

**PUBLIC PROTECTION, JUSTICE & HEALTH COLLABORATIVE
DATA SHARING AGREEMENT
FOR CRIMINAL JUSTICE INFORMATION**

This Public Protection, Justice & Health Collaborative Data Sharing Agreement for Criminal Justice Information (“DSA”) is made and entered into by and between the following parties:

Alameda Alliance for Health (“AAH”)
Alameda County Probation Department (“Probation”)
Alameda County Sheriff’s Office (“ACSO”)
Alameda County Social Services Agency (“SSA”)
California Health Policy Strategies, LLC
Wendy Still, an individual
Wendy Ware, an individual

RECITALS

1. The Chair of the Public Protection Committee, Supervisor Richard Valle, District 2, established the Public Protection, Justice & Health Collaborative (“PPJHC”) in January 2022.
2. The objective of the PPJHC is to create a seamless and robust service delivery model for the population involved with the justice system by:
 - a. Identifying and leveraging data sources;
 - b. Aligning and coordinating existing initiatives and systems;
 - c. Assessing existing gaps and opportunities for expansion of services;
 - d. Leveraging state and federal funding opportunities; and
 - e. Eliminating duplication of effort and barriers to success.
3. The PPJHC is composed of four members as described below, each responsible for a Service Area or Initiative:

PPJHC Member	Title	County Agency	Service Area or Initiative
Dr. Kathleen Clanon	Agency Medical Director	Alameda County Health Care Services Agency	Health and Homeless Service Area
Dr. Karyn Tribble	Director	Alameda County Behavioral Health Care Services	Care First/Jails Last Initiative
Scott Coffin	Chief Executive Officer	Alameda Alliance for Health	CalAIM Initiative

Wendy Still	Special Advisor to the Public Protection Committee	Alameda County Board of Supervisors, District 2	Reimagine Adult Justice Initiative
-------------	--	---	------------------------------------

4. The four Service Areas or Initiatives are described below:

Service Area or Initiative	Brief Description of Service Area or Initiative
Health & Homelessness Service Area	Consists of three related areas: (1) Alameda County Health Care for the Homeless, a federally-funded health center program focused on improving the health of individuals who are homeless or at-risk of becoming homeless by ensuring access to culturally-informed, whole-person health care and housing services; (2) Health Program of Alameda County provides healthcare for low income individuals who are uninsured, to include the population involved with the justice system; and (3) Health Measure Pilot Program which expands access to healthcare services to formerly incarcerated populations through pre-release, post-release and wraparound services.
Care First/ Jails Last Initiative	This initiative calls for the just and equitable transformation of criminal justice, behavioral health, and wraparound services to reduce the number of individuals in the Santa Rita Jail with mental illness, substance use, and co-occurring disorders.
CalAIM Initiative	Alameda County's CalAIM initiative strives to leverage local, state and federal funding opportunities to align services for supporting the re-entry population with serious behavioral challenges and those experiencing homelessness.
Reimagine Adult Justice	The ultimate goal of RAJ is to assess and inventory current existing justice related diversion programs and identify gaps and opportunities that will reduce a reliance on incarceration. The objectives associated with this initiative will be accomplished through 12 elements that will explore areas related to mental health, behavioral health, pretrial, re-entry services and programs associated with those in-custody and in the community, and the potential establishment of civilian oversight of the Alameda County Sheriff's Department.

5. The PPJHC will report its progress to the Board of Supervisors, Public Protection Committee, and the Community Corrections Partnership Executive Committee, as needed.
6. Probation and ACSO find it necessary to disclose clients' identifiable information to Data Recipients for Data Recipients to fulfill the objectives of the PPJHC as described above.

Now, therefore, the parties hereby agree as follows:

A. PURPOSE

The purpose of the DSA is to establish clear confidentiality rules for the data disclosed by Probation and ACSO, and redisclosed by Data Recipients, under this Agreement. The disclosed data includes identifiable information maintained in the Consolidated Records Information Management System (“CRIMS”) and Enterprise Supervision.

B. DEFINITIONS

“Agreement” means this DSA, including all documents attached or incorporated by reference.

“Consolidated Records Information Management System” or “CRIMS” is a countywide Intranet browser-based software application that serves as a criminal justice information portal, facilitating information sharing among all participating justice partners in Alameda County. The software has been designed using modern technologies and practices, promoting inter-operability between a variety of criminal justice computer systems within and outside Alameda County. These systems include but are not limited to Records Management System information provided by participating law enforcement agencies, Criminal Oriented Records Production Unified System, Automated Warrant System, Multi-Agency Unified Imaging System, Enterprise Geographic Information System, Alameda County Assessor’s Office, Alameda County Public Works and the California Department of Justice (DOJ). The system makes criminal justice information more readily available to the local justice partners, including the officer on the street.

“Criminal Offender Record Information” means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. (California Penal Code §§ 11075, 13102.)

“Data Discloser” means a signatory to this Agreement that discloses Shared Data under this Agreement. (See Section D.)

“Data Encryption” means ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

“Data Recipient” means a signatory to this Agreement that either receives Shared Data from ACSO or Probation directly or receives Shared Data via redisclosure by another Data Recipient. (See Section D.)

“Data Storage” means the state data is in when at rest, i.e., when it is not being used, viewed or analyzed.

“Data Transmission” means the methods and technologies used to move a copy of the data between systems, networks, and/or workstations.

“Enterprise Supervision” or “Tyler” is Probation’s case management system. It is a cloud-based solution that resides in the Amazon Web Services Government Cloud and has been approved to maintain all criminal justice information that is both Probation and DOJ derived data. An application for an approval has been received by DOJ for data to be stored consistent with DOJ protocol and is subject to control oversight by the DOJ California Law Enforcement Telecommunications System (CLETS) Advisory Committee.

“Non-Shared Data” means data that is not Shared Data.

“Shared Data” means the data disclosed by ACSO or Probation, or redisclosed by a Data Recipient, to a Data Recipient, which contains certain data maintained in CRIMS and Enterprise Supervision.

C. TERM OF AGREEMENT AND TERMINATION; DESTRUCTION OF SHARED DATA

1. This DSA shall commence on November 1, 2022 (“Effective Date”) and terminate on June 30, 2023 (“Termination Date”) unless earlier terminated pursuant to this Section C.
2. ACSO or Probation may terminate its participation in this Agreement upon five (5) calendar days written notice to all parties. ACSO’s termination shall not affect Probation’s participation, nor shall Probation’s termination affect ACSO’s participation, in this Agreement.
3. Upon termination of ACSO or Probation’s participation in this Agreement, each Data Recipient shall destroy all the terminating party’s Shared Data in its possession and provide written confirmation of such destruction within five (5) business days of termination.
4. At any time, ACSO or Probation may direct any Data Recipient to destroy all or a subset of Shared Data in the Data Recipient’s possession. The Data Recipient shall comply with such direction and provide written confirmation of such destruction within five (5) business days of receipt of the direction by ACSO or Probation.

D. DATA DISCLOSERS AND DATA RECIPIENTS

1. The following parties shall act as Data Disclosers under this Agreement:

ACSO
Probation

2. The following parties shall act as Data Recipients under this Agreement:

Alameda Alliance for Health
California Health Policy Strategies, LLC
SSA
Wendy Ware
Wendy Still

E. DESCRIPTION OF SHARED DATA

ACSO will disclose to Data Recipients certain data, including data containing identifiable information, maintained in CRIMS. As an example, this may include, but will not be limited to the following: Person file number (PFN), Corpus Event Number (CEN), name, residential address, race, ethnicity, and birthdate.

Probation will disclose to Data Recipients certain data, including data containing identifiable information, maintained in Enterprise Supervision. As an example, this may include, but will not be limited to the following: client demographics, caseload types, and pre-trial supervision levels.

F. DESCRIPTION OF PERMITTED USES AND REDISCLOSURES

Data Recipient Alameda Alliance for Health shall only use Shared Data to implement applicable CalAIM components and may only redisclose Shared Data to another Data Recipient as necessary for such implementation.

All other Data Recipients (for clarity, excluding Alameda Alliance for Health) shall only use Shared Data for the program planning and evaluation purposes of the PPJHC as set forth in the Recitals; and may only redisclose Shared Data to another Data Recipient in this paragraph (for clarity, excluding Alameda Alliance for Health) for the purposes described above in this paragraph. Data Recipients may redisclose Shared Data to Alameda Alliance for Health only as necessary to implement applicable CalAIM components.

G. LEGAL AUTHORITY

The following legal authorities permit the disclosure of individually identifiable information by Probation and ACSO: Penal Code section 13202 (disclosures to public agency concerned with the prevention or control of crime, the quality of criminal justice, or the custody or correction of offenders); Welfare and Institutions Code section 14184.102(j) (disclosures to counties and Medi-Cal managed care plans to implement applicable CalAIM components); Penal Code section 4011.11(h)(5)(B) (disclosures necessary to develop and implement a mandatory process by which county jails and county juvenile facilities coordinate with Medi-Cal managed care plans and Medi-Cal behavioral health delivery systems to facilitate continued behavioral health treatment in the community for county jail inmates and juvenile inmates that were receiving behavioral health treatment before their release); and [Department of Health Care Services, CalAIM Data Sharing Authorization Guidance \(March 2022\)](#).

H. CONFIDENTIALITY

1. A Data Recipient may only use Shared Data for the purpose described in Section F.
2. A Data Recipient may only redisclose Shared Data as described in Section F unless the Data Recipient has received prior written authorization from Probation or ACSO, as applicable.
3. Only a Data Recipient's personnel needing access to Shared Data for an applicable Permitted Use as described in Section F shall access and use Shared Data. Prior to accessing any Shared Data, all such personnel shall be notified in writing of the obligations set forth in this Agreement.
4. Data Recipients shall comply with all laws with respect to the use or disclosure of Shared Data, including but not limited to, California Penal Code sections 11142 & 13302.

I. SECURITY

This Section sets forth the minimum-security requirements applicable to Data Recipients with respect to the Shared Data.

1. Shared Data Transmission.

Transmittal Method:

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> FTP | <input type="checkbox"/> Hardcopy | <input type="checkbox"/> Tape |
| <input type="checkbox"/> CD | <input type="checkbox"/> Removable Media (flash drive) | <input type="checkbox"/> Database View |
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Other (please describe) _____ | |

Transmittal Frequency:

- | | | |
|--------------------------------------|--|------------------------------------|
| <input type="checkbox"/> Weekly | <input type="checkbox"/> Monthly | <input type="checkbox"/> Quarterly |
| <input type="checkbox"/> Annually | <input checked="" type="checkbox"/> As Needed/On request | <input type="checkbox"/> One-time |
| <input type="checkbox"/> Other _____ | <input type="checkbox"/> Data will not be transmitted, users will access data. | |

2. Shared Data Storage. Data Recipients shall store Shared Data using only one or more of the following media and protect the Shared Data as described below.

- i. Workstation Hard disk drives. Access to Shared Data stored on local workstation hard disks will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password. If the workstation is located in an unsecured physical location the hard drive will be encrypted to protect Shared Data in the event the device is stolen.
- ii. Network server disks. Access to Shared Data stored on hard disks mounted on network servers and made available through shared folders will be restricted to

authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password. Backup copies for Data Recipient purposes will be encrypted if recorded to removable media.

- iii. Optical discs (e.g., CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Shared Data provided by Probation or ACSO on optical discs will be used in local workstation optical disc drives and will not be transported out of a secure area. When not in use for the purposes authorized by the Agreement, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access Shared Data on optical discs will be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- iv. Optical discs (e.g., CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. Access to Shared Data provided by Probation or ACSO on optical discs which will be attached to network servers and which will not be transported out of a secure area will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security. Shared Data on discs attached to such servers will be located in an area which is accessible only to authorized individuals with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- v. Paper documents. Any paper records will be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.
- vi. Portable devices or media.
 - a. Shared Data may be stored on portable devices or media subject to the following requirements:
 - 1. Encrypt the Shared Data with a key length of at least 128 bits.
 - 2. Control access to devices with a unique user ID and password or stronger authentication method.
 - 3. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity if this feature is available. Maximum period of inactivity is 20 minutes.
 - 4. Physically protect the portable device(s) and/or media by:

- I. Keeping them in locked storage when not in use;
 - II. Using check-in/check-out procedures when they are shared; and
 - III. Taking frequent inventories.
- b. When being transported outside of a secure area, portable devices and media with confidential Shared Data will be under the physical control of Information Technology Department staff with authorization to access the Shared Data.
 - c. Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g., USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.
 - d. Portable media includes but is not limited to; optical media (e.g., CDs, DVDs, Blu-Rays), magnetic media (e.g., floppy disks, tape, Zip or Jaz disks), or flash media (e.g., CompactFlash, SD, MMC).

3. Data Segregation.

- i. If feasible, Shared Data must be segregated or otherwise distinguishable from Non-Shared Data. This is to ensure that when no longer needed by members, all Shared Data can be identified for return or destruction. It also aids in determining whether Shared Data has or may have been compromised in the event of a security breach.
- ii. Shared Data will be kept on media (e.g., hard disk, optical disc, tape, etc.) which will contain no Non-Shared Data.
- iii. Shared Data will be stored in a locked container on electronic media, such as a partition or folder dedicated to Shared Data. Or,
- iv. Shared Data will be stored in a database which will contain no Non-Shared Data. Or,
- v. Shared Data will be stored within a database and will be distinguishable from Non-Shared Data by the value of a specific field or fields within database records. Or,
- vi. When stored as physical paper documents, Shared Data will be physically segregated from Non-Shared Data in a drawer, folder, or other container.
- vii. When it is not feasible or practical to segregate Shared Data from Non-Shared Data, then both Shared Data and the Non-Shared Data with which it is commingled must be protected as described in this Agreement.

4. Breach or Compromise; Notification; Corrective Action.

If any Data Recipient detects an actual or potential breach or compromise in the IT security system for Shared Data such that personal information may have been accessed or disclosed without proper authorization, Data Recipient shall give notice to ACSO and/or Probation, as applicable, within one (1) business day of discovering the breach or compromise or potential breach or compromise.

Data Recipients shall take corrective action as soon as practicable to eliminate the cause of the breach or compromise and shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed.

J. DISCLOSURE OF WORK PRODUCT DERIVED FROM SHARED DATA; NOTICE

At least five (5) business days prior to any Data Recipient's disclosure of work product derived from any Shared Data, Data Recipient shall provide written notice to ACSO and/or Probation, as applicable, of the substance of the anticipated disclosure in sufficient detail for ACSO and/or Probation to review and provide feedback. Data Recipient shall not disclose any Shared Data that identifies, or could reasonably be used to identify, individual clients except as set forth in Sections F through H.

K. MODIFICATIONS

All modifications to this DSA shall be in writing and signed by all parties.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

SIGNATURES

By signing below, each signatory warrants and represents that the signatory executed this DSA in the signatory's authorized capacity and that by signature on this DSA, the signatory has the legal authority, or has received such authority from the entity, to bind the entity upon whose behalf the signatory executed this DSA.

The parties have executed this DSA by and through their duly authorized representatives.

Alameda County Probation Department


DocuSigned by:

436902B1EF8A47A...
Marcus Dawal
Chief Probation Officer

11/1/22

Date

Alameda County Sheriff's Office

DocuSigned by:

F05B6DA11FD248A...
Gregory J. Ahern
Sheriff-Coroner

11/1/22

Date

Alameda County Social Services Agency

DocuSigned by:

CFBDBF387EBC293...
Andrea Ford
Interim Agency Director

11/2/2022

Date

Alameda Alliance for Health


DocuSigned by:

9FC0ACFD3A6A42A...
Scott Coffin
Chief Executive Officer

11/1/22

Date


California Health Policy Strategies, LLC

DocuSigned by:

EAB841413E0E464...
David Panush
President

11/1/22

Date

Wendy Still, an individual

DocuSigned by:

CF59A6ED28434AF...
Wendy Still
Special Advisor to the Public Protection
Committee

11/1/22

Date

Wendy Ware, an individual

DocuSigned by:

Wendy Ware

7AF007D0F30140F...

Wendy Ware

11/2/2022

Date

Approved as to Form: DONNA ZIEGLER
County Counsel for the County of Alameda

DocuSigned by:

DZiegler

11/1/22

9D77AF6FB7F6431...

Certificate Of Completion

Envelope Id: 1BD3814159C14278A7426C2E495CEA17

Status: Completed

Subject: Complete with DocuSign: Data Sharing Agreement Combined CRIMS and Tyler - Enterprise Systems, F...

Envelope Comments:

Document Id:

Status:

Source Envelope:

Document Pages: 11

Signatures: 8

Envelope Originator:

Certificate Pages: 3

Initials: 0

Margarita Perez

AutoNav: Enabled

393 13th Street

Envelopeld Stamping: Disabled

Oakland, CA 94612

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Margarita.Perez2@acgov.org

IP Address: 73.48.142.77

Record Tracking

Status: Original

Holder: Margarita Perez

Location: DocuSign

11/1/2022 7:33:29 AM

Margarita.Perez2@acgov.org

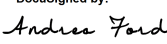
Signer Events

Andrea Ford

AAFord@acgov.org

Interim Assistant Agency Dir

Alameda County

Security Level: Email, Account Authentication
(None)**Signature**DocuSigned by:

CFBDBF387EBC493...**Timestamp**

Sent: 11/1/2022 7:40:36 AM

Viewed: 11/2/2022 9:56:03 AM

Signed: 11/2/2022 9:56:11 AM


Signature Adoption: Pre-selected Style
Using IP Address: 166.107.98.1**Electronic Record and Signature Disclosure:**

Not Offered via DocuSign

David Panush

d.panush@calhps.com

President

Security Level: Email, Account Authentication
(None)DocuSigned by:

EABB41413E0E464...

Sent: 11/1/2022 7:40:35 AM

Resent: 11/1/2022 8:18:33 AM

Viewed: 11/1/2022 8:45:15 AM

Signed: 11/1/2022 8:47:59 AM

Signature Adoption: Drawn on Device
Using IP Address: 98.36.124.166**Electronic Record and Signature Disclosure:**

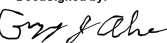
Not Offered via DocuSign

Gregory Ahern

gahern@acgov.org

Sheriff

Alameda County

Security Level: Email, Account Authentication
(None)DocuSigned by:

F05B6DA11FD248A...

Sent: 11/1/2022 7:40:35 AM

Viewed: 11/1/2022 7:59:46 AM

Signed: 11/1/2022 8:00:42 AM

Signature Adoption: Drawn on Device
Using IP Address: 174.249.152.144
Signed using mobile**Electronic Record and Signature Disclosure:**

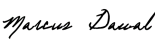
Not Offered via DocuSign

Marcus Dawal

mdawal@acgov.org

Assistant Chief

Alameda County Government

Security Level: Email, Account Authentication
(None)DocuSigned by:

436902B1EF8A47A...

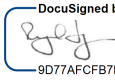

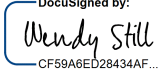
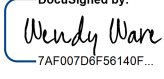
Sent: 11/1/2022 7:40:36 AM

Viewed: 11/1/2022 9:06:37 AM

Signed: 11/1/2022 4:03:08 PM

Signature Adoption: Pre-selected Style
Using IP Address: 166.107.98.71**Electronic Record and Signature Disclosure:**

Not Offered via DocuSign

Signer Events	Signature	Timestamp
Raymond Leung raymond.leung@acgov.org Deputy County Counsel County of Alameda SFDC Security Level: Email, Account Authentication (None)	DocuSigned by:  9D77AFCFB7F6431... Signature Adoption: Uploaded Signature Image Using IP Address: 166.107.111.254	Sent: 11/1/2022 3:17:16 PM Viewed: 11/1/2022 3:18:10 PM Signed: 11/1/2022 3:21:05 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Scott Coffin scoffin@alamedaalliance.org Chief Executive Officer Alameda Alliance For Health Security Level: Email, Account Authentication (None)	DocuSigned by:  9FC0ACFD3A6A42A... Signature Adoption: Pre-selected Style Using IP Address: 209.232.58.1	Sent: 11/1/2022 7:40:36 AM Viewed: 11/1/2022 10:57:31 AM Signed: 11/1/2022 10:57:42 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Wendy Still wendy.still2@acgov.org Security Level: Email, Account Authentication (None)	DocuSigned by:  CF59A6ED28434AF... Signature Adoption: Pre-selected Style Using IP Address: 207.237.155.194	Sent: 11/1/2022 7:40:35 AM Viewed: 11/1/2022 3:17:45 PM Signed: 11/1/2022 3:18:13 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Wendy Ware wpnaro@gmail.com Consultant Security Level: Email, Account Authentication (None)	DocuSigned by:  7AF007D6F56140F... Signature Adoption: Pre-selected Style Using IP Address: 75.70.255.253	Sent: 11/1/2022 7:40:34 AM Resent: 11/2/2022 3:19:59 PM Viewed: 11/2/2022 4:16:16 PM Signed: 11/2/2022 4:16:24 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	11/1/2022 7:40:37 AM
Certified Delivered	Security Checked	11/2/2022 4:16:16 PM

Envelope Summary Events	Status	Timestamps
Signing Complete	Security Checked	11/2/2022 4:16:24 PM
Completed	Security Checked	11/2/2022 4:16:24 PM
Payment Events	Status	Timestamps