NCHIIN North Coast Health Improvement and Information Network

PARTICIPATION AGREEMENT

PROJECT ADDENDUM
NORTH COAST CARE CONNECT, A COMMUNITY HEALTH INFORMATION EXCHANGE

Project Name	North Coast Care Connect NCHIIN has established a Community Information Exchange ("CIE") containing demographic, health and social data provided by various parties ("CIE Participants") regarding individuals ("Individuals") served by organizations in the community. NCHIIN provides the CIE (dba "North Coast Care Connect") to facilitate the exchange of electronic data, coordinate care, and improve the quality of health in the community. North Coast Care Connect is a resource and information hub that connects Individuals to health and social services, insurance, financial aid, debt and tax preparation counseling, housing, food, transportation, employment and job training, disaster relief and other service providers through a network of community partners using an information technology (internet) platform. North Coast Care Connect supports referrals to service providers, care coordination, outreach, education, and other services in connection with its trusted network of referral providers who deliver services to members of the North Coast.
Data Submitted for Exchange	The platform data will include client demographics, health status and clinical (physical and behavioral health) and social encounter data, and social determinants of health data. Only the minimum necessary data will be exchanged.
Data Providers	Exchange partners include health care providers and health plans subject to HIPAA ("Covered Entities"), some of whom are current Health Information Exchange Participants, as well as community-based organizations not subject to HIPAA that will participate in and support CIE activities.
Data Recipients	Authorized Users at participating organizations which include health care providers (physical and behavioral health) and community-based organizations.
Exchange Conditions	The CIE platform will support day-to-day activities of Authorized Users supporting clients referred to community services. The platform uses a care team model to allow a client to choose who sees what level information. While some referrals may be made without a consent (e.g., self-referral by client), the majority of data exchange is after a consent has been signed by

	the Individual. Once consented, Authorized Users will be able to make referrals, coordinate care, and actively case manage clients.
Authorized Users	CIE Participants who have signed a CIE Participation and Data Use Agreement and whose workforce members have (i) been authenticated and given access in compliance with North Coast Care Connect Policies and Procedures; (ii) accept responsibility for compliance with the terms of the Participation Agreement; and (iii) require access to Data to facilitate the provision of CIE services.
Specific Safeguards and Privacy Requirements	Client Consent: See Addendum Appendix A Notice of Privacy Practice: See Addendum Appendix B All Participants shall adhere to the North Coast Care Connect Policies and Procedures: See Addendum Appendix C
Licensed Software	NinePatch SaaS from QS Systems
Project Fee	Provision of the NinePatch Platform and support through individual licenses $ 75.00/per month for 17 licenses = $1,275/per month for 3 years (36 months) = **$45,900.00**
Participation Fees	$6,000.00 1-time fee per program for 7 programs = **$42,000** There are no fees until July 1, 2023
Total Fees	$49,500.00 + $42,000.00 = **$87,900.00 TOTAL**

Effective Date. The Effective Date for this Addendum to Participation Agreement is _____. The Participation Agreement will continue until terminated as set forth in the NCHIIN Health Information Exchange Participation Agreement Section 2.

Humboldt County DHHS

By: _____

Name: _____

Title: _____

Date: _____

North Coast Health Improvement and Information Network (NCHIIN)

By: _____

Name: _____

Title: _____

Date: _____

ADDENDUM APPENDIX A
AUTHORIZATION FOR THE USE AND DISCLOSURE OF HEALTH AND SOCIAL SERVICE INFORMATION
North Coast Care Connect

The North Coast Health Improvement and Information Network (NCHIIN), dba North Coast Care Connect is focused on improving the health and wellbeing of all residents of Humboldt County. The North Coast Care Connect (Care Connect) is a partnership of health, social, and community services organizations that help you get services, work with you to understand your needs, and connect you to resources that can help you. Your permission is needed to allow sharing of your protected health information and other personal information, including through electronic systems used by North Coast Health Improvement and Information Network (NCHIIN) and participating organizations. Granting permission allows your providers to communicate better with each other to provide you better care. If you agree, your information will be stored and shared with (to and from) the following types of organizations to help the coordination of your care, resources, and human services:

- Health care providers
- Behavioral health providers
- Social services providers
- Health plans
- Housing providers
- Organizations involved with the justice system
- Community organizations, for example, food banks, legal services
- County Departments, for example, The Department of Health and Human Services
- Wellness and others

A current list of Participants, which may change from time-to-time, can be found at https://www.nchiin.org/cie

Sharing information makes it easier to see if you are eligible for resources, get referred to services and care, and take part in programs from organizations in Humboldt County to improve your health. It also makes it easier for your providers to coordinate your care, receive payment for services, conduct program work, and improve the quality of services. For more information on how Care Connect uses and protects your information, and how to get a copy of this

Authorization for your records, please view the Care Connect information page at https://www.nchiin.org/cie

Signing this form is your choice. No matter what you choose, it will not change your ability to receive services.

By signing this form, you are giving permission for your information including information disclosed and re-disclosed by you, your family, to be shared with (to and from) the types of organizations shown above. It will be used to see if you are eligible for resources, help link you to them, and help coordinate between them to better serve you.

By signing my name below, I agree that my current, past, and future treating providers and organizations may disclose my health information, records, social services information, and other data to NCHIIN and that such data may be shared among and between the North Coast Care Connect participating organizations.

- Information that may be shared will include but not be limited to information about:
  - my personal characteristics, for example name, date of birth, housing status, and contact information,
  - my medical history, mental or physical condition,
  - my social service information (including CalFresh, General Relief, CalWorks, Cash Assistance Program for Immigrants, Medi-Cal, and other public benefits that I may apply for), and
  - treatment and services I receive.
- I understand that this Authorization will apply to data from all services I receive from Care Connect providers and partners.

ADDENDUM APPENDIX A
AUTHORIZATION FOR THE USE AND DISCLOSURE OF HEALTH AND SOCIAL SERVICE INFORMATION
North Coast Care Connect

I specifically authorize my current, past, and future treating providers and organizations, NCHIIN, and Care Connect participating organizations to share the following information (*check as appropriate*):

- ☐ Mental health treatment information (excluding psychotherapy notes) _____ (*initial*)
- ☐ Information about my HIV/AIDS test results _____ (*initial*)

I understand:

- This authorization will remain in effect for a period of one (1) year from the date this is signed, or until I change or revoke my authorization in writing.
- I have the right to cancel or change this authorization at any time. I can start this process by talking with any of my Care Connect providers. (A verbal or written notice to revoke your consent will be processed within five business days.) At that time, I will either cancel my authorization or complete a new authorization to reflect the change(s) to the sensitive information that I want to share. If I limit my information sharing, my sensitive information will not be shared with partnering providers or organizations from that date forward. Any sensitive information previously shared with current or past treating providers cannot be recalled. Should I elect not to share any sensitive information, I may receive limited care coordination services through the North Coast Care Connect system but does not affect services from the providers.
- When my information is shared, there is a chance it will be re-shared with others. Federal law or California privacy law may not protect the re-sharing of my information.
- I have the right to:
    - Inspect or obtain a copy of my health information and social services information that is shared by this authorization
    - Refuse to sign this authorization
    - Receive a copy of this authorization

ADDENDUM APPENDIX A
AUTHORIZATION FOR THE USE AND DISCLOSURE OF HEALTH AND SOCIAL SERVICE INFORMATION
North Coast Care Connect

I have read this authorization or my provider has read it to me. I authorize the use and sharing of my health and social services information as described above.

_____ _____

Client Signature Date

_____

(Print first name, middle name and last name of individual)

Date Authorization and Consent Expires_____

If this Authorization is signed by a person other than the client, please indicate the relationship:

_____

Relationship to Client

_____ _____

Name Date

ADDENDUM APPENDIX B

NOTICE OF PRIVACY PRACTICES

Effective date: January 1, 2022

THIS NOTICE DESCRIBES HOW PERSONALLY IDENTIFIABLE INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.

What We Do:

The North Coast Health Improvement and Information Network is doing business as the North Coast Care Connect (Care Connect) and is a resource and information hub that connects individuals to health and social services, insurance, financial aid, debt and tax preparation counseling, housing, food, transportation, employment and job training, disaster relief and other service providers through network of community partners using an information technology (internet) platform. Care Connect provides referral to service providers, care coordination, outreach, education, and other services in connection with its trusted network of referral providers who deliver services to members of the North Coast.

Information We Collect About You:

To address your needs and connect you to appropriate providers in our network, Care Connect may collect and keep a record of information about you. This information may include your name, social security number, telephone number, address and email, your age, gender, nationality, ethnicity, physical and mental health condition, health care, health insurance and care team, finances, debt, and employment, housing and housing needs, names and contact information for your family members, friends and care givers, military background, information about the community programs you have been or are currently enrolled in, and other information that may be required to determine if you are eligible for government benefits, tax credits, income/debt assistance, insurance coverage, housing assistance and other programs and services offered by our referral providers. Some of the information we collect may be considered “protected information” under federal and/or state privacy laws. Care Connect maintains information about its Clients, in a secure electronic database and takes precautions to prevent third parties from accessing Client information inappropriately. The system allows us to document the source of the information, who accessed your information and control what information is shared with Care connects network of referral providers. Care connects network of referral providers are legally and/or contractually obligated to protect your information.

Where the Information Comes From

Information about you may come from a variety of sources. The information you provide to us directly when you speak to one of our Care Connect service providers is

considered "self-reported" information. When you provide us with self-reported information, you give us permission to share the information with staff members within the organization you are speaking with or other members of the network depending on the choices you make about sharing your information. The information we disclose depends on how you give us authorization when you participate with a service provider(s) in our network.

a. If you authorize participation with only to a single agency there would not be care coordination or sharing of your information with other agencies or programs (no authorization for network participants). Each referral for service will require you to provide much of the same information

b. If you authorize participation with the full Care Connect network, providers at Care Connect agencies can make referrals and contact other network providers on your behalf and share your information to provide services to you or to refer you to other providers and programs in the North Coast Region.

c. If you authorized participation with only Care Connect network providers approved by your current network team members, then only those agencies can make referrals and share your information to provide services to you or to refer you to other providers and programs in the North Coast Region.

d. If you authorized participation with only Care Connect network providers you approved, then only those agencies can make referrals and share your information to provide services to you or to refer you to other providers and programs in the North Coast Region.

Information about you may also be disclosed to Care Connect by your providers if they are a member of our trusted network. The information will be shared with us when they use access our database to provide services to you or to refer you to other providers and programs in the region. For example, we may receive and share information about you with individuals, businesses, government agencies and community programs that provide meals, emergency or low cost shelter, transportation, healthcare, behavioral health counseling and education services, debt counseling or debt reduction services, tax preparation, employment and job training. This information will also be shared within our organization and with other providers in our referral network in order to provide you with services. In some situations, we may receive protected health information from your healthcare provider. In those situations, we may use and disclose your information only as permitted by the business associate agreement we have entered into with your provider or as expressly permitted by you or as permitted or required by law.

Regardless of the source of information, Care Connect and its referral providers are committed to safeguarding your protected information from unlawful use and disclosure.

For information about the referral providers with whom we may share your information, please visit: https://www.nchiin.org/cie

NORTH COAST CARE CONNECT'S RESPONSIBILITIES

Privacy of Information:

Under California and Federal privacy laws we have a responsibility to maintain the privacy of "protected information." We are required to provide you with this notice of our privacy practices (this notice), and follow the terms of the notice currently in effect. We must notify you when we become aware of unauthorized access, use or disclosure of your unsecured protected health and personally identifiable information.

Changes to this notice:

We reserve the right to change this notice at any time. We reserve the right to make the revised or changed notice effective for the protected information we already have about you as well as any protected information we receive about you in the future.

How to Obtain a Copy of this Notice:

We will post a copy of the current notice on our web site https://www.nchiin.org/cie A copy of the notice currently in effect will be available at the registration area of our facility located 2315 Dean St., Eureka CA 95501. You have a right to receive a paper copy of this Notice and a copy will be mailed to you upon request.

HOW CARE CONNECT MAY USE AND DISCLOSE YOUR PROTECTED INFORMATION INCLUDING HEALTH INFORMATION

We may disclose protected information about you in accordance with the Privacy Laws, or as permitted by you or as permitted or required under state and federal laws. In some situations, we may disclose your information without your oral or written permission. The following list describes examples of different situations where we may use and disclose your information to individuals outside our organization.

Legally Permissible Uses and Disclosures of Information About You:

To Contact You, a Family Member, Friend or Personal Representative:

When you meet with or call us, you will be asked to provide us with contact information for yourself and other persons involved in your care. If you do so, you give us permission to use that information to contact you and the individuals you have identified and to provide services to you in person, by telephone, email or text. We may use the information to communicate necessary information about your appointments, to update you on your care or care management options, programs and benefits you or your family may be eligible for, or to connect you with any of our referral network providers and to follow up with our referral providers about services you have received or programs you have enrolled in. We may contact you or the individuals involved in your care by fax, cell phone, telephone, email or in writing.

To Verify Your Identity:

We may use your protected information and require you to provide us with a copy of a photo or other identification to verify your identity and link it to your record or communicate with you about your information.

Referral for Treatment (including Care Coordination, Case Management and the Determination of Eligibility for Benefits and Programs)

We may gather, use and disclose your protected information to network referral providers to facilitate the delivery of healthcare, care coordination, for health and human services agencies, case management, the determination of eligibility for governmental or other private program benefits, in an emergency or for other purposes permitted by you or permitted by or required by law. Our referral network providers may include doctors, nurses and other healthcare professionals, public health agencies and officials, insurers, social workers, housing officials, and other professionals that provide or coordinate healthcare, mental health or behavioral health treatment, housing and emergency shelter, transportation, education, food and financial assistance among other things. For example, a Different departments within our organization may also share protected information about you in order to coordinate the referral of services you need to and amongst members of our referral network.

For Payment, Qualification for Government Benefits:

We may disclose your protected information to insurance or managed care companies, Health and Human Services Agency, Medicare, Medicaid, Social Security Administration, Public Agencies, utility companies and other providers to assist in the

payment of your bills, reduce debt or tax liability or to qualify you for government benefits or other programs.

For Business Operations:

We may use and disclose your protected information for our business operations. For example, we may use protected information to review the quality of our referral services, and to evaluate the performance of our staff. We may use your information for our business planning and program development, and to investigate complaints.

Business Associates:

We may use or disclose your protected information to our subcontractors, and "business associates" when they perform services that may require the use of your protected information, such as technology, accounting, auditing, legal, and consulting services. Our business associates will be required to keep your protected information confidential.

Disclosures Required by Law:

We may use or disclose your protected information when required or permitted to do so by federal, state, or local law. The following are examples of some of the situations where we may be required to use or disclosure information about you without your Consent.

Public Health Activities:

We may use or disclose your protected information for public health activities that are permitted or required by law. For example, we may disclose your protected health information in certain circumstances to control or prevent a communicable disease, injury or disability; for public health oversight activities or interventions.

Health Oversight Activities:

We may disclose your protected information to a health oversight agency for activities authorized by law. Oversight activities may include audits; investigations; inspections; licensure or disciplinary actions; or civil, administrative, or criminal proceedings or actions. Oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and government agencies that ensure compliance with civil rights laws.

Lawsuits and Other Legal Proceedings:

We may disclose your protected information in the course of a judicial or administrative proceeding or in response to an order of a court or

administrative tribunal, a subpoena, a discovery request, or other lawful process.

Law Enforcement:

We may be required to disclose your protected information to law enforcement officials for law enforcement purposes, such as to: (1) respond to a court order; (2) locate or identify a suspect, fugitive, material witness, or missing person; (3) report suspicious wounds, burns or other physical injuries; or (4) report a crime or identify a victim.

Abuse or Neglect:

We may disclose your protected information to a government authority that is authorized by law to receive reports of abuse, neglect, or domestic violence. If we believe you have been a victim of abuse, neglect, or domestic violence, we may disclose your protected health information to a governmental entity authorized to receive such information.

To Avert a Serious Threat to Health or Safety:

We may disclose your protected information if disclosure is necessary to prevent or lessen a serious and imminent threat to your health or safety or the health or safety of another person or the public.

Research:

We may use and share your protected information for certain kinds of health or social services research. For example, a project may involve comparing the housing outcomes of all clients who received services from a referral agency to those received from another. Some research projects may require a special approval process and your written authorization. In some instances, the law allows us to do some research using your protected information without your approval.

Shared Medical Record/Health Information or Social Information Exchanges:

Some of our referral providers maintain protected information about their clients in a common electronic record that allows business associates to share protected information. We may participate in various electronic health or social information exchanges that facilitate the sharing of protected information among healthcare, health and human service agencies or other referral network providers.

Military:

If you are a member of the armed forces, we may use and disclose protected information as required by military command authorities, Department of Veteran Affairs, or other authorized federal officials.

National Security, Intelligence and Emergencies:

We may disclose health information about you to authorized federal officials for intelligence, counterintelligence and other national security activities authorized by law, and in emergencies.

Other Uses and Disclosures of Your Protected Information

Disclosures Requiring Your Written Authorization:

Most uses and disclosures of psychotherapy notes, substance use disorders, and uses and disclosures of protected health information, disclosures for marketing purposes and disclosures that constitute the sale of protected information require your ***written authorization***. A written authorization may be created in paper or electronic format. Once received, we will store a copy of your authorization electronically

YOUR RIGHTS REGARDING YOUR PROTECTED INFORMATION

The Right to Access Your Own Information

You have the right to inspect and copy your information for as long as we maintain it. All requests for access must be made in writing. We may charge you a nominal fee for each page copied and postage if applicable. You also have the right to ask for a summary of this information. If you request a summary, we may charge you a nominal fee for preparation of the summary and postage if applicable

Right to Request Restrictions:

You have the right to request certain restrictions on our use or disclosure of your protected information. We are not required to agree to your request in most cases. But if we agree to the restriction, we will comply with your written request unless the information is needed to provide you emergency treatment or we are required to disclose the information by law. We reserve the right to terminate any previously agreed-to restrictions (other than a restriction we are required to agree to by law). We will inform you of the termination of the agreed-to restriction and such termination will only be effective with respect to protected information created after we inform you of the termination.

Right to Request Confidential Communications:

You may request that we communicate with you in a certain manner or at an alternative location. For example, you may ask that we contact you only at home. Your request must be in writing and specify the alternative means or location for communicating with you. We will accommodate a request for confidential communications that is reasonable based on our system capabilities**.**

Right to be Notified of a Breach:

You have the right to be notified in the event that we (or one of our business associates) or referral providers discovers a breach of your unsecured protected information. We may notify you in writing or by email or other electronic means

Right to Inspect and Copy Your Record:

You have the right to inspect and receive a copy of protected information about you that may be used to make decisions about your health. A request to inspect or receive a copy of your records may be made by completing a Request for Release of Information form. For protected information in a designated record set maintained in electronic format, you can request an electronic copy of such information. If the information you request is protected health information, Care Connect may be required to forward your request to your healthcare provider for a response. There may be a charge for these copies.

Right to Amend:

You may ask us to amend, or correct your self-reported information. If the information was reported to us by your healthcare provider, a government agency, or other third party provider, you must contact that provider to correct or amend the information.

Right to an Accounting:

With some exceptions, you have the right to receive an accounting of disclosures of your protected information made for purposes other than treatment, payment, healthcare operations, disclosures excluded by law or those you have authorized. A nominal fee can be charged for the record search and preparation of the accounting of disclosures**.**

Right to Revoke Your Authorization:

You may revoke your written authorization or consent to share your information at any time in writing by mailing your request to the address listed below. If you revoke your written authorization or consent, it will be effective for future uses and disclosures of your protected information. Once your authorization has been revoked, we will render your record inaccessible and our referral partners will no longer be able to see your information in our system. However, the revocation will not be effective for information that we have used or disclosed to a referral partner in reliance on your authorization or consent and prior to receipt of your written revocation. After revocation, we will continue to store and use your information internally for our own business purposes, including auditing, accounting, training and quality improvement.

Complaints:

You may also file a complaint with us, or the Secretary of the U.S. Department of Health and Human Services if you feel that your rights have been violated. There will be no penalty or retaliation for you making a complaint. Our Street Address, Email Address and Phone Number:

Attn: Administration
North Coast Care Connect
2315 Dean St.
Eureka, CA 95501

Email: adminnorthcoastcareconnect@nchiin.org Phone Number: 707-443-4563 Ext 114

Right to Receive a Copy of this Notice:

You may request a paper copy of this Notice at any time, even if you previously agreed to receive this Notice electronically. You may also access this Notice on our website at: https://www.nchiin.org/cie

Requests:

Please submit all requests in writing to our Privacy Officer at:

North Coast Care Connect
Attn: Privacy Officer
2315 Dean St.
Eureka, CA 95501

ADDENDUM APPENDIX C

NORTH COAST HEALTH IMPROVEMENT AND INFORMATION NETWORK (NCHIIN)

POLICIES AND PROCEDURES

as of January 1, 2022

Prepared by: NCHIIN

This document contains the procedures to be followed by all NCHIIN North Coast Care Connect Participants to comply with privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Table of Contents

Definitions

"**Authorized User**" means an individual designated to have, on behalf of Participant, login and associated access to NCHIIN Systems for the purpose of providing Shared Information to NCHIIN Systems if Participant is a Data Provider and/or for the purpose of receiving Shared Information from NCHIIN if Participant is a Data Recipient, including without limitation an employee of Participant and/or a credentialed member of Participant's medical or other staff.

"**Breach of Privacy or Security**" is a use or disclosure of Shared Information other than in compliance with the Participation Agreement that either, (a) pursuant to applicable laws or regulations, must be reported to affected individuals and/or government officials, including without limitation federal or state data breach notification rules, or (b) that adversely affects either (i) the viability of NCHIIN or any Program; (ii) the trust among NCHIIN and Program Participants; or (iii) the legal liability of NCHIIN or any Program Participant.

"**North Coast Care Connect (Care Connect)**" refers to the NCHIIN System (dba North Coast Care Connect), which is provided by NCHIIN. North Coast Care Connect is a partnership of health and social and community services organizations that help individuals get services, work with individuals to understand their needs, and connect individuals to resources that can help them. North Coast Care Connect will provide information and other resources to promote Participant's performance and/or integration of health care and other services provided to individuals in Humboldt County who have consented to share their information with NCHIIN and its other Participants, using the North Coast Care Connect to provide Shared Information to health care and other providers participating in North Coast Care Connect, and connecting care teams to better link those Individuals to services.

"**Data Provider**" means a Participant or other party that provides Shared Information to North Coast Care Connect.

"**Data Recipient**" means a Participant or other party that obtains Shared Information from North Coast Care Connect.

"Individual," when that term is capitalized, means an individual person for whom Shared Information is maintained in North Coast Care Connect and/or who is or may be eligible to receive health care and/or other services from a Participant and, when that term is not capitalized, means any individual person, as appropriate to the context in which the term appears.

"**NCHIIN System**" refers to the secure database of information about Individuals who have consented to share their information with NCHIIN and its other Participants through the Community Information Exchange (CIE). NCHIIN provides the NCHIIN System (dba North Coast Care Connect) to facilitate the exchange of electronic information, coordinate care, and improve the quality of health in the community.

"**HIPAA Rules**" **or** "**HIPAA**" means the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 addressing the privacy and security of health information, the provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") 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") addressing the privacy and security of protected health information, and the regulations promulgated thereunder at 45 CFR Parts 160, 162, and 164.

"**Program Participant (Participant)**" means a party that entered into a Participation Agreement with NCHIIN, pursuant to which that party is to act as a Data Provider and/or a Data Recipient in connection with one or more Programs.

"Policies and Procedures" means this NCHIIN Participation Agreement Policies and Procedures.

"Protected Health Information (PHI)" means health information that contains individually identifiable information. Individually identifiable health information is information that can be linked to a particular person (e.g. names, social security numbers, addresses, or birth dates) and which relates to the individual's past, present, or future physical or mental health; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual.

"Program" means a program conducted or supported by NCHIIN and/or North Coast Care Connect pursuant to which health care and/or related services are provided to Individuals or information and/or other resources are provided to Participants to promote Participants' performance and/or integration of health care and other services provided to Individuals or connecting care teams to better link those Individuals to services, including such services as physical and mental health, substance abuse diagnosis and treatment, and housing and other social services.

"**Security Official**" means the individual or individuals responsible for implementing and maintaining Privacy and Security requirements, including but not limited to 45 CFR 164; SB 541; AB 211, ARRA/ HITECH ACT, and 42 CFR, Part 2 in relationship to data privacy.

"Shared Information" means information provided to NCHIIN by North Coast Care Connect Program Participants and others for inclusion in North Coast Care Connect.

"Substance Use Disorder (SUD)" means a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. This definition does not include tobacco or caffeine use. **"Substance Use Disorder (SUD) information"** means *any information that would identify a person as having or having had a Substance Use Disorder. This includes any of the individual identifiers, as well as anything that could reasonably be used to identify a specific individual. SUD information includes any information related to the treatment, diagnosis, or referral for a Substance Use Disorder.*

"**Unsuccessful Security Incident**" means any security incident (as defined at 45 C.F.R. § 164.304) that does not result in unauthorized access, use, disclosure, modification, or destruction of Shared Information or interference with system operations in an information system.

I. Purpose of Policies and Procedures

These Policies and Procedures are adopted by NCHIIN for the organization and maintenance of the NCHIIN System (dba North Coast Care Connect, Care Connect) and that apply to the conduct by NCHIIN, which includes but is not limited to and Participants as applicable to the Programs in which they participate, including without limitation any operations manual(s), privacy and/or security policy(ies), and technical specifications for access to the NCHIIN System.

II. Authorized Users

A. Identification of North Coast Care Connect Authorized Users

In preparation for Participant's record authorized user go-live, Participant managers will receive an email with a spreadsheet that contains the information submitted by their staff at the time of registering for training. The managers must review and verify that the information is correct, or amend as appropriate for accuracy, and approve their users before accounts are created.

Information is required at time of registration to create an end user account includes the following: First and last name, entity, job title, office phone number and email address, short bio, user name and user role.

Updates to this list should be sent to Partner Integration Manager to reflect changes. Note: Logins are deactivated after 90 days without a successful user login.

B. Termination of Authorized Users

Upon termination of employment for an authorized user or a change in responsibilities such that an authorized user no longer needs access to North Coast Care Connect to fulfill his/her responsibilities, the participant's security official must do the following immediately:

1. Remove the user ID, passwords and system privileges of such individual. All remote access privileges will also be disabled. All email accounts will either be disabled or forwarded to a security official address.

2. Contact the Partner Integration Manager to disable these account(s).

3. Retrieve any mobile computers or devices. The participant's security official will ask for and retrieve any back up media that may contain Protected Health Information (PHI). If these devices are the property of the individual leaving, the participant's security official will require evidence that the devices do not include any PHI.

4. Remove web access and access to any web-based applications such as web-based eligibility portals.

5. Remind the departing user of their continuing responsibility to protect sensitive information with which they have come in contact during their period of employment.

6. Collect and/or disable keys, tokens, badges and any other physical access control devices from the departing employee.

III. Security Measures with respect to access to and use of North Coast Care Connect

A. <u>User Access to Protected Health Information</u>

1. The Participant's security official along with the designated human resources officer will ensure that references were checked for staff accessing North Coast Care Connect applications.

2. The Participant's security official will ensure that, where possible, electronic PHI access control is granted based on the role or job description with respect to PHI. Access to PHI should be granted to users only as needed.

3. The Participant's security official will ensure that password protection and strength is in place on computers and mobile devices used by workforce members to access PHI.

4. The Participant's security official will ensure appropriate supervision of users and other workforce members who work with PHI (including the locations where PHI is accessed). Supervision may be provided by managers or supervisors in collaboration with the Participant's security official.

5. The Participant's security official will take all other actions appropriate to ensure that users comply with the requirements set forth in the NCHIIN Participation Agreement and these Policies and Procedures.

B. Provide and Maintain User Access to Protected Health Information

1. The Participant's security official will evaluate any new information systems or equipment that maintains, stores, creates or transmits electronic PHI and they will develop passwords, user ID/log-ons and system privilege codes if appropriate.

2. The Participant's service desk will assign (or request to assign) existing users and workforce members the appropriate access.

3. The Participant's security official will ensure that access is always a combination of passwords, user ID's, and system level privileges. Additionally, the participant's security official will maintain the job responsibility with respect to PHI data and use this to apply or deny additional application or data specific access.

4. Periodically, the Participant's security official will audit the access provided by the network and specific applications to ensure that workforce access levels are appropriate and reflect job/role changes, terminations, and so forth.

5. The Participant's security official will ensure that the fewest number of users possible are given administrator level access, or access to all files and systems.

6. When a user changes their job responsibilities, management will review the change. Where appropriate, if the change results in a reduction of responsibilities or access, the Participant's service desk or designee will modify the password and system privileges for the appropriate applications and data to restrict access. Where the change requires new access or increased access, the Participant's service desk will modify the password and system privileges for the appropriate applications and data to allow access.

IV. Software and Hardware Requirements for North Coast Care Connect

North Coast Care Connect (QS Systems NinePatch) is accessible via https://ninepatch.qssystems.net/NCCC .

The NinePatch Service & Care Coordination Platform is a web-based application. Use of the platform requires a supported web browser running on a computer with a minimum 4 GB of system memory (RAM) and a minimum 3 MBPS Internet connection. While the platform is based on HTML, which is supported by all web browsers, it leverages features that may not be common to all. Currently supported web browsers include:

- Google Chrome v94+
- Microsoft Edge v45+
- Mozilla Firefox v90+

V. Training

A. Privacy and Security Training:

1. The privacy or security official or designee will be responsible for establishing and maintaining a personnel training and awareness program. The privacy official or designee will identify the training resources as appropriate.

2. All personnel who assist in the performance of functions or activities on behalf of covered entities or access or disclose PHI must complete information Privacy and Security Training, at hire and/or prior to be given access to PHI/ePHI and at least annually. The content of the training must include HIPAA Omnibus Rule Employee Training & Implementation Protocols, at a minimum. Each staff member who receives information Privacy and Security Training must sign a certification, indicating the member's name and the date on which the training was completed.

3. Ensure that all new staff as well as temporary staff will have a basic orientation in the policies and procedures related to their job function which includes but is not limited to completing Privacy and Security Training.

4. Ensure all new staff understands the organization's computer, internet and email use policies and have signed to this effect.

5. New staff must complete privacy and security training for HIPAA training and complete the certification statement.

6. Train all personnel not to share their passwords or user ID's and to change them according to this Participant's procedure.

7. Train all personnel with access to electronic PHI to log off whenever they are away from their computer for prolonged periods of time.

8. Train personnel to use the security incident reporting form listed in Appendix C whenever a suspected or actual security incident occurs.

9. Maintain an end user Training Log and HIPAA certifications in the HIPAA records filing system central file.

B. North Coast Care Connect Training

North Coast Care Connect Training will be provided by NCHIIN training designees in partnership with QS Systems via a combination webinar and field support. Training will include, but is not limited to, patient look-up, scheduling patients, navigation within application, orientation to reporting functionality and configuration of notification rules.

VI. Use of Systems

A. Ownership and Rights in the NCHIIN Systems

Any shared information provided by Participant as a Data Provider and provided to other Program Participants in accordance with the NCHIIN Participation Agreement(s) shall be retained by and may be further used and disclosed by such other Participants in any lawful manner.

B. General North Coast Care Connect Data Transmission Security

Transmittal security: All HIPAA protected data will be encrypted using FIPS 140-2 certified algorithm prior to transmission.

C. Data Accuracy

1. Ensuring that data are accurate, relevant, timely, and complete for the purposes they are intended to be used should be a high priority issue.

2. Participants will maintain a proactive approach to data governance that requires establishing and regularly updating strategies for preventing, detecting, and correcting errors and misuses of data.

3. Participants will have policies and procedures in place to ensure that data are accurate, complete, timely, and relevant to stakeholder needs.

4. Regular data quality audits will be conducted to ensure that its strategies for enforcing quality control are up-to-date and that any corrective measures undertaken in the past have been successful.

D. Use and Disclosures for North Coast Care Connect and Participants

1. Access to PHI and SUD information should only be available to those staff members who require access to PHI and SUD information to perform their individual duties.

2. Regular data privacy audits will be conducted to ensure that Participants are requiring that users comply with the requirements set forth in the NCHIIN Participation Agreement and these Policies and Procedures and that any corrective measures undertaken in the past have been successful.

3. All SUD information disclosed out of the Part 2 Program (the Department or Program that holds itself out as providing SUD treatment, diagnosis, or referral) must be specifically consented to, in writing, by the individual.

   All disclosures of SUD information require the data recipient of SUD information may not redisclose that information to anyone unless permitted by Part 2 (e.g., explicitly allowed by signed release of information).

E. Individual Authorization and Control

1. North Coast Care Connect brings together Participants that serve their Individuals in different ways and that are subject to different legal frameworks affecting how they may use and disclose their Individuals' personal information. For example, Participants that are health care providers must comply with the HIPAA Privacy Rule, among others, while other Participants such as housing counselors do not. Therefore, North Coast Care Connect allows Individuals to choose whether or not to have their information (beyond what State and Federal laws allow Participant to share without authorization for some sharing of information) accessible through North Coast Care Connect. North Coast Care Connect permits information sharing without the Individual's authorization when applicable laws and regulations permit that sharing without authorization. Individuals may choose to authorize that expanded data sharing among Participants by completing the North Coast Care Connect Authorization Form. NCHIIN has developed this form and will be responsible for revising this form as necessary to comply with new laws, regulations, or changes to existing laws and regulations that apply the use and disclosure of Individuals' personal information by Participants. NCHIIN will notify all Participants if and when the forms are revised.

2. Each Participant is responsible, at the time of first contact, to notify Individuals of their right to choose to authorize expanded information sharing among Participants and to offer the opportunity to sign this form (available online and on paper). Other forms of authorization are not sufficient (for example, authorizations given by telephone or on other forms). The Participant is to discuss the authorization with the Individual and if necessary, help that Individual to make necessary selections and sign the document properly. At that time, the Participant will share with the Individual the current list of Participants who may receive the Individual's information as a result of that authorization. NCHIIN will maintain a current copy of this list at [insert webpage] and will notify Participants by e-mail when the list changes.

a) Online authorization forms are available within North Coast Care Connect. Participant sends a link to the form electronically to an Individual's email or smartphone for electronic signature. Individual makes selections on data sharing and "signs" electronically at which point the form is available for printing. North Coast Care Connect automatically populates record consistent with Individual data sharing choices and is effective immediately. The completed PDF form is available in the Individual's North Coast Care Connect record containing Individual's choices and electronic signature.

b) Paper versions of the forms may be provided to Individuals to sign and a copy will be provided to the Individual. The executed form is uploaded into North Coast Care Connect by Participant and selections entered into the system. North

Coast Care Connect automatically populates record with Individual data sharing choices and is effective immediately. Participant must ensure that the paper is uploaded and legible before destroying or storing according to Participant Policy.

North Coast Care Connect will maintain a record for each Individual of the authorizations they have given and will only permit Individuals' expanded data to be shared throughout North Coast Care Connect if the Individual has a current, legally compliant authorization on file.

c) Revocation of authorization:

(1) Revocation may be initiated verbally, with an email or a letter to a participant.

(2) Online revocation forms are available in North Coast Care Connect: https://www.nchiin.org/cie

When requested, Participant sends the form electronically to an Individual's email or smart phone for electronic signature. Individual makes selection to revoke the authorization and "signs" electronically to make effective immediately. The PDF form also becomes available to the Individual's record containing Individual's choices and electronic signature.

(3) If done via email or letter, the revocation must be submitted to the North Coast Care Connect Participant and include name, date of birth, and contact information. Each Participant shall upload the written request and attest/record all Individual decisions to exclude Information from North Coast Care Connect. Participant will enter the revocation in the North Coast Care Connect within 5 business days. Participant must ensure that the paper is uploaded and legible before destroying or storing according to Participant Policy.

3. Participants shall establish reasonable and appropriate processes to enable the exercise of an Individual's choice not to have information about him or her accessible through North Coast Care Connect. North Coast Care Connect will manage Individual authorizations and ensure access is blocked to an Individual's expanded data if that Individual has not authorized North Coast Care Connect to share their data.

VII. Privacy and Security of Shared Information

A. NCHIIN Compliance with Policies and Procedures

NCHIIN shall comply with NCHIIN Participation Agreement and the corresponding Policies and Procedures as indicated in this document. Further, it will comply with its organizational Privacy and Security Policies.

B. Notice of Privacy Practices

The North Coast Care Connect Notice of Privacy Practices may be found at: https://www.nchiin.org/cie

C. Security Incident Reporting and Response for NCHIIN and Participant

1. Security official of the party that sustained the security incident will coordinate review of the incident to establish if a possible HIPAA Breach has occurred.
2. Security official will follow all HIPAA and California breach notification requirements whenever a security incident is identified as a breach.
3. Use the Security Incident Form (Appendix C) and distribute copies to all personnel as well as instruct personnel and management on how to complete the form.
4. Train personnel to report both suspicious as well as actual incidents.
5. Security official (or designee) will review any incident report within twenty-four (24) hours of receipt. In the event of a violation that does not have an incident report; the security official will review the violation within twenty-four (24) hours and also document this using the incident report.
6. The security official will determine if the incident is an actual violation or just suspicious activity. If needed, the security official will contact the systems vendor for assistance.
7. The security official will address actual violations immediately based on the nature of the violation.
8. If a security incident occurs where PHI has been breached, the security official will investigate the breach immediately, and follow the HIPAA Breach Notification procedures, if applicable, and the applicable requirements of the Participation Agreement. The security official will take reasonable steps to determine the scope of the breach and restore the reasonable integrity of the data system. The security official, where appropriate, will contact the organization's attorney or outside

advisors to determine the most appropriate compliance plan, which will generally include notification of all affected patients.

9. If the security official, organization's attorney or outside consultants determine that PHI, medical information, personal information or health insurance information (as defined in SB1386 and AB1298) in an unencrypted form likely was accessed by an unauthorized person or otherwise breached and cannot demonstrate a low probability that the PHI was compromised, the security official will immediately notify law enforcement if criminal activity is involved; and, unless opposed by law enforcement, will notify all Individuals who had information on the PHI file/program that was breached, consistent with the requirements of SB1386 and AB1298.

10. The security official will update all procedures to ensure that security measures are enhanced to minimize the likelihood of future violation. The nature of the update will depend on the seriousness and extent of the problem.

11. The security official will ensure that all data has been restored and integrity checked if applicable.

12. The security official, in conjunction with the privacy official, will implement appropriate remediation and corrective action as a result of security incident responses

D. Unsuccessful Security Incident Reporting

NCHIIN and Participant shall annually (i.e., December year-end) provide a report base upon available information to the other describing in summary form the nature and extent of Unsuccessful Security Incidents concerning Shared Information or the Participant's access or use of the NCHIIN Systems experienced during the period covered by that report. The Participant report should be emailed to the NCHIIN Privacy Officer, at Privacy Officer at:

2315 Dean St.

Eureka, CA 95501

Phone: 707.443.4563 x114

VIII. Business Associate Agreement

If Participant is not a Covered Entity, NCHIIN is to act as the Business Associate of Participant pursuant to the HIPAA Rules; NCHIIN shall enter into a Business Associate Agreement with Participant in the form set forth **in Policies and Procedures Appendix A**. The terms of that

Business Associate Agreement shall supersede the terms of these Policies and Procedures with respect to the matters subject to that Agreement.

IX. Insurance

NCHIIN will require the Participant to secure and keep in force a minimum insurance coverage, limits and endorsements as detailed in **Policies and Procedures Appendix B: Insurance Requirements**

(Exhibit B: NCHIIN MINIMUM INSURANCE REQUIREMENTS).

X. Maintenance of Policies and Procedures

NCHIIN will monitor and remain informed of laws and regulations applicable to the programs and activities of NCHIIN contemplated hereunder, and to the enactment, amendment, and/or repeal of laws and regulations so applicable, and shall pursuant to Section 1.2 (Development and Dissemination of Policies and Procedures; Amendments) of the NCHIIN Participation Agreement amend the Policies and Procedures from time to time as NCHIIN determines necessary and appropriate to maintain compliance with all applicable laws and regulations.

XI. Subscription Fee

NCHIIN may modify or use a different fee structure or formula for calculating fees and the amount of the annual or other Fees from time to time, but fee changes shall not occur more often than once in any calendar year. Changes to fees shall become effective and binding on Participant after not less than sixty (60) days' notice to Participant. All fees payable shall be non-refundable in the event of an early Termination.

Policies and Procedures Appendix A – Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement ("BAA"), is entered into by and between North Coast Health Improvement and Information Network, dba North Coast North Coast Care Connect, ("Business Associate") and the Covered Entity or Business Associate named on the signature page hereto ("Covered Entity"), each a "Party" and collectively, the "Parties." This BAA shall be effective on the date indicated at the signature page hereto, or the date commensurate with the effective date of the Participation Agreement or other agreement entered into by the Parties ("Agreement") pursuant to which Business Associate will be granted access to protected healthcare information, (whichever effective date is earlier). ***This BAA applies to the parties only to the extent that a business associate relationship exists within the meaning of 45 CFR 160.03.***

Recitals

Whereas, at times, North Coast Care Connect, may serve as a Business Associate that creates, receives, maintains, stores, aggregates, transmits, or facilitates the exchange of protected health information ("PHI") for, behalf of and between "Covered Entities" or other Business Associates for Permitted Purposes.

Whereas, at various times, Business Associate may provide Services for, or on behalf of a Covered Entity that requires Business Associate to collect, store, transmit, retrieve, use or disclose an Individual's protected health information, orally, or in paper or electronic form. In doing so, it is the intent of each of the Parties to this Agreement to observe and faithfully perform the duties and obligations of a Business Associate, and Covered Entity, as the context may require, in accordance with the "Privacy Laws" and the following Terms and Conditions.

Now therefore, in light of the foregoing Recitals and for valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereto hereby agree as follows:

Terms and Conditions

1 Definitions.

1.1 Definition of Capitalized Terms. Unless otherwise defined in this BAA, capitalized terms shall have the meaning set forth in the Privacy Laws.

1.1.1 "Agreement" means and refers to collectively, the Participation Agreement and each statement of work, if any, and this BAA, or if there is no Participation Agreement, then Agreement means this BAA.

1.1.2 **“**Breach**”** as defined by 45 CFR §164.402 means the unauthorized acquisition, access, use, or disclosure of PHI or any activity that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

1.1.3 "Business Associate" as defined by 45 C.F.R. 160.13, includes any entity that creates, receives, maintains, or transmits protected healthcare information (“PHI”) on behalf of a Covered Entity.

1.1.4 “Business Associate Subcontractor” or “Subcontractor” means a contractor to Business Associate that performs services as a Business Associate as that term is defined in 45 CFR §160.103.

1.1.5 "Covered Entity" refers to a Health Plan, Health Care Clearinghouse, or Health Care Provider that transmits any protected healthcare information in electronic form in connection with a transaction covered by HIPAA and shall have the same meaning as the term "Covered Entity" as stated at 45 CFR §160.103.

1.1.6 “Participation Agreement” means and refers to the agreement between Business Associate and Covered Entity and each statement of work pursuant to which Business Associate agrees to perform Services that involve the use or disclosure of PHI.

1.1.7 “Permitted Purpose” means and refers to the purposes for which PHI may be used and disclosed under the Privacy Laws, including, without limitation, treatment, payment, healthcare operations, healthcare oversight, public health, emergency medical services and the determination of eligibility for and the delivery of government benefits to the Individual that is the subject of the PHI.

1.1.8 "Protected Healthcare Information" or "PHI" means any information, whether oral or recorded in any form or medium, including electronic PHI or “ePHI”: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term at 45 CFR §160.103.

1.1.9 “Privacy Laws" means and refers to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 CFR Parts 160, 162 and Subparts A, C, D and E of Part 164, the "HIPAA Regulations"), and the Health Information Technology for Economic and Clinical Health Act of 2009 (the “HITECH Act”) Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (February 17, 2009).

1.1.10 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System and shall have the meaning given to such term at 45 CFR §164.304.

1.1.11 "Services" shall mean, to the extent and only to the extent they involve the creation, use, storage, transmission, encryption, destruction or disclosure of PHI for a Permitted Use by a Business Associate or Business Associate Subcontractor under the Participation Agreement.

2 Compliance with Privacy Laws

2.1 Parties Mutual Obligation to Comply with Privacy Laws. The Parties to this BAA shall observe and comply with the Privacy Laws and faithfully perform the duties and obligations of a Business Associate, or Covered Entity, respectively as such terms may pertain to them from time to time under the Privacy Laws, at all times during the Term of this Agreement and for such period of time following termination as may be required by the Privacy Laws.

2.2 Effect of BAA. This BAA amends, supplements, and is made a part of any and all Agreements between North Coast Care Connect and the Covered Entity, to the extent North Coast Care connect is to perform Services as a Business Associate. To the extent the terms and conditions of the Participation Agreement are inconsistent or conflict with the terms of this BAA, this BAA shall govern.

3 Use and Disclosure of PHI

3.1 Permitted Uses and Disclosures. Business Associate may use or disclose PHI if necessary and consistent with 42 U.S.C Section 17935(b) only to the extent necessary to perform functions, activities or services specified in this BAA, or the Participation Agreement on behalf of Covered Entity, provided such use or disclosure would not violate the Privacy Laws, if done by Covered Entity.

3.2 Management and Administration. Except at otherwise indicated in this BAA, Business Associate may use and disclose PHI (a) to properly manage and administer Business Associate's business, and carry out Business Associate's legal responsibilities.

3.3 Data Aggregation. Business Associate may use and disclose PHI to provide Data Aggregation services relating to the Health Care Operations of the Covered Entity.

3.4 De-Identified. Business Associate may use PHI to de-identify the information in accordance with 42 CFR 164.514(a)-(c) for any lawful purpose.

3.5 Limited Data Set. Business Associate may request PHI in the form of a Limited Data Set, to be used for research, public health or health care operations.

3.6 Minimum Necessary. Business Associate shall limit access to PHI within its own workforce and place the same requirements upon its Business Associate Subcontractor's to those knowledgeable of the Privacy Laws and only on a need to know basis.

4 Obligations of Business Associate

4.1 Nondisclosure. Business Associate shall not use, access or disclose PHI other than as permitted or required by the Participation Agreement, this BAA or by the Privacy Laws.

4.2 Safeguards. Business Associate shall adopt, implement and update administrative, physical and technological safeguards that reasonably and appropriately protect the privacy, integrity, and security of PHI and to comply with the applicable standards of Subpart C of 45 CFR Part 164. Covered Entity shall have the right to audit these security controls and review Business Associates' written information privacy and security policies and procedures, from time to time upon not less than five (5) business days notice to Business Associate. Business Associate will implement technology or methodology specified by the Secretary pursuant to 42 USC Section 17932(h) that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

4.3 Report Unauthorized Use or Disclosures to Covered Entity. Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for by the Agreement that is not otherwise permitted by Law. In this regard, Business Associate will report Breaches of Unsecured ePHI as required at 45 CFR 164.410,

4.4 Business Associate Subcontractors. In accordance with 45 CFR 164.502(e) (1) (ii) and 164.308(b) (2), if applicable, Business Associate will take reasonable steps to ensure those of its

subcontractors, (and their employees or agents) that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to substantially the same restrictions, conditions, and requirements, including requirements for reporting any Breaches or Security Incidents as apply to Business Associate herein.

4.5 Accounting to Individual of Disclosures. Business Associate shall maintain, and within twenty (20) days of a written request, provide the information required or reasonably necessary to permit Covered Entity to satisfy its obligations under 45 CFR 164.528 to provide an accounting of disclosures to an Individual. Unless otherwise agreed, Business Associate shall not be required to provide an accounting of disclosures directly to the Individual, but shall forward such requests to Covered Entity.

4.6 Amendments to PHI. To the extent Business Associate maintains PHI in a central database on behalf of Covered Entity, Business Associate will make such amendments to PHI in a Designated Record Set as directed or agreed to by Covered Entity pursuant to 45 CFR 64.526.

4.7 Compliance Audit. Business Associate shall make its internal practices, books, and records available to the Secretary and/or Covered Entity upon request, for purposes of determining compliance with the Privacy Laws, and to investigate any Breach or Security Incident.

4.8 Marketing or Sale of PHI. Subject to the limitations set forth in Section 13405(d)(2) of the HITECH Act, and in compliance with 45 CFR Section 164.502(a)(5), except for compensation for services provided under the Participation Agreement, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI from a third party.

4.9 Indecipherable or Lost PHI. Business Associate shall take reasonable steps, at its sole cost and expense, to trace lost PHI or translate and recreate indecipherable transmissions of ePHI where such loss or corruption is the result of or related to a disruption or malfunction of Business Associate's internet connection, hardware, software or a breach of or defect in its security system.

4.10 Designated Record Set. Within ten (10) day of receiving a request, and to the extent Data is maintained by Business Associate, Business Associate shall make PHI available to Covered Entity in a Designated Record Set to permit Covered Entity to satisfy its obligations under 45 CFR 164.524.

4.11 Standard Transactions. To the extent Business Associate conducts Standard Transactions, Business Associate shall comply with the Privacy Laws and specifically the Administrative Requirements set forth at 45 CFR Part 162.

4.12 Covered Entity's Obligations. To the extent Business Associate is to carry out Covered Entity's obligations under 45 CFR Part 164, Subpart E, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

4.13 Export of PHI. Business Associate, its agents or Subcontractors shall not perform any services that require the export of PHI outside the United States of America without the prior written consent of the Covered Entity.

4.14 Notice and Opportunity to Oppose Disclosure. In the event Business Associate is required by law to disclose PHI pursuant to a court order or other legal proceeding or investigation, Business Associate shall promptly Notify Covered Entity of such requirement so as to afford Covered Entity sufficient time to take appropriate action to oppose the disclosure.

5 Covered Entity Obligations

5.1 Restriction on Use or Disclosure. Covered Entity will immediately notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR §164.522, to the extent that such restriction may affect Business Associate's (or that of its Subcontractor) use or disclosure of PHI.

5.2 Consent or Authorization. Covered Entity will not disclose or provide Business Associate or its Subcontractors access to PHI except to the extent Covered Entity is permitted or required to do so under the Privacy Laws or pursuant to the consent or authorization of the Individual (or his or her representatives) that is the subject of the PHI.

5.3 Notice of Privacy Practices. Covered Entity shall provide Business Associate with a copy of its most current Notice of Privacy Practices, and updates as and when made.

6 Breach or Security Incident

6.1 Breach or Security Incidents. Business Associate shall promptly notify Covered Entity as required by 45 CFR 164.410, but no later than five (5) business days after Business Associate becomes aware of a Breach or Security Incident. Business Associate shall be deemed to be aware of a Breach or Security Incident as of the first day on which such Breach or Security Incident is

actually known or reasonably should have been known by any of its officers, employees, agents or subcontractors.

6.2 Investigation and Corrective Action. The Parties will cooperate with each other in good faith in the investigation of the Breach or Security Incident. Business Associate will promptly take such steps as are reasonable to mitigate any harmful effects of such Breach or Security Incident and shall Notify Covered Entity, no later than twenty (20) days after discovery of the Breach or Security Incident of; (i) the identity of each Individual whose Unsecured PHI was accessed, acquired, used or disclosed as a result of the Breach, and
(ii) such other information required by the actions taken by Business Associate to mitigate any harmful effect of such Breach or Security Incident, and (ii) the corrective action such Party has taken or shall take to prevent future similar Breaches or Security Incidents, and (iii) any other action required by Applicable Laws pertaining to the Breach or Security Incident.

6.3 Notification To Individuals. Unless the parties agree in writing otherwise, Covered Entity shall provide Individuals affected by a Breach or Security Incident such notification required by the Privacy Laws.

6.4 Notification to Media. A notification required to be given to the public via the media pursuant to 45 CFR 164.406 shall be provided by Covered Entity, unless the parties agree in writing otherwise. Business Associate will not communicate with the media concerning a Breach or Security Incident unless directed to do so by Covered Entity in Writing.

7 Term and Termination

7.1 Term. The Term of this BAA shall commence on the Effective Date and terminate on the date that is commensurate with the Termination Date of the Participation Agreement, (as the same may be extended or renewed).

7.2 Termination for Cause. Either Party may terminate this BAA (and the Participation Agreement) immediately upon Notice for "Cause." "Cause" shall mean and refer to (i) a Party's failure to cure a material breach of this BAA within thirty (30) days of Notice of such breach; (ii) any act or omission of a Party resulting in a Breach or Security Incident, (iii) failure of Business Associate to provide the accounting of disclosures or security audit in a timely manner, (iv) failure of a Party

to take reasonable corrective action to prevent Breaches or Security Incidents. In addition, Covered Entity may terminate this BAA for any reason upon one (1) month's notice.

7.3 Obligations of a Party Upon Termination. Upon termination of this BAA for any reason, and with respect to PHI received solely from Covered Entity or created, maintained, or received by Business Associate solely for Covered Entity, Business Associate shall, if feasible, return to Covered Entity or (if agreed to by Covered Entity), destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for the proper management and administration of its business and legal responsibilities or for the Permitted Purposes for which such PHI was originally used or retained.

8 Miscellaneous Provisions

8.1 Contradictory Terms; Construction of Terms. Any capitalized term or provision of the Agreement that contradicts one or more terms and conditions of this BAA, including the definition of a Capitalized Term shall be superseded by the definitions and term and conditions set forth in this BAA for the purposes of complying with the Privacy Laws.

8.2 Amendment. This BAA shall be amended from time to time as is necessary in order for a Party to comply with the requirements of the Privacy Laws. All other amendments must be in writing and executed by both parties to be effective.

8.3 Interpretation**.** This BAA represents the Parties' entire understanding and supersedes any and all prior agreements between the Parties whether written or oral, as they may pertain to the subject matter of this BAA. Any ambiguity in this BAA or the Agreement shall be interpreted to permit or require compliance with the Privacy Laws. The terms and conditions stated in this BAA shall control over any conflicting or varying terms and conditions in the Participation Agreement.

8.4 No Agency. Nothing in this BAA is intended to create or imply an employment relationship, partnership or joint venture between Covered Entity and Business Associate. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the Parties and their respective successors and assigns, any rights, remedies obligations or liabilities.

8.5 Survival**.** Those obligations of a Party which by their meaning are intended to survive termination, including, but not limited to the obligations to protect the privacy and security of PHI from unlawful disclosure, shall continue in effect for a period of seven (7) years following termination.

8.6 Notice. Any Notice required to be provided to the other Party shall be in writing and shall be sent by first class certified U.S. Mail, return receipt requested, overnight courier and delivered to the address provided by such Party, or to such change of address as a Party may specify by Notice.

8.7 Severability**.** The provisions of this Agreement shall be severable, and the invalidity or unenforceability of any provision (or part thereof) of this Agreement shall in no way affect the validity or enforceability of any other provision (or remaining part thereof.) If any part of any provision contained in this Agreement is determined by a court of competent jurisdiction to be invalid, illegal or incapable of being enforced, the provision shall be interpreted in a manner so as to enforce it to the fullest extent permitted by law.

8.8 Attorney's Fees. Each party shall bear its own costs in connection with any legal action or proceeding brought to enforce, enjoin or interpret this Agreement or the rights and obligations of a Party hereto.

8.9 Jurisdiction/Venue. This BAA shall be governed by California law notwithstanding any conflicts of law provisions to the contrary. Venue for any legal proceeding brought to enforce, enjoin or interpret this BAA shall be conferred on the State or Federal Court situated in Humboldt County.

8.10 Counterparts**.** Any number of counterparts of this Agreement may be signed and delivered, each of which shall be considered an original and all of which, together, shall constitute one and the same Agreement.

IN WITNESS WHEREOF, the Parties identified below have executed this Business Associate Agreement.

BUSINESS ASSOCIATE:

Signature:

By:_____

Its:_____

Date:_____

Address For Notice:

COVERED ENTITY/BUSINESS ASSOCIATE:

Signature:

By: _____

Its: _____

Date:_____

Address For Notice:

Policies and Procedures Appendix B: Insurance Requirements

EXHIBIT B

NCHIIN MINIMUM INSURANCE REQUIREMENTS

Without limiting any other obligation or liability under this Agreement, the Participant, at its sole cost and expense, shall secure and keep in force during the entire term of the Agreement or longer, as may be specified below, the following minimum insurance coverage, limits and endorsements:

	TYPE OF INSURANCE COVERAGES	MINIMUM LIMITS
A	**Commercial General Liability** Premises Liability; Products and Completed Operations; Contractual Liability; Personal Injury and Advertising Liability	$1,000,000 per occurrence (CSL) Bodily Injury and Property Damage
B	**Workers' Compensation (WC) and Employers Liability (EL)** Required for all contractors with employees *(not required if contractor provides written verification it has no employees)*	WC: Statutory Limits EL: $1,000,000 per accident for bodily injury or disease

Policies and Procedures Appendix C

NORTH COAST CARE CONNECT

COMPUTER/INFORMATION SECURITY INCIDENT REPORT FORM

Participants shall report information system incidents to North Coast Care Connect within 48 hours in compliance with the Policy and Procedures. Please Print or Type your responses. If a question does NOT apply, enter "N / A" to signify not applicable.

Mail or Email Completed Form To: ATTN: Information Security Officer 2315 Dean Street Eureka, CA 95501 adminnorthcoastcareconnect@nchiin.org	Questions / Comments: Security Officer Phone: 707.443.4563 x114 2315 Dean St. Eureka, CA 95501

I. Participant Information		
Point(s) of Contact (First Name, Last Name, M.I.)	Participant/Agency Name	
Agency Address	City	Zip Code
Work Phone Number	Email Address	
Date of Report	Date of Incident	

II. Incident Information
Location(s) of Incident:
System(s) and/or Data Affected (e.g., CAD, RMS, File Server, etc.):
Method of Detection:
Nature of Incident:
Incident Description:
Actions Taken / Resolution:

III. Incident Report
1. How was the incident discovered? (e.g. via an audit trail, or accidental discovery)
2. What applications, systems and/or data were accessed? Did access include any personally identifying information? Is the hard drive encrypted? Provi description / list as to who you believe is affected or vulnerable to a similar incident.
3. When did the incident occur? Identify the time-frame and the operational phase (i.e., Was this a one-time occurrence or continuing? Could it occur any certain events trigger it?)
4. Why did this incident happen? What allowed this incident to occur? Were there policies in place which may be applicable to this incident? Should there controls in place which may help to prevent this type of incident from reoccurring?
5. What are the vulnerabilities and impacts associated with this incident? Describe what you believe are the vulnerabilities and impacts to other informati as a result of this incident.

POLICIES AND PROCEDURES APPENDIX D

COMMUNITY INFORMATION EXCHANGE

EXHIBIT D
MULTIPLE PROGRAM SCHEDULE

Contracting Organization

_____

Program 1 Name:

_____

Service Description:

_____

Seats/Users: _____

Additional Fee: _____

Program 2 Name:

_____

Service Description:

_____

Seats/Users: _____

Additional Fee: _____

Program 3 Name:
_____

Service Description:
_____

Seats/Users: _____

Additional Fee: _____

Program 4 Name:
_____

Service Description:
_____

Seats/Users: _____

Additional Fee: _____

Program 5 Name:
_____

Service Description:
_____

Seats/Users: _____

Additional Fee: _____

_____	_____
For NCHIIN	For _____