws and regulations, either CCHC or the external HIO may make that disclosure on behalf of the Data Supplier without Consent.
- XVI. CCHC will maintain an active Business Association Agreement (BAA) between CCHC and the external HIO.
- XVII. CCHC and the external HIO shall not make Protected Health Information available to anyone other than the specified recipient. For example in the case of a Pilot:
 - a. This information will not be made available on any Patient Portal
 - b. No de-identification of patient information will be allowed and then used within the HIE
- XVIII. CCHC and the external HIO shall use best efforts to ensure appropriate security is in place to protect Protected Health Information.
- XIX. CCHC and the external HIO shall make access to Patient Information available only to their own internal Data Users and their respective Authorized Users, and only for purposes of treatment, healthcare operations and payment, as defined under the HIPAA Rules, of an individual with whom the Participant has a provider-patient relationship.

PROCEDURE

- I. CCHC and the external HIO will perform due diligence and ensuring that each has in place:
 - a. Adequate safeguards to ensure privacy and security of PHI
 - b. Has been accredited by the requisite preferred certifying agency:
 - i. NATE – National Association for Trusted Exchange

Data Exchange Between HIO to HIO Policy #30

- ii. HealtheWay
 - iii. CAHIE – California Association of Health Information Exchange
 - c. Has adequate and compliant Policies & Procedures in place
 - d. Has adequate and compliant Data Exchange Agreements in place with appropriate participants
 - e. Has never had a breach of PHI in its own HIE
- II. CCHC and the external HIO have appropriate Data Sharing agreement in place between the two organizations
- III. CCHC and/or its agents to conduct annual audit of the external HIO

RESOURCES

Data Exchange Between HIO to Data Participant Policy #31

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure that providers or provider organizations participating on the CCHC Health Information Exchange (HIE) adhere equally to all guidelines, policies and procedures needed to securely exchange patient health information and to be able to access this information in an equally secure environment.

POLICY DETAILS

- I. CCHC and the Provider or Provider Organization, agree to follow and adhere to all federal and state laws applicable to the governance and protection of Patient Health Information (PHI).
- II. The burden of safely and securely providing and accessing this PHI is the equal burden of the data provider and the data user. Therefore both CCHC and the Data Participant share in this responsibility of ensuring security of patient information, equally.
- III. CCHC and the Data Participant agree to execute and maintain an active HIE Participant Agreement between CCHC and the Data Participant.
- IV. CCHC may enter into agreements with other HIOs to provide, exchange, or access another Health Information Exchange. Therefore the same burden of ensuring security of IT infrastructure environment is shared equally between CCHC and the Data Participant.
- V. CCHC will maintain an active Business Associate Agreement between CCHC and any Data Participant on CCHC's HIE.
- VI. CCHC shall make access to Patient Information available only to Data Participants and their respective Authorized Users, and only for purposes of treatment, healthcare operations and payment, as defined under the HIPAA Rules, of an individual with whom the Participant has a provider-patient relationship.
 - a. Without limiting the foregoing, CCHC 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.
- VII. CCHC may make Access to Patient Information available to the operators and/or users of other HIO's or Private Health Information Exchanges to the extent CCHC determines appropriate to permit such users to Access that information for the purpose of treatment, as defined in the HIPAA Rules, of an individual with whom each such user has a provider-patient relationship. Based on the information provided by the Participant.

Data Exchange Between HIO to Data Participant Policy #31

- VIII. Based on the information provided by the Participant CCHC shall issue a User Name and Password (and/or other security measures) to each Authorized User that shall permit the Authorized User to access the Services of CCHC.
- a. CCHC, or its Agent, shall provide each user name and password (and/or other security measures) to the Data Participant and the Data Participant shall be responsible to communicate that information to the appropriate Authorized User.
 - b. Removal of an Authorized User will be centralized via CCHC's termination policy and procedures.
 - c. Each Data Participant will provide CCHC or its Agent with a list identifying all of the Participant's Authorized Users. At the time that a Participant identifies an Authorized User to CCHC's HIE the Data Participants will also certify that the Authorized User:
 - i. Has completed a training program conducted by CCHC or its Agent, the Data Participant, and the Authorized User,
 - ii. Will be permitted by Participant to use the Services of CCHC only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered, and
 - iii. Has acknowledged in writing that failure to comply with the Terms and Conditions of Use of the HIE may result in the withdrawal of privileges to use the Services of CCHC and may constitute cause for disciplinary action by and of the Data Participant.
- IX. Data Participant shall maintain sufficient safeguards and procedures to maintain the Security and Privacy of Data received through the HIE.
- X. The Data 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 the Participant's Data Exchange Participation Agreement or similar agreement or CCHC's Policies and Procedures.
- a. This responsibility of omission is carried over to the Data Participant's employees, contractors, agents and any other parties who access or use the HIE.
- XI. The Data Participant shall provide or arrange for appropriate training in the use of the HIE.
- XII. The Data Participant shall provide or arrange for appropriate training and the requirements of the Standard Terms and Conditions for all the Data Participant's Authorized Users.
- XIII. Without limiting the generality of the foregoing, the Data Participant shall inform its Authorized Users of the applicable terms and conditions of its Data Exchange Participation Agreements and these Policies and Procedures, 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.
- XIV. The Data Participant shall designate a single individual who shall be responsible for managing communications between the Participant and CCHC.
- XV. In connection with the Data Participant's participation on the HIE, the Data Participant shall maintain a Designated Lead for its participation in the HIE.
- XVI. The Data Participant shall be solely responsible for obtaining, installing and maintaining, at the Data Participant's expense, the Data Participant's Prerequisite Systems to access the HIE.

Data Exchange Between HIO to Data Participant Policy #31

- XVII. CCHC shall not be responsible for the Data Participant's inability to Access or Use the HIE if that inability is for any reason other than the HIE's failure to comply with the specifications therefore set forth or failure to perform its obligations under the applicable Model Modular Participant Agreement, including without limitation any factors arising from the Data Participant's computing environment, software, interfaces, or hardware, or any upgrade or alteration..
- XVIII. The Data Participant shall be solely responsible for the control and protection of all data stored within the Data Participant's firewall, including without limitation Patient Information, and for the Data Participant's compliance with all laws and applicable regulations.
- XIX. The Data Participant shall exercise reasonable care to assure that the Patient Information to which the Data Participant provides access pursuant to its participation in the HIE is correct, accurate, free from serious error and reasonably complete and provided in a timely manner and that the necessary consent has been obtained.
- XX. The Data Participant shall, within as soon as reasonably possible, notify CCHC or its Agent of any Patient Information to which the Data Participant has provided access that the Data Participant determines is corrupt, incomplete, erroneous or otherwise incorrect, or which is otherwise inappropriate for availability through the HIE.
- a. CCHC will then take, as per the direction of the Data Participant, any and all means necessary to remove data that is corrupt, incomplete, erroneous or otherwise incorrect, or which is otherwise inappropriate for availability through the HIE.
- XXI. Without limiting any other provision of the Data Provider's Participation Agreement, the Data Participant shall not:
- a. allow to be transmitted to the HIE 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;
- b. knowingly allow to be transmitted to the HIE any information or software that contains a virus, Cancelbot, Trojan horse, worm or other harmful component; or
- c. knowingly allow to be transmitted to CCHC's HIE any information that violates the proprietary rights, privacy rights, or any other rights of a third party, including without limitation any patient.
- d. If such instances were to occur, CCHC is to be immediately notified by the Data Participant and any and all damage resulting from this act will be the liability of the Data Participant.
- XXII. The Data Participant shall not release any of the following to the patient's online record (i.e. for patient's viewing) that contains (Reference Policy #32 Sensitive Health Information):
- a. HIV antibody Tests
- b. Tests indicating a presence of antigens indicating a hepatitis infection
- c. Toxicology results documenting the abuse use of drugs
- d. Test results relating to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy

Data Exchange Between HIO to Data Participant Policy #31

- e. Any information specifically relating to the patient’s participation in outpatient treatment with a psychotherapist, specifically psychotherapy notes
 - f. Any information that discloses results of at test for a genetic characteristic or provides identifying characteristics of the person to whom the test results apply.
- XXIII. The Data Participant shall take reasonable steps to ensure that the Patient Information that the Data Provider makes available through the HIE is
- a. accurate and does not violate any intellectual property rights, privacy rights, or other rights of any third party,
 - b. not unlawful, libelous, defamatory, or otherwise objectionable,
 - c. not in violation of any local, state or federal law or regulation, and
 - d. prudent in that it owns or has obtained all necessary rights in the Patient Information, and consents for its use and disclosure by the Data Provider, so that its use by CCHC or other Participants does not violate any intellectual property rights, privacy rights, or other rights of a patient or other third party.
- XXIV. The Data Participant shall notify CCHC of any breach notifications that the Data Participant is required to report to comply with applicable state and federal law when the breach may include data under the control of the HIO such as when an unauthorized-user has access PHI in transport.
- XXV. The Data Participant shall use its best efforts to ensure that any of its Authorized End Users (in the role of sender or receiver) will no longer share or acquire data through the HIO in the event of the termination of its Participant Agreement with the HIO.

PROCEDURE

- I. The Data Participant shall execute the HIE Participation Agreement before any services can be provided and provide to CCHC, two original signed signatures of the agreement:
 - a. One original signed agreement for CCHC’s files
 - b. One original signed agreement for the Data Participant
- II. The Data Participant will provide an updated list of Authorized Users in writing to CCHC or its Agent 30-days prior to any Go-Live so that CCHC or its Agent can create the request for access credentials.
- III. Any changes to the Authorized Users (i.e. termination or new employees) must require the completion of the CCHC Authorized User Change Request Form and any additions/deletions and requisite information provided on this form.
 - a. It is the responsibility of the Data Participant to provide CCHC or its Agent with any additions/deletions to the list of Authorized Users within 10 business days of any effective date.
 - b. Data Participant and their authorized Users shall review training materials on how to access and use the HIE.

RESOURCES

- Reference: CCHC HIE Portal Access Policy
- Reference: CCHC HIE Access Termination Policy

Data Exchange Between HIO to Data Provider Policy #32

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure that any Data Provider of information into the CCHC HIE follows guidelines set forth to ensure that the methodology of providing the patient information is done securely and safely to ensure the data integrity and to avoid or limit the possibility of any intrusions.

PROCEDURE

- I. The authorized End User in the role of the Data Provider shall comply with all applicable federal and state laws and regulations.
- II. The HIO shall ensure that all exchange is completed in a secure and safe environment following standards, procedures and guidelines as necessary and recommended to ensure and significantly reduce and eliminate any possible breach.
- III. The Data Provider will participate in the Program in accordance with the terms and conditions of the HIE Participation Agreement and CCHC's Policies and Procedures.
- IV. Any lapses, discrepancies or recommendations communicated to the Data Provider will be in writing, signed by the Data Provider and CCHC's Privacy or Compliance Officer and a copy of any lapses, discrepancies or recommendations identified given to the Data Provider.
- V. The Data Provider will have 30-days with which to rectify any recommendations made and provide written documentation of remedy.

RESOURCES

HIE Access Termination Policy #33

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to define the process for terminating access by CCHC Workforce or Participating Organization Authorized Users to CCHC HIE's Protected Health Information (PHI) when employment of a Workforce member ends or contract affiliation with a Participating Organization Authorized User concludes.

PROCEDURE

- I. CCHC Workforce designee shall serve as the primary facilitator for all CCHC Workforce and/or Participating Organization's request for Authorized User access termination and is responsible for managing and maintaining the documentation of access system privileges.
 1. Request for termination shall be submitted in writing or email to CCHC Workforce designee at CCHC-HELP@CentralCoastHealthConnect.org in writing to CCHC – Attn: HIE Support Services Department, 10 Ragsdale, Suite 102, Monterey, California 93940.
 2. Upon receipt of request and verification, CCHC Workforce designee shall immediately submit the proper documentation to its Technology Vendor for access termination. The originating requestor will be notified by email when the termination is complete.
 3. CCHC's Security & Privacy Officer and CCHC HIE Administrator are responsible for monitoring of termination requests and facilitation oversight.
- II. Participating Organization's shall promptly request access termination to CCHC HIE immediately for any Authorized User who no longer requires access by reason of termination of employment, and within five (5) business days for Authorized Users who no longer require access by reason of change in function.
 1. Participating Organization's shall immediately request access termination access to CCHC HIE for any Authorized User that engages in conduct that could undermine the security, privacy or integrity of CCHC HIE.
- III. CCHC reserves the right to immediately terminate or suspend access to CCHC HIE to any Authorized User who discloses his or her ID or password, or fails to abide to the CCHC Security and Privacy policies and procedures.

RESOURCES

- Reference – 45 C.F.R. § 164.308 (a)(3)(ii)(B) – Termination Procedures

HIE Participation Agreement Policy #34

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to ensure that any access, use and disclosure of Protected Health Information (PHI) maintained within CCHC HIE from its Participating Organizations/Data Providers/Contracted Entities have an executed HIE Participant Agreement which outlines strict adherence to HIPAA and HITECH privacy and security regulations.

POLICY BACKGROUND

- I. Under the HIPAA Privacy Standards, an entity performing certain types of services on behalf of a Covered Entity constitutes a Business Associate. HIPAA also requires that a Covered Entity and its Business Associates must enter into a BAA designed to protect the privacy and security of PHI made available to the Business Associate during the performance of services on behalf of the Covered Entity.
- II. A Business Associate is defined in 45 C.F.R. Part 160, as a person or entity that performs a function activity or service on behalf of a Participating Organization or another Business Associate involving the disclosure of Protected Health Information to the Business Associate. CCHC is a Business Associate to each of its Participating Organizations. Subcontractors and vendors to CCHC may be considered Business Associates of CCHC.
- III. CCHC HIE operation and management facilitation may require access, use or disclosure of PHI by CCHC or its Business Associates/Subcontractors acting under a Business Associate Agreement to perform functions or activities on behalf of Participating Organizations. A Business Associate is contractually obligated not to use or disclose PHI other than as permitted or required by the BAA or required by law.

PROCEDURE

- I. CCHC shall ensure each Participating Organization, Data Provider or Business Associate/Subcontractor executes an HIE Participation Agreement with a Terms and Conditions Exhibit prior to utilizing PHI or data through CCHC HIE.
 - a. Access will not be granted to Protected Health Information, nor User Account Set-Up, nor financial compensation for services paid until the agreement is executed.
 - b. CCHC's contracted partners shall comply fully with all necessary safeguards and requirements outlined in the HIPAA Privacy Standards and Security Rules, and HITECH regulations as it pertains to PHI permitted uses.
 - c. Should either CCHC or a Participating Organization/Business Associate/Subcontractor elect to terminate its agreement for any reason, then the

HIE Participation Agreement Policy #34

Participating Organization/Business Associate/Subcontractor will no longer be allowed to access CCHC HIE. User access termination protocols are referenced in CCHC's HIE Termination Policy

- II. CCHC and its Business Associates/Subcontractors may access, use or disclose only the Minimum Necessary Protected Health Information obtained from or on behalf of any Participating Organization for the following purposes (but not limited to):
 - a. Installing, testing functionality or maintaining interface connectivity to CCHC HIE;
 - b. Trouble shooting CCHC HIE technology-related issues;
 - c. Providing CCHC HIE administrative or system maintenance support;
 - d. Providing training to Workforce members, Participating Organizations or Business Associates/Subcontractors;
 - e. Assisting with security or PHI breach investigations; and
 - f. Performing any other function or service needed to support CCHC HIE as directed by CCHC's Executive Committee or CCHC HIE Administrative Designee.
- III. CCHC's Security and Privacy Officer or Designee, shall keep a copy of each executed agreement and provide continued oversight of compliance by contracted partners of HIPAA and HITECH regulations.
- IV. CCHC's Security and Privacy Officer or Designee shall investigate any report of unauthorized use or disclosure of PHI or any other material security breach by any Participating Organization/Business Associate/Subcontractor and take appropriate action after full investigation, including possible contract termination.
- V. For Participating Organizations who have been utilizing the CCHC HIE prior to the effective date of this HIE Participation Agreement Policy, it is required that an executed retro-active agreement be enforced to meet contractual and Security and Privacy compliance. Should a Participating Organization not have an executed agreement within 30 days from the policy's effective date, then CCHC maintains the right to temporarily disable HIE privileges for all Authorized Users until the agreement is executed.

RESOURCES

- Reference – CCHC's HIE Participation Agreement and Terms and Conditions Exhibit
- Reference - 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)
- Reference - 45 C.F.R., Part 160
- Reference – California Association of Health Information Exchanges (CAHIE), HIE Participation Agreement Release 2.2, April 2014
- Reference – CCHC HIE Termination Policy

Amendment of PHI Policy #35

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to describe the role of CCHC when Patients seek to amend their Protected Health Information (PHI) and to clarify that only Participating Organizations (POs) can amend PHI of a Designated Record Set that is requested directly by Patients and is exchanged through CCHC HIE.

POLICY BACKGROUND

- I. Patients have the right to amend their PHI or information used and disclosed through CCHC HIE as established by HIPAA Privacy Standards.
 - a. A Designated Record Set is any grouping of medical or billing records used to make Treatment or Payment decisions about a Patient.
 - b. Requested amendments are evaluated by the Covered Entity whose records are subject to the Patient's requested amendment and maybe either accepted or denied.
 - c. CCHC is neither a Covered Entity nor a Healthcare Provider and serves to facilitate the exchange of PHI between POs for Permissible Purpose. POs serve as the originators of PHI and maintain the Designated Record Sets in which this information resides and because of that protocol, POs are the only organization that may assuage and make Patient amendment requests after proper validation.
- II. In the event that CCHC receives a request for an amendment directly from a Patient, CCHC shall promptly communicate the proper steps in writing to the requestor.

PROCEDURE

- I. The procedure for Participating Organization's is as follows:
 - a. Any requests for PHI amendments by a Patient will be directed to the PO.
 - b. The applicable PO(s) will be solely responsible for evaluating the written request and determining whether to grant or deny a Patient's request to amend his or her PHI in compliance with all Federal legal requirements.
 - c. The PO's process used to evaluate an amendment request must be compliant with all Federal legal requirements including HIPAA Privacy Standards.
 - d. Should a Patient's request for PHI amendment be granted, then the applicable PO(s) will be solely responsible for timely amendment of its Designated Record Set.
 - e. Should a Patient's request for PHI amendment be denied, then the applicable PO(s) must inform the Patient of this decision in writing and explain why the request was denied and advise the Patient of their right to submit a written statement of disagreement in the Designated Record Set.

Amendment of PHI Policy #35

- f. Should a Patient submit a statement of disagreement, then the PO must include that statement in any subsequent disclosure of PHI through the HIE of the disagreement.
- II. The procedure for CCHC is as follows:
 - a. CCHC will not process or approve any request for PHI amendments by Patients.
 - b. Should CCHC receive a direct request for an amendment to his or her PHI directly from a Patient, CCHC Workforce designee will write a letter to the Patient within five (5) business days to contact his or her health care provider at the appropriate Participating Organization for amendment facilitation.
 - c. Additionally the CCHC Workforce designee will forward the patient's request for PHI amendment to the Participating Organization lead contact within five (5) business days.
 - d. CCHC template language for a direct patient inquiry is as follows:
 - i. On (insert Patient request receipt date), CCHC HIE received a request from you to amend Protected Health Information (PHI) data about you that may have been exchanged through CCHC HIE. CCHC HIE does not maintain or amend designated record set data, as that information is provided by your health care providers. As a result, CCHC HIE cannot make the requested amendment on your behalf. If you would like to amend your PHI, you will need to contact your health care provider directly for assistance.
 - e. CCHC shall maintain a log of all requests for amendments made by Patients directly to CCHC.

RESOURCES

- Reference – 45 C.F.R. § 164.526 – Amendment of Protected Health Information

Patient Record Merge Policy #36

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to outline the procedure for patient record merge management within CCHC HIE. The Master Patient Index (MPI) combined with the Record Locator Services provides the method for robust patient matching from various Participating Organizations and Data Providers. The subsequent process to manage patient record merging by Participating Organizations in a timely fashion, aids in continued data integrity of CCHC HIE.

POLICY BACKGROUND

- I. The Master Patient Index is a database containing a unique identifier for all patients under the domain of an HIO. Hospitals, health systems, labs and other entities may have their own identifiers for patients, and as a result, there will be multiple identifying codes in use among participants in an HIO that can refer to one patient.
- II. The Master Patient Index uses several matching algorithms to find all of a given patient's records across disparate systems and match these records to the correct patient within the HIE. These algorithms typically use the patient's first and last name, date of birth, sex, mailing address and/or a combination of additional data elements, such as telephone number, to promote accuracy.
- III. Within an HIE, a Record Locator Service is the part of the system that determines what records exist for a patient and where the source data is located.
- IV. The more data elements incorporated into the patient matching process, the more accurate the process becomes. The patient matching mapping system process divides the possible records into three categories: (1) matched, (2) not matched; and (3) undetermined. At times, human intervention in the matching process is necessary to ensure the accuracy of the records being associated with an individual.
- V. CCHC maintains strong process controls with its technology vendor, RelayHealth on MPI metrics and opportunities or stronger specificity matching criteria and enhancements.

PROCEDURE

- I. CCHC, with its technology vendor, RelayHealth ensures that the core patient matching platform services are in place and MPI criteria are reviewed routinely for additional enhancements. CCHC HIE utilizes four (4) mandatory patient matching items (First Name, Last Name, Date of Birth and Gender), and an optional fifth item, Zip Code.
- II. CCHC HIE architecture aids Participating Organizations in the ability to identify easily any patient records needed to be individually reviewed under a system tab called "duplicate task". Within the duplicate task queue, an assigned hospital Participating Organization

Patient Record Merge Policy #36

- designee, or CCHC Workforce, can perform additional review to ascertain if the record matches an existing patient record and if so, provide a method to merge the patient records.
- III. Patient Record Merges cannot be completed at the patient record level and only at the duplicate queue level.
 - IV. Non-hospital Participating Organizations will not be provisioned with access to complete patient record merges. If a non-hospital Participating Organization identifies two or more patient records that are for the same patient, they shall contact CCHC and request a patient record merge be completed.
 - V. Hospital Participating Organizations shall be responsible for having identified and trained staff to manage the duplicate task queue on, at minimal, a weekly basis and keep the number of duplicate records to an appropriate level. Queues that exceed 1000 will be reported to the Executive Committee.
 - VI. All incorrect Patient Record Merges need to be reported to CCHC immediately. CCHC Workforce will notify the CCHC Security & Privacy officer and contact RelayHealth/vendor to advise of the incorrect merge and will assist with coordination of the reconciliation of the patients' accounts, with the affected Participating Organizations.

RESOURCES

- Reference – RelayHealth Service Feature Guide Patient Match/Merge, Release 14.11, November 2014

Security Management Policy #37

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement and define procedures to prevent, detect, contain and correct security violations. This policy covers the PHI risk analysis that CCHC will conduct, the security measures and safeguards that CCHC will implement for its PHI based upon such risk analysis, and the information systems review activity that CCHC will conduct to ensure the security of such PHI.

PROCEDURE

- I. **Risk Management:** In order to determine those areas of the HIE that may be vulnerable to internal or external loss, destruction or other loss of Confidentiality, Availability or Integrity, and to identify and initiate appropriate prevention and remediation programs, CCHC assesses potential risks and vulnerabilities to the PHI in its possession and develops, implements, and maintains appropriate Security Measures. The risk assessment process is reviewed when a significant change occurs or at least once every other year. At a minimum, a description of the risk, its current level, an acceptable level and the specific safeguards to be implemented or modified to address variance between the current level and acceptable level of risk is documented. CCHC implements a risk analysis process to assess the risk to HIE assets as part of an overall risk management process. The overall process is documented. Workforce members, participating organizations and CCHC's technology vendor are expected to cooperate fully with any risk assessment being conducted on HIE systems.
- II. **Risk Assessment:** Risk assessments are conducted by CCHC personnel on any portion of HIE, including applications, servers, desktops, laptops and networks, and any process or procedure by which these systems are administered and/or maintained including, without limitation, the creation, handling, transportation, storage, and disposal of storage media of any media type or format. Risk assessments may include qualitative and quantitative factors, including a determination of the monetary value of the CCHC asset, and the CCHC's requirements for the Availability and Integrity of the asset. In addition to assessing the risk associated with HIE system components, CCHC must assess the risk posed by connection to the HIE by Participating Organizations, and Authorized Users.
- III. **Information System Activity:** Formal HIE system activity review procedures are intended to assure the regular monitoring and review of HIE system activity, including audits, access reports and Security Incident tracking reports. They will be employed on a regular basis to ensure the Integrity, Confidentiality and Availability of information and resources, to permit

Security Management Policy #37

the investigation of possible Security Incidents and to provide general monitoring of system activity.

- IV. **Evaluation of Administrative Safeguards:** CCHC will perform a periodic technical and nontechnical evaluations based initially upon the Security Standards and subsequently, in response to environmental or operational changes affecting the Security of PHI that establishes the extent to which the Security Policies meet the requirements of the Security Standards.

RESOURCES

- Reference – 45 C.F.R. § 164.308(a)(1)(ii)(A)
- Reference – 45 C.F.R. § 164.308(a)(1)(ii)(B)
- Reference – 45 C.F.R. § 164.308(a)(8)

Facility Access Control Policy #38

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement a process to limit physical access to its electronic Information Systems and the Facility or Facilities in which they are housed, while ensuring that properly authorized access is allowed. CCHC will also establish and implement procedures that allow Facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

PROCEDURE

- I. **Contingency Operations** - CCHC requires its technology vendor to have in place certain contingency plans, or disaster control plans, to identify and respond to disasters, protect PHI and HIE systems, and to limit damage to RelayHealth's physical Facilities.
- II. **Facility Security Plan:** It is the expectation of the CCHC that its Facilities are protected from unauthorized access, and that the equipment therein is protected from unauthorized physical access, tampering and theft. All CCHC information processing areas are protected by physical controls appropriate for the size and complexity of the operations therein and the criticality or sensitivity of the systems operated at those locations. Physical access to areas controlled by CCHC is restricted only to authorized personnel, Business Associates, and subcontractors that need access to the Facilities to perform services (pursuant to a Business Associate/subcontractor agreement) and authorized visitors. Authorized visitors must be recorded, identified and supervised.
- III. **Theft Protection:** To minimize the risk of theft to equipment such as Workstations, communications gear, laptops, etc., deterrents such as locked rooms and storage areas, controlled access rooms, and the monitoring of Business Associates/subcontractors and visitors are in place. Laptops, external drives, and other easily pilferable items must be equipped with a suitable locking cable and secured to a fixed object when unattended. Personnel in the possession of laptops, PDAs and other transportable computers or Electronic Media containing PHI must NOT check these items in airline luggage systems. They must remain in the possession of the traveler as hand luggage. Whenever PHI and equipment or Electronic Media on which it is located must be removed from CCHC premises, a record of the date, the PHI and equipment involved, and the persons possessing the PHI and equipment must be made. Equipment containing PHI must have the PHI Encrypted and boot disk locks must be employed. Electronic Media containing PHI must be Encrypted.
- IV. **Access Control and Validation:** All CCHC information processing areas are protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to

Facility Access Control Policy #38

controlled areas is restricted to authorized Workforce members, Business Associates, subcontractors and visitors. Authorized visitors must be recorded, identified and supervised.

- V. **Maintenance Records:** Records of repairs and modifications to the physical components of a Facility, such as walls, doors, and locks must be maintained and kept according to the CCHC's record retention policy.

RESOURCES

- Reference – 45 C.F.R. § 164.308(a)(7)
- Reference – 45 C.F.R. § 164.310

Physical Safeguards Policy - Workstation Policy #39

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

PROCEDURE

- I. Workstations that handle PHI must employ an approved access control mechanism (e.g., software or hardware) to restrict access to authorized Users. Only CCHC authorized applications and utilities may be loaded on User Workstations. Unauthorized applications will be removed by CCHC administrative staff and the individual who installed the unauthorized application subject to possible disciplinary actions.
- II. All PHI is to be stored on network drives, unless otherwise authorized by the CCHC's Security Official. PHI that is allowed to leave the Facility, whether it is on a laptop, PDA, or other form of portable device, must be properly protected with passwords and files encrypted in secure file structures. Laptops must also have a plain language policy prohibiting the transmission of PHI over public communication lines without a proper protection mechanism approved by CCHC.
- III. CCHC Workstations (including laptops) must be physically protected from theft, damage, or other loss to the Workstation or the PHI contained therein by the use of locks, bolts and other physical deterrents.
- IV. **Protection for Sensitive Workstations:** All Workstations that have access to PHI are configured with screen savers to blank the screen, and require a Password to resume operation whenever the Workstation is unattended for more than 30 minutes. A power-on Password is also used on Workstations that access PHI. Whenever operationally feasible, electronic sessions should terminate after 30 minutes.
- V. **Access Key Control:** When access keys or combinations (such as room or cabinet keys or locks) are used, a specific, identified individual shall be designated as responsible for managing, distributing, and logging the issuance of keys and combinations to other authorized individuals.
- VI. **Portal Equipment Control:** A Workforce member who receives permission to remove equipment or Electronic Media containing PHI from a CCHC Facility must provide a reasonable level of protection for that equipment and associated PHI, software, data, and media from theft and damage. Equipment shall be configured with security safeguards at least equivalent to those implemented on equipment installed within CCHC Facilities. Employees shall be prohibited from altering or disabling such Security Measures except with CCHC Security Officer approval.

Physical Safeguards Policy - Workstation Policy #39

- VII. **Hardware Changes/Configuration Management:** All computer and communications systems used for processing PHI employ a formal change control procedure to ensure that only authorized changes are made. The change control procedure is used to document all significant changes to software, hardware, communications links, and operational procedures, including changes to the physical deterrents (such as a change of locks or combinations) protecting such items.
- VIII. **Workstation and Terminal Control:** Devices outside computer or communications rooms must be logged off or physically secure when unattended; housed in a Facility that provides adequate protection from theft or provided with additional Physical Safeguards; and protected from environmental hazards (e.g., extreme temperature changes, electrical power surges, dust, dirt, and liquids).
- IX. **Removal of Sensitive Information:** Workforce members must receive authorization from CCHC's Security Officer prior to removing from CCHC Facilities any computer, PDA or Electronic Media containing PHI.
- X. **Storage:** CCHC staff must not store sensitive information, including PHI, on Workstation hard-disk drives unless CCHC's Security Officer has determined that adequate information Security Measures will be employed on the Workstation. Additionally, sensitive information shall not be stored on diskettes without approval of CCHC's Security Officer.

RESOURCES

- Reference – 45 C.F.R. § 164.310

Technical Safeguards – Access Control Policy #40

Created Date: 2/1/2015

Effective Date: 12/1/2015

Revised Date: 10/8/2015

Committee Approval: Executive

Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to implement technical policies and procedures for CCHC systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights pursuant to the Security Policies. Access control procedures are set forth in the HIE Portal Access Control Policy #17.

PROCEDURE

- I. **Unique User Identification** - Each CCHC Workforce member shall be assigned a unique name and Password to permit tracking User identity. Access to PHI is granted to Workforce members only on a “need to know” basis. This approval must be documented.
- II. **Automatic Log-Off:** Workstations and other systems are equipped with automatic logoff capabilities to ensure that, if unattended or otherwise not in use for 30 minutes, such Workstation or other system will automatically log-off the CCHC Workforce member. If Workstations are connected to a network and are not performing specialized background functions such as monitoring or logging, when unattended for 30 minutes, such Workstation must always be logged off. For specialized Workstations that cannot be logged off, measures such as screensavers or physical Security access to keyboards and monitors are employed.
- III. **Encryption and Decryption:** Any PHI transmitted over the Internet must be Encrypted to ensure that anyone who may intercept the data while in transit may not be able to access or use it. PHI must also be Encrypted when stored on disks, tapes or other media. Encryption must be done via approved Encryption programs. CCHC’s Security Officer shall ensure that the most appropriate and up-to-date Encryption technology is employed.

RESOURCES

- Reference – 45 C.F.R. § 164.312(a)(2)

Contingency Plan Policy #41

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is for CCHC to implement and define procedures for responding to an emergency or other occurrence that damages systems that contain PHI.

PROCEDURE

- I. **Data Backup Plan:** CCHC will require its technology vendor, RelayHealth, to have a data backup plan in place in order to ensure that exact copies of PHI are retrievable in the event HIE systems are down, breached, corrupted or otherwise subject to a disaster event.
- II. **Disaster Recovery Plan:** CCHC will require its technology vendor, RelayHealth, to ensure that all computer and network resources considered critical to HIE operations have recovery capabilities to minimize the impact of any disruption or unavailability due to fire, vandalism, natural disaster or system failure from any cause. RelayHealth will be required to implement a disaster recovery plan to recover from losses ranging from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery planning in preparation for catastrophic losses of information resources.
- III. **Emergency Mode Operation Plan:** CCHC will require its technology vendor, RelayHealth, to implement appropriate procedures to enable continuation of critical HIE processes for protection of the security of PHI while operating in emergency mode.

RESOURCES

- Reference – 45 C.F.R. § 164.308(a)(7)

Master Appendix Policy #42

Created Date: 2/1/2015
Effective Date: 12/1/2015
Revised Date: 10/8/2015
Committee Approval: Executive
Next Scheduled Review: 10/1/2016

PURPOSE

The purpose of this policy is to provide and maintain a central reference list of URL's, custom forms listed in Appendix materials and additional helpful references associated with the CCHC suite of Security and Privacy Policies and Procedures.

PROCEDURE

- I. The CCHC Security & Privacy Officer or Designee will maintain the attached master Appendix of key reference materials indicated in the CCHC suite of Security and Privacy Policies and Procedures.
- II. All CCHC policy and procedure forms, if updated, shall be reviewed by the CCHC Security & Privacy Officer or Designee for input, approval and ensure updated materials are provided in a timely fashion to applicable Participating Organizations and/or posted on the CCHC SharePoint or Website.

MASTER REFERENCE RESOURCE LIST

Policy #	Policy Name	Reference or Name of Form	URL/Notes
3	HIE Portal Access	RelayHealth Training Suite/Modules	Process Lab, Radiology, Transcriptions and Forward Results to Colleagues/Patients RelayClinical Record Invite Patients to Register for RelayHealth
4	HIE Portal Access Monitoring and Adherence	45 C.F.R § 164.308(a)(1)	http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf
5	HIE Downtime	CCHC Downtime Notification Contact List	To be developed by CCHC, list of key contacts at CCHC and Participating Organizations
6	Security Monitoring and Reminders	45 C.F.R. § 164.308	http://www.gpo.gov/fdsys/granule/CFR-2010-title45-vol1/CFR-2010-title45-vol1-sec164-308
		45 C.F.R. § 164.306	http://www.gpo.gov/fdsys/pkg/CFR-2013-

Master Appendix Policy #42

			title45-vol1/pdf/CFR-2013-title45-vol1-sec164-306.pdf
		California Civil Code 1798 § et seq.	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798-1798.1
8	Individual Authorization	CFR Part 160 and Part 164, Subparts A and C	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
9	Restrictions by Individual	45 C.F.R. § 164.522	http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-522.pdf
		California Civil Code 56	http://www.leginfo.ca.gov/.html/civ_table_of_contents.html
12	Confidentiality Agreement Form for Workforce	CCHC Workforce Confidentiality Acknowledgement Form	See Appendix A
15	Workforce and User Training	45 C.F.R. §164.308(a)(1)(i)	http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf
16	De-Identification	45 CFR § 164.514(a)-(c)	http://www.gpo.gov/fdsys/pkg/CFR-2002-title45-vol1/pdf/CFR-2002-title45-vol1-sec164-514.pdf
17	Disposal of PHI	NIST Special Publication 800-88 Revision 1 (regarding media sanitation)	NIST Special Publication 800-88 (regarding media sanitation): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
		45 CFR 164.310(d)(2)(ii) and (ii) (regarding re-use of media)	http://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/pdf/CFR-2003-title45-vol1-sec164-312.pdf
		45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i) which ensures appropriate training for anyone involved in the disposal of PHI	http://www.hhs.gov/ocr/privacy/hipaa/faq/safeguards/575.html
		HHS HIPAA Security Series 3: Security Standards – Physical Safeguards	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.p

Master Appendix Policy #42

			df
18	Certification Form for Disposal of PHI	CCHC Certification Form for Disposal of PHI	See Appendix E
19	Malicious Software, Virus and Other Threats	45 § C.F.R. 164.308(a)(5)(ii)(B) - HIPAA Administrative Specifications regarding Security Rules	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
20	Disaster Recovery and Data Backup Plan	45 C.F.R. 164.308(a)(7) – Disaster Recovery	http://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/pdf/CFR-2003-title45-vol1-sec164-308.pdf
		45 C.F.R. 164.308(10(7)(ii)(a) - Data Back Up Plan	http://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/pdf/CFR-2003-title45-vol1-sec164-308.pdf
22	Complaint Resolution	78 Fed. Reg. at 5578–79 (to be codified at 45 C.F.R. §§ 160.306(c), 160.308)	http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
		45 C.F.R. § 160.306, 45 C.F.R. 164.520(b)(vi)	http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
		CCHC Compliant Form	See Appendix D
23	Response to Breach and Security Incidents	45 C.F.R § 164.400-41 – HIPAA Breach Notification Rule	http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
		45 C.F.R § 164.412 Subpart D – HIPAA Law Enforcement Delay	http://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-412
		45 C.F.R § 164.408 – Instructions for Submitting Notice of Breach to Secretary	http://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-408
		HITECH Omnibus FR, 78 FR 5566, January 25, 2013	http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
		HITECH Act, Section 13407	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf
		CCHC HIE Breach	See Appendix B

Master Appendix Policy #42

		Notification Form	
		CCHC HIE Breach Risk Assessment Form	See Appendix C
		CCHC HIE Individual Breach Notification Form	See Appendix D
24	Firewall	NIST SP 800-41, Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
		45 C.F.R. §164.308(a)(5)(ii)(B)	http://www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/pdf/CFR-2003-title45-vol1-sec164-308.pdf
		RelayHealth Network Security Plan	CCHC Master RelayHealth Resource Documents
25	Auto Release of Clinical Results	42 CFR 493	http://www.gpo.gov/fdsys/pkg/FR-2014-02-06/pdf/2014-02280.pdf
		45 CFR Part 164	http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
		42 CFR 496.6 (k)(i)	http://www.acr.org/~media/ACR/Documents/PDF/Advocacy/Fed%20Relations/Meaningful%20Use/acr_comments_cmsncrfi_hie_interoperability_42013.pdf
		California Health and Safety Code, Section 123148	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=123001-124000&file=123100-123149.5
		California Health and Safety Code, Section 123148 (f)	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=123001-124000&file=123100-123149.5
		78 FR 14793	http://www.gpo.gov/fdsys/pkg/FR-2013-03-07/pdf/FR-2013-03-07.pdf
27	Opt Out	45 C.F.R. §§ 164.506(b), 164.522(a), and 164.524	http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-

Master Appendix Policy #42

			sec164-522.pdf
		California's Confidentiality of Medical Information Act (CMIA—Cal. Civ. Code §§ 56 et. seq.)	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56-56.07
		CCHC Opt Out Patient Education Materials	See Appendix F
28	Sensitive Health Information	45 C.F.R § Part 164, 164.522	http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-522.pdf
		California Civil Code §§ 56-56.37	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56.35-56.37
29	Patient Consent and Permissible Uses	45 C.F.R § 160-163	http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
		45 C.F.R § 164.506	http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-506.pdf
		California Civil Code § 56, et seq.	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56-56.07
		California Civil Code Sections 1798.29 and 1798.82	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
33	HIE Access Termination	45 C.F.R. § 164.308 (a)(3)(ii)(B) – Termination Procedures	http://www.gpo.gov/fdsys/granule/CFR-2010-title45-vol1/CFR-2010-title45-vol1-sec164-308
34	HIE Participation Agreement	45 C.F.R., Part 160	http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
		45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
		California Association of Health Information	http://www.ca-hie.org/news/model-modular-participants-agreement-release-

Master Appendix Policy #42

		Exchanges (CAHIE), MMPA Release 2.2, April 2014,	2-2-1
35	Amendment of PHI	45 C.F.R. § 164.526 – Amendment of Protected Health Information	http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-526.pdf
36	Patient Record Merge	RelayHealth Service Feature Guide Patient Match/Merge, Release 14.12	https://app.demo.relayhealth.com/resource/library/downloads/FeatureGuides/FG_Orders.pdf

Master Appendix Policy #42

Appendix A – Policy 12

Workforce Confidentiality Acknowledgement Form

For the Workforce Member:

I have read and understand the Central Coast Health Connect (CCHC) Confidentiality Policies on the use, collection, disclosure, storage, and destruction of Protected Health Information (“PHI”).

I agree to follow the Confidentiality Policies and all related policies including. I agree that while I am employed or have a contract with CCHC, I will not reveal or disclose PHI to any person except as authorized by California and federal law. I also understand that my obligations to maintain strict confidentiality of PHI will continue after my employment or association with CCHC ends. Lastly, I understand that unauthorized use or disclosure of PHI may result in disciplinary action, which may include termination of employment or contract, the imposition of civil and criminal fines against me pursuant to California and federal laws, and reporting to any appropriate professional licensing board.

Include: Date, Employee Name, Employee Signature

Master Appendix Policy #42

Appendix B – Policy 23

CCHC HIE Breach Notification Form

To be completed by the entity who identified the PHI breach.

Brief description of information disclosed (provide copies of information disclosed)	
Date disclosure occurred	
Date of disclosure awareness	
How you (your department) became aware of the disclosure (including name(s) of individuals notified)	
Name, medical record, and account number of patient(s) whose information was disclosed	
Address for patient whose information was disclosed	
Name of intended recipient	
Name of actual recipient	
Actions taken to retrieve/remove misdirected information	
How did the disclosure occur?	
Actions taken to prevent recurrence (includes counseling, discipline and procedure changes as appropriate)	
Individual, department, or facility responsible for the disclosure (include staff name, title, department or phone number of other facility)	

Master Appendix Policy #42

Additional information	
Name of individual completing this form	

Time critical document

Please submit via Secure E-mail: CCHC-Help@CentralCoastHealthConnect.org

Phone: 831-644-7494

Master Appendix Policy #42

Appendix C – Policy 23

CCHC HIE Breach Risk Assessment Form

This worksheet must be completed by the CCHC SPO or designee for each possible breach of Protected Health Information (PHI) and sent to the affected Participating Organization's Privacy Officer within 24 hours of receiving an HIE Participant Breach Notification form.

Date(s) of breach of PHI _____
Date breach detected _____

Submitter Contact Information

Full Name: _____

Organization: _____

Address: _____

Phone: _____

Email: _____

Incident Background

2. Was protected health information (PHI) involved?

- Yes, PHI was involved. *Continue to Question 2.*
- No, PHI was not involved. No breach reporting required under HIPAA.
Describe the information involved:

2. Was the PHI unsecured? (*"Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance, such as encryption or destruction. The guidance can be found on the DHHS website at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.)*)

- Yes, PHI was unsecured. *Continue to Question 3.*
- No, PHI was secured. No breach reporting required under HIPAA.
Describe the PHI (for example, was it verbal, paper, or electronic? Encrypted or password protected, other?):

Master Appendix Policy #42

3. Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule? *(Providers should keep in mind that a violation of the “minimum necessary” standard is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. Providers may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule.)*

Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. *Continue to Question 4.*

No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

Describe who acquired, accessed, used and/or disclosed the PHI, whether the person(s) was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed:

4. Does an exception apply? Check any box below that applies:

Exception A.

A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

(i) Was made in good faith; and

(ii) Was within the course and scope of authority; and

(iii) Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce” includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether or not they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

Exception B.

A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

Exception C.

A breach does not include disclosure of PHI where the provider or business associate has a good faith belief that the unauthorized person who received it would not reasonably have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse

Master Appendix Policy #42

mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.

- Yes, an exception applies. No breach reporting required under HIPAA.
- No, an exception does not apply. *Continue to Question 5.*

5. Risk assessment. An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL of the factors listed below.)

Factor A. Consider the nature and extent of the PHI involved, including the types of identifiers (and the likelihood of re-identification if the PHI is de-identified). *(Consider whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, STD, cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interests. Hospitals should also determine whether there is a likelihood that the PHI could be re-identified (if the PHI is de-identified) based on the context and the ability to link the information with other available information.)*

Describe the PHI involved, including identifiers and likelihood of re-identification (if the PHI is de-identified):

Consider whether PHI could be used in a manner adverse to the patient(s) or to further the unauthorized person's interests:

Factor B. Consider the unauthorized person who used or received the PHI. *(This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information - for example, is the person a covered entity required to comply with HIPAA, or a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.)*

Master Appendix Policy #42

Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified):

Factor C. Consider whether the PHI was actually acquired or viewed. *(If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.)*

Describe whether the PHI was actually acquired or viewed (attach report from a computer forensic analyst, if one was obtained):

Factor D. Consider the extent to which the risk to the PHI has been mitigated — for example, as by obtaining the recipient’s satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) has been completely returned, or has been/will be destroyed. *(Hospitals should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results in terms of the risk to PHI. For example, a hospital may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)*

Describe risk mitigation steps taken:

Factor E. Describe any other relevant factors (write “none” if appropriate):

Based on the factors noted above, is there a low probability that the PHI has been compromised?

- Yes (there is a low probability), thus **No** breach reporting required under HIPAA.
- No (there is not a low probability; there is a higher probability) thus breach reporting is required under HIPAA.

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether reporting is required under federal law (HIPAA). State laws require notification of a breach as defined in state law regardless of the results of this risk assessment. (See “IV. State Law:

Master Appendix Policy #42

Breach of Unencrypted Computerized Data in Any California Business” on page 12.2, and “V. State Law: Breach in a Licensed Health Care Facility” on page 12.4, for information regarding notification under state law.) A provider may also have reporting obligations pursuant to a business associate agreement or other contract.

Signature of person completing this form: _____

Title: _____

Date: _____

Master Appendix Policy #42

Appendix D – Policy 23

CCHC HIE Individual Breach Notification Form

To be printed on letterhead and filled out by CCHC SPO or designee

To: Add Individual Name

Address: Add Individual's Address

Date:

RE: *Individual Breach Notice*

Dear _____,

We are writing to inform you of an alleged breach of your Protected Health Information (PHI) contained in the Central Coast Health Connect (CCHC) Health Information Exchange (HIE). Our team is investigating the details of the alleged breach below and has included steps in the meantime you may do to help ensure ongoing safety of your information. We are committed to protection of your PHI and will remain in touch as our investigation continues. Our contact information is included below for any additional questions you may have at this time.

Description of Occurrence (Alleged Breach):

Type of PHI (Protected Health Information) Involved:

Actions Taken & Undergoing to Investigate, Mitigate and Protect against any further Breaches:

Suggested Steps for Personal Protection:

We recommend that you immediately take the following Fraud Alert steps outlined below.

4. Call one of the three major credit bureaus listed below to place a "Fraud Alert" on your credit report. This can help prevent anyone from opening additional accounts in your name. Once the credit bureau confirms your Fraud Alert, the other two credit bureaus will automatically place alerts on your credit report.
 - a. Equifax: 1-800-525-2685; www.equifax.com
 - b. Experian: 1-888-397-3742; www.experian.com
 - c. Transunion: 1-800-680-7289; www.transunion.com
5. Order your credit reports from all three bureaus. When you set up a Fraud Alert, you can also receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts or activities that are not yours.

Master Appendix Policy #42

6. Monitor your credit reports carefully. Even with Fraud Alerts on your credit bureau accounts, we recommend that you continue to monitor your credit reports to ensure no one has opened an account using your personal information.

Again, we are committed to a thorough investigation of the alleged breach of PHI and will provide an update after our investigation. Our contact information is below for your reference as well.

For More Information at CCHC:

Add Telephone: _____

Add Email: _____

Add Address: _____

Add CCHC Website: _____

Sincerely,

CCHC Security & Privacy Officer (or Designee)

Master Appendix Policy #42

Appendix E – Policy 18

CCHC Certification Form for Disposal of PHI

Facility Name

The information described below was destroyed in the normal course of business pursuant to a proper retention schedule and destruction policies and procedures.

Date of Destruction: _____ Authorized By: _____

Description of Information Sanitized: _____

Inclusive Dates Covered: _____

Method of Destruction:

Burning Shredding Pulping Demagnetizing Overwriting Pulverizing

Other: _____

Records Destroyed By: _____

Witness Signature: _____

Department Supervisor: _____

Media Reused Internally or Externally: Yes – to whom, No – confirm

Media Returned to Manufacturer: Yes – to whom, No – confirm

Other – If records is destroyed by outside firm, must confirm that a Business Associates contract exists and certificate of destruction has occurred.

Master Appendix Policy #42

Appendix F – Policy 27

CCHC Opt Out Patient Education Materials

Your Guide to Understanding Central Coast Health Connect

A Health Information Exchange for Monterey County

What is Central Coast Health Connect (CCHC)?

CCHC is a community health information exchange (HIE), a system established to help patients and healthcare providers securely share health information electronically. An HIE helps to ensure that only you and the caregivers you authorize — including doctors, hospitals, and labs — have secure, instant access to vital medical information necessary to provide you the best care possible.

Why is it important to participate in CCHC?

Many people see multiple care providers, often in separate locations. The information about their care, such as doctors' office visits, prescriptions, lab tests, and imaging, historically has also been kept separate. That fragmentation can lead to unnecessary duplication of services and increased safety risks. To increase safety, efficiency, and collaboration, leading-edge organizations are implementing health information exchanges to link patients and their care providers and close the information gaps. When you and your healthcare providers participate in CCHC, your healthcare teams can securely access and share pertinent medical information, enhancing their ability to make the best decisions for your care.

How is my information secure?

Protecting privacy is a top priority in the CCHC system. Access to patient data is strictly regulated and state and federal privacy laws and policies are strictly followed and enforced. CCHC understands that patient privacy is essential, and we make every effort to ensure patient data is securely managed.

What if I don't want to participate in CCHC?

If you don't want to participate in CCHC, you may choose to opt out. It is also important to understand that **opting out prevents the sharing of your information through CCHC between providers**. If they choose, your doctor and other care providers will still be able to use the electronic health information exchange to have your lab results, radiology reports, and other data sent directly to them; previously, they may have received this information by fax, mail, or other electronic communication.

If you still choose to opt out, please e-mail cchc-help@centralcoasthealthconnect.org or call (831) 644-7494 to leave a message and a staff member will contact you.

To learn more about Central Coast Health Connect, please call (831) 644-7494 or visit www.CentralCoastHealthConnect.org and click on the link on the bottom of the page.

Master Appendix Policy #42

CCHC Opt Out Form

This form is for patients who do not wish to participate in Community Hospital of the Monterey Peninsula's electronic health information exchange, known as Central Coast Health Connect (CCHC).

A health information exchange (HIE) is a way of sharing your health information among participating doctors' offices, hospitals, labs, radiology centers, and other healthcare providers through secure, electronic means. This gives participating caregivers the most recent information available from your other caregivers when they are making decisions about your care. If you opt out of participating in CCHC, your doctor and other care providers will still be able to use the system to have your lab results, radiology reports, and other data sent to them; previously, they may have received this information by fax, mail, or other electronic communication. Choosing to opt out only restricts the sharing of information between providers. When applicable, in accordance with laws, the required reporting of infectious diseases to public health officials will also occur through the HIE, even if you opt out.

To opt out of HIE complete this form; it is not necessary to complete a form for each provider. If you do not live in Monterey County, but still receive care in Monterey County, you should complete this form to opt out. If you wish to reverse your decision, you may opt back in at any time by calling (831) 644-7494. Please note: Opt-out requests will be processed within (5) business days.

Mail signed and completed form to: CCHC Administrator, 10 Ragsdale Drive, Suite 102, Monterey, CA 93940
Or scan and e-mail signed form to cchc-help@centralcoasthealthconnect.org or fax to (831) 644-7451.

INFORMATION OF PATIENT OPTING OUT (please print clearly)

Hospital Name _____
 Patient Name _____
 Address _____ City _____ State _____ Zip Code _____
 Primary Phone Number _____ Secondary Phone Number _____
 E-mail Address _____
 Date of Birth _____ Sex: Male or Female _____

Reason for opting out (optional) _____

If this form is signed by someone other than the person above, the person signing the form hereby certifies that he/she is acting as:
 Parent _____ Legal Guardian _____ Other (specify relationship) _____

Contact information for individual completing this form if other than patient:

Printed Name _____ Phone Number _____
 Patient Information _____
 Printed Name _____
 Signature _____ Date _____