SOCIAL HEALTH INFORMATION EXCHANGE (SHIE)

DATA SHARING AGREEMENT (DSA)

POLICIES AND PROCEDURES

as of July 1, 2021

Prepared by: Alameda County Health Care Services Agency

This document contains the procedures to be followed by all Health Care Services Agency Social Health Information Exchange Data Sharing Agreement participants and Alameda County Health Care Services Agency personnel to comply with privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Content is based on Policies and Procedures purchased from PrivaPlan.

"AFBH Program" or "Adult Forensic Behavioral Health Program" means the Program pursuant to which each Data Provider provides specified Shared Information that HCSA shall provide to Alameda County Behavioral Health Care Services, or its designee, as a Data Recipient, for the purpose of providing mental health services in a coordinated and integrated manner for any Individuals who are inmates in the Santa Rita Jail and coordinating the care of those Individuals after their release.

"Authorized User" means an individual designated to have, on behalf of Participant, login and associated access to HCSA Systems for the purpose of providing Shared Information to the SHIE if Participant is a Data Provider and/or for the purpose of receiving Shared Information from the SHIE and/or the Community Health Record 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 this Data Sharing 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 HCSA or any Program; (ii) the trust among HCSA and Program Participants; or (iii) the legal liability of HCSA or any Program Participant.

"Care Connect Program" means the Program conducted by HCSA under the name "Alameda County Care Connect" or "Care Connect" pursuant to which HCSA will provide information and other resources to promote Participant's performance and/or integration of health care and other services provided to Individuals in Alameda County who are either eligible or enrolled in the Care Connect Program, using the Community Health Record to provide Shared Information to health care and other providers participating in the Care Connect Program, and connecting care teams to better link those Individuals to services, including physical and mental health, substance abuse diagnosis and treatment, and housing and other social services. The Care Connect Program also includes but is not limited to determining the eligibility for enrollment of, facilitating the enrollment of, and providing services to, Individuals participating in other comprehensive care management programs conducted in Alameda County by HCSA and/or the County of Alameda, including without limitation the Health Homes Program ("HHP"), Targeted Case Management ("TCM"), Full Service Partnerships ("FSP"), Level 1 Service Teams ("Service Teams"), and care management through the Drug Medi-Cal Organized Delivery System ("DMC-ODS").

"Care Connect+ Program" means the data exchange, data analytics, and provider coordination activities facilitated by HCSA to support services and programs benefiting Medi-Cal (including Medi-Cal/Medicare) and uninsured residents of Alameda County for whom information exists in the SHIE.

"Community Health Record" means the electronic community health record maintained by HCSA that contains Shared Information obtained from the SHIE and/or other sources that is made available to specified Participants in connection with their participation in a specified Program, such as, without limitation, the Care Connect+ Program and AFBH Program. The Community Health Record is not to be a "qualified electronic health record," as defined at Section 3000 of the HITECH Act (42 USC § 300jj).

"Data Provider" means a Participant or other party that provides Shared Information to the SHIE.

"Data Recipient" means a Participant or other party that obtains Shared Information from the SHIE and/or the Community Health Record.

"Drug Medi-Cal Organized Delivery System (DMC-ODS)" means a continuum of care modeled after the American Society of Addiction Medicine Criteria for substance use disorder treatment services, enables more local control and accountability, provides greater administrative oversight, creates utilization controls to improve care and efficient

use of resources, implements evidenced based practices in substance abuse treatment, and coordinates with other systems of care.

"Individual," when that term is capitalized, means an individual person for whom Shared Information is maintained in the SHIE 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.

"Full Service Partnerships (FSP)" means Adult Full Service Partnership (FSP) programs designed for adults ages 26-59 who have been diagnosed with a severe mental illness and would benefit from an intensive service program.

"**HCSA Systems**" means the technology used by HCSA to operate a SHIE, the Community Health Record and/or SHIE, to receive Shared Information from Data Providers for inclusion in the SHIE, and to provide Shared Information to Data Recipients from the SHIE or the Community Health Record, as described in the Policies and Procedures.

"**Health Homes Program**" or (HHP) is designed to serve eligible Medi-Cal beneficiaries with multiple chronic conditions who are frequent utilizers and may benefit from enhanced care management and coordination. The HHP coordinates the full range of physical health, behavioral health, and community-based long-term services and supports (LTSS) needed by eligible beneficiaries.

"**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.

"Level 1 Service Teams" means Multidisciplinary Service Teams that coordinate community-based services to provide individually-customized mental health care for people experiencing frequent setbacks or persistent challenges to their recovery. Coordinating care includes traditional mental health services while encompassing primary healthcare, housing, transportation, social relationships, and community participation.

"**Program Participant (Participant)**" means a party that entered into a SHIE Data Sharing Agreement with HCSA, 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 SHIE Data Sharing 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 HCSA and/or the County of Alameda 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, including without limitation the Care Connect+ Program and the AFBH Program.

"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.

"SHIE" means the electronic facilities maintained by HCSA for the collection, storage, and sharing of Shared Information..

"Shared Information" means information provided to HCSA by Program Participants and others for inclusion in the SHIE and/or the Community Health Record.

"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.

"Targeted Case Management (TCM) Program" means a program that reimburses participating counties for the federal share of costs (typically 50%) for case management services provided to Medi-Cal beneficiaries in specific target populations. Participating Local Governmental Agencies (LGAs) use their certified public expenditures (CPEs) to draw down federal funds.

"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 HCSA for the organization and maintenance of the SHIE and including without limitation the Care Connect+ Program and AFBH Program, and that apply to the conduct by HCSA, which includes but is not limited to AFBH authorized users, 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 HCSA Systems.

II. Authorized Users

A. Identification of Community Health Record Authorized Users

In preparation for Participant's CHR 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 a CHR 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.

*First Name	*Last Name	*Email	*Registration Date	Phone	*Organization	*Job Title	Work Address	NPI	Other Worksite Addresses	*Program or Department	Attend Annual HIPAA Training (Y/N)	*Supv. Last Name	*Supv. First Name	*Supv. Email	Supv. Phone	Supv. Title

* Required fields at time of registration in order to create an end user account.

Updates to this list should be sent to Care Connect Help Desk at CareConnectHelp@acgov.org as 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 the SHIE and/or the CHR 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 HCSA Care Connect Help Desk at CareConnectHelp@acgov.org 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 his/her continuing responsibility to protect sensitive information with which he/she has come in contact during his/her 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 the HCSA System

A. User Access to Protected Health Information

1. The Participant's security official along with the designated human resources officer will ensure that references were checked for staff accessing CHR 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 SHIE Data Sharing 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 he/she 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 e.g. access to CHR) 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 document 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 (such as Active Directory) 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 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 CHR

CHR system (Thrasys SyntraNet) is accessible via_https://shie.accareconnect.org/. Evergreen version of the major browsers are acceptable (i.e., Chrome, Firefox, Safari, Edge).

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 and 42 CFR Part 2 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 A 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. CHR Training

CHR Training will be provided by HCSA training designees in partnership with Thrasys via a combination of classroom, 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 HCSA Systems

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

B. General CHR Data Request, Transmission, Frequency and Security

1. HCSA and Participant shall submit a data request with specifics on:

a) Requesting Organization
b) Disclosing Entity (DE)
c) Date of Request:
d) Request and Purpose
e) Data Recipient (Recipient)
f) Test File Due
g) Frequency of data needed
h) Timeframe for data needed
i) Recipient Contacts
j) Recipient Organization
k) Recipient Phone and Email
l) DE Contacts
m) DE Organization
n) DE Phone and Email
o) DE Data Systems/Sources
p) DE Individual Population
q) DE Data Fields and Format

The preferred data request form is supplied in Appendix D.

2. General Transmittal Methods Supported by HCSA:

☒ FTP
☒ VPN TUNNEL
- HL7

3. General Transmittal Frequency (Unless otherwise agreed upon):

☒ Daily	☐ Weekly	☐ Monthly
☐ Annually	☐ As Needed/On request	☐ One-time
☐ Other_	☐ Data will not be transmitted; users will access data.	

4. 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 HCSA 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. Routine requests for PHI that are not related to treatment shall be periodically reviewed to ensure that only the information reasonably necessary to accomplish the purpose of the request is provided. Disclosure of PHI is subject to the separate Use and Disclosure procedure. Disclosure of PHI specifically authorized by the patient is not subject to Minimum Necessary rules (45 CFR 164.502(b), 164.514(d)).

3. Every non-routine request for PHI that is not related to treatment shall be reviewed to ensure that only the information reasonably necessary to accomplish the purpose of the request is provided. Disclosure of PHI is subject to the separate Use and Disclosure procedure. Disclosure of PHI specifically authorized by the patient is not subject to Minimum Necessary rules. Disclosure of PHI for the purpose of a legally required HIPAA compliance audit is not subject to Minimum Necessary rules.

4. When a request for disclosure of PHI is received, as necessary determine that a valid authorization is in effect for disclosures covered by an authorization on file. Upon validation, disclose the records according to the specifics of the authorization only.

5. 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 for SUD information must utilize a SUD release of information form. and 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. The SHIE 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, the SHIE 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 the SHIE. The SHIE 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 Alameda County Information Sharing Authorization (ISA) Form and Substance Use Disorder ("SUD") Release of Information (ROI) Form as applicable. HCSA has developed these forms and will be responsible for revising those forms 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. HCSA 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 these forms (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 ISA and/or SUD ROI, as the case may be, 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. HCSA will maintain a current copy of this list at www.accareconnect.org/organizations, and will notify Participants by e-mail when the list changes

   There are two means of capturing an Individual authorization (unless the Individual declines).

a) Online consent forms are available within the SHIE (i.e., Alameda County ISA, SUD ROI). Participant sends the blank form electronically to an Individual's email or smartphone for electronic signature via DocuSign. Individual makes selections on data sharing and "signs" electronically. The SHIE automatically populates record consistent with Individual data sharing choices and is effective immediately. The completed PDF form also becomes available to the Individual's Community Health Record containing Individual's choices and electronic signature. The Participant will print a copy of the executed form for the Individual.

b) Paper versions of the forms may be provided to Individuals to sign. The executed form is uploaded into the SHIE by Participant and selections entered into CHR. The CHR 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.

The SHIE will maintain a record for each Individual of the authorizations he/she has given and will only permit Individuals' expanded data to be shared throughout the SHIE if the Individual has a current, legally compliant authorization on file.

c) Revocation of authorization:

i. Online revocation forms are available in the SHIE. 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 Community Health Record containing Individual's choices and electronic signature.

ii. If done via email or letter, the revocation must be submitted to the SHIE 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 the SHIE. Participant will enter the revocation in the SHIE within 3 business days. Participant must ensure that the paper is uploaded and legible before destroying or storing according to Participant Policy.

iii. ISA revocation must be done in writing using options "i." or "ii" above

iv. SUD ROI, when it becomes available, may be revoked according to "i." and "ii." above or verbally by talking with their treating provider over phone or in-person. The treating provider (Participant) will be able to record some details about the conversation (phone call or in-person conversation) on the CHR and confirm with electronic attestation. If a SUD ROI is revoked verbally by an Individual, the Participant informed of such revocation is responsible for making the appropriate electronic attestation consistent with the timeline specified in "ii" above.

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 the SHIE. The SHIE will manage Individual authorizations and ensure access is blocked to an Individual's expanded data if that Individual has not authorized the SHIE to share his/her data.

VII. Privacy and Security of Shared Information

A. HCSA Compliance with Policies and Procedures

HCSA shall comply with SHIE Data Sharing 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

For the time being, HCSA does not require the use of a specific Notice of Privacy Practices, if Participant is a member of the Organized Health Care Arrangement.

C. Security Incident Reporting and Response for HCSA 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. Customize the Security Incident Form (Appendix A) 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 Data Sharing 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

HCSA 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 HCSA Systems experienced during the period covered by that report. The Participant report

should be emailed to the HCSA Chief Compliance and Privacy Officer, at HCSA.Compliance@acgov.org.

VIII. Business Associate Agreement

If Participant is not participating in the Care Connect+ Organized Health Care Arrangement (OHCA) then HCSA is to act as the Business Associate of Participant pursuant to the HIPAA Rules, HCSA shall enter into a Business Associate Agreement with Participant in the form set forth in Appendix B. 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

HCSA will require the Participant to secure and keep in force a minimum insurance coverage, limits and endorsements as detailed in Appendix C (Exhibit C COUNTY OF ALAMEDA MINIMUM INSURANCE REQUIREMENTS).

X. Maintenance of Policies and Procedures

HCSA will monitor and remain informed of laws and regulations applicable to the programs and activities of HCSA contemplated hereunder, and to the enactment, amendment, and/or repeal of laws and regulations so applicable, and shall pursuant to Section 2.1 (Development and Dissemination of Policies and Procedures; Amendments) of the SHIE Data Sharing Agreement amend the Policies and Procedures from time to time as HCSA determines necessary and appropriate to maintain compliance with all applicable laws and regulations.

XI. Subscription Fee

Each Participant shall pay a one-time fee of $5.00 to access the SHIE.

Appendix A: Security Incident Report Form

Security Incident Report

Name of Organization:_____

Date completed:_____
Name of person reporting incident:_____

Describe the incident:

_____
_____
_____
_____
_____
_____

Was incident (check one):

- ❑ Suspected
- ❑ Actual

Date and time or estimate of incident:

_____

Location (include workstation number or location):
_____ Was any electronic PHI (check one):

- ❑ Taken
- ❑ Transferred
- ❑ Corrupted
- ❑ Accessed

==========

Office Use:

Was this an (check one)**:** ❑ **Administrative,** ❑ **Physical, or**
❑ **Technical violation?**

Has the incident been verified? Y/N
When: _____
By whom:_____
Who has been identified as the individual responsible for committing the incident?

_____
_____

Describe the corrective action plan to mitigate:

_____
_____
_____

Are sanctions applied? Y/N

<u>30 Day Tracking:</u>

Has 30 day follow up and tracking been done? Y/N
Is the corrective action plan in place? Y/N
Are modifications needed? Y/N

Appendix B: Alameda County Business Associate Agreement

County of Alameda
Health Care Services Agency

HIPAA Business Associate Agreement for
SHIE Data Sharing Agreement

This HIPAA Business Associate Agreement ("Business Associate Agreement") is hereby incorporated into and made a part of the SHIE Data Sharing Agreement ("Data Sharing Agreement") by and between the County of Alameda Health Care Services Agency ("HCSA" or "Business Associate") and the HIPAA covered entity identified on the Signature Page hereto as a "Participant" under the Data Sharing Agreement ("Participant" or "Covered Entity"). This Business Associate Agreement is effective as of the effective date of the Data Sharing Agreement.

RECITALS

A. HCSA and Participant anticipate that, pursuant to the Data Sharing Agreement, HCSA shall create, receive, maintain, and/or transmit Protected Health Information in the performance of a function, service, or activity performed by HCSA for or on behalf of the Participant, and that HCSA therefore shall perform as a Business Associate with respect to the Participant;

B. Covered Entity and Business Associate intend to protect the privacy and provide for the security of Protected Health Information created, received, maintained, and/or transmitted by Business Associate for or on behalf of Covered Entity pursuant to the Data Sharing Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act"), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations"), and other applicable laws; and

C. The Privacy Rule and the Security Rule in the HIPAA Regulations require Covered Entity to enter into a contract, containing specific requirements, with Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and as contained in this Business Associate Agreement.

AGREEMENT

Section 1
Definitions

1.1 Capitalized terms used, but not otherwise defined, in this Business Associate Agreement shall have the same meaning as those terms are defined in the HIPAA Regulations. In the event of an inconsistency between the provisions of this Business Associate Agreement and the mandatory provisions of the HIPAA Regulations, as amended, the HIPAA Regulations shall control. Where provisions of this Business Associate Agreement are different than those mandated in the HIPAA Regulations, but are nonetheless permitted by the HIPAA Regulations, the provisions of this Business Associate Agreement shall control. All regulatory references in this Business Associate Agreement are to HIPAA Regulations unless otherwise specified.

1.2 The following terms used in this Business Associate Agreement shall have the same meaning as those terms in the HIPAA Regulations: Data Aggregation, Designated Record Set, Disclosure, Electronic Health Record, Health Care Operations, Health Plan, Individual, Limited Data Set, Marketing, Minimum Necessary, Minimum Necessary Rule, Protected Health Information, and Security Incident. The following term used in this Business Associate Agreement shall have the same meaning as that term in the HITECH Act: Unsecured PHI.

1.3 Specific Definitions.

1.3.1 "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. section 160.103, the HIPAA Regulations, and the HITECH Act, and in reference to a party to this Business Associate Agreement shall mean HCSA. "Business Associate" shall also mean any subcontractor that creates, receives, maintains, or transmits PHI in performing a function, service, activity delegated by Business Associate.

1.3.2 "Contractual Breach" shall mean a material failure to perform the contractual obligations set forth in this Business Associate Agreement.

1.3.3 "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. section 160.103, and in reference to the party to this Business Associate Agreement shall mean the Participant.

1.3.4 "Data Sharing Agreement" shall mean the SHIE Data Sharing Agreement between HCSA and the Participant, into which this Business Associate Agreement is incorporated by reference.

1.3.5 "Electronic Protected Health Information" or "Electronic PHI" means Protected Health Information that is maintained in or transmitted by electronic media.

1.3.6 "Business Associate Agreement" shall mean this HIPAA Business Associate Agreement. *HIPAA.*

1.3.7 "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

1.3.8 "HIPAA Breach" shall mean a breach of Unsecured Protected Health Information as defined in 45 C.F.R. section 164.402.

1.3.9 "HIPAA Regulations" shall mean the regulations promulgated under HIPAA by the U.S. Department of Health and Human Services, including those set forth at 45 C.F.R. Parts 160 and 164, Subparts A, C, D, and E.

1.3.10 "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act").

1.3.11 "PHI" shall mean Protected Health Information that Business Associate creates, receives, maintains, and/or transmits in the performance of a function, service, or activity for or on behalf of Covered Entity pursuant to the Data Sharing Agreement, and that is held by Business Associate or a Subcontractor of Business Associate.

1.3.12 "Privacy Rule" and "Privacy Regulations" shall mean the standards for privacy of individually identifiable health information set forth in the HIPAA Regulations at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

1.3.13 "Secretary" shall mean the Secretary of the United States Department of Health and Human Services ("DHHS") or his or her designee.

1.3.14 "Security Rule" and "Security Regulations" shall mean the standards for security of Electronic PHI set forth in the HIPAA Regulations at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Section 2
Permitted Uses and Disclosures of PHI by Business Associate

Business Associate may only Use or Disclose PHI:

2.1 As necessary to perform functions, services, or activities for, or on behalf of, Covered Entity as specified in the Data Sharing Agreement, provided that such use or Disclosure would not violate the Privacy Rule if done by Covered Entity;

2.2 As required by law; and

2.3 For the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Section 3
Protection of PHI by Business Associate

3.1 Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording and electronic display, by Covered Entity or its operating units to Business Associate, or is created or received by Business Associate on Covered Entity's behalf, shall be subject to this Business Associate Agreement.

3.2 Business Associate agrees to not use or further disclose PHI other than as permitted or required by the HIPAA Regulations, this Business Associate Agreement, or as required by law. Business Associate may not use or disclose PHI in a manner that would violate the HIPAA Regulations if done by Covered Entity.

3.3 Business Associate shall Use, Disclose, or request only the minimum PHI necessary to accomplish the intended purpose of that Use, Disclosure, or request.

3.4 Business Associate shall use appropriate administrative, physical and technical safeguards, and comply with the Security Rule and HIPAA Security Regulations with respect to Electronic

PHI, to prevent the use or Disclosure of the PHI other than as provided for by this Business Associate Agreement.

3.5 Business Associate shall report to Covered Entity promptly any Security Incident or unauthorized Use or Disclosure of PHI. Notwithstanding the foregoing, Covered Entity and Business Associate hereby acknowledge and agree that Unsuccessful Security Incidents (as defined below) are anticipated to occur from time to time. Covered Entity and Business Associate hereby agree that this Section 3.5 shall satisfy Business Associate's obligations to report Unsuccessful Security Incidents to Covered Entity as contemplated by 45 C.F.R. section 164.314(a)(2)(i)(C), and that no additional reports thereof 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, disclosure, modification, or destruction of electronic PHI or any interference with system operations in Business Associate's information system.

3.6 Business Associate shall report to Covered Entity without unreasonable delay and in no case later than thirty (30) calendar days after discovery of any Breach of Unsecured PHI. Business Associate's report shall include, as and when and to the extent available, all of the information required to be reported to Covered Entity pursuant to 45 C.F.R. section 164.410(c). The provisions of Section 12.3 (Limitation on Damages) of the Data Sharing Agreement notwithstanding, the parties shall be responsible for providing or bearing the cost of any legally required notification and identity theft protection and mitigation services resulting from a breach for which notice is required under federal or state law, in accordance with their respective roles and legal responsibilities in the relevant events.

3.7 Business Associate shall require any Subcontractor of Business Associate that creates, receives, maintains, or transmits PHI for or on behalf of Business Associate to agree in writing to the same restrictions and conditions that apply to Business Associate with respect to that PHI pursuant to this Business Associate Agreement.

3.8 Business Associate shall make its internal practices, books, and records relating to the use and Disclosure of PHI the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Regulations.

3.9 To the extent that Business Associate is required to carry out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations.

Section 4
Individual Control over PHI

4.1 Business Associate shall within a reasonable period of time following Covered Entity's request make available to Covered Entity PHI held by Business Associate in a Designated Record Set as necessary for Covered Entity to satisfy Covered Entity's obligations under 45 C.F.R. section 164.524.

4.2 Business Associate shall maintain and within a reasonable period of time following Covered Entity's request make available the information required to provide an accounting of Disclosures to an Individual as necessary to satisfy Covered Entity's obligations under 45 C.F.R. section 164.528.

4.3 Business Associate shall within a reasonable period of time following Covered Entity's request make any amendment(s) to PHI held by Business Associate in a Designated Record Set as directed or agreed to by Covered Entity pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. section 164.526.

Section 5
Termination

5.1 A Contractual Breach by Business Associate of this Business Associate Agreement shall constitute a material breach of Business Associate's obligations under the Data Sharing Agreement and be grounds for termination of this Business Associate Agreement and the Data Sharing Agreement in accordance with the applicable provisions of the Data Sharing Agreement.

5.2 In the event of the termination or expiration of this Business Associate Agreement, Business Associate shall return or destroy all PHI held by Business Associate or its Subcontractors, if feasible to do so. If Business Associate determines that returning or destroying PHI is infeasible, Business Associate shall notify Covered Entity of the conditions making return or destruction infeasible and extend the protections of this Business Associate Agreement to such PHI and limit further uses and Disclosures to those purposes that make the return or destruction of the information infeasible.

Section 6
Miscellaneous

6.1 A reference in this Business Associate Agreement to a section in HIPAA, the HIPAA Regulations, or the HITECH Act means the section as in effect or as amended, and for which compliance is required.

6.2 The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of HIPAA, the HIPAA Regulations, and the HITECH Act.

6.3 Except as expressly provided herein or expressly stated in the HIPAA Regulations, the parties to this Business Associate Agreement do not intend to create any rights in any third parties.

6.4 The provisions of this Business Associate Agreement are intended to establish the minimum requirements regarding Business Associate's use and Disclosure of PHI under HIPAA, the HIPAA Regulations and the HITECH Act. The use and Disclosure of individually identified health information is also covered by applicable California law, including but not limited to the Confidentiality of Medical Information Act (California Civil Code section 56 *et seq.*). To the extent that California law is more stringent with respect to the protection of such information, applicable California law shall govern Business Associate's use and Disclosure of confidential information related to the performance of this Business Associate Agreement.

6.5 Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the HIPAA Regulations, the HITECH Act, and in favor of the protection of PHI.

By the following signatures of their duly authorized representatives, Covered Entity and Business Associate have entered into this Business Associate Agreement as of the Effective Date described above.

Signature Page Follows
County of Alameda
Health Care Services Agency

HIPAA Business Associate Agreement for
SHIE Data Sharing Agreement

Signature Page

County of Alameda Health Care Services Agency ("Business Associate")	[*Name of Participant*] ("Covered Entity")
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Appendix C: Insurance Requirements

EXHIBIT C
COUNTY OF ALAMEDA 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 consultant provides written verification it has no employees)*	WC: Statutory Limits EL: $1,000,000 per accident for bodily injury or disease
C	**Cyber Liability** Insurance. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Participant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.	$2,000,000 per occurrence $2,000,000 project aggregate

Appendix D: Data Request Form

DATA REQUEST FORM

Requesting Organization	
Disclosing Entity (DE)	
Date of Request:	
Request and Purpose	
Data Recipient (Recipient)	
Test File Due	
Frequency of data needed	
Timeframe for data needed	
Recipient Contacts	
Recipient Organization	
Recipient Phone and Email	
DE Contacts	
DE Organization	
DE Phone and Email	
DE Data Systems/Sources	
DE Patient Individual Population	
DE Data Fields and Format	
File Submission Mode	