

Santa Barbara County Interagency
MEMORANDUM OF UNDERSTANDING
Regarding the County Integrated Justice Information System

1. PARTIES

This Memorandum of Understanding (MOU) is entered into by the following parties:

- County Probation Department (Probation)
- County District Attorney's Office (DA)
- County Public Defender's Office (PD)
- County Sheriff's Office (Sheriff)
- Superior Court of California, County of Santa Barbara (Court)

The foregoing parties are referred to herein individually as an "Agency" or "Party" and collectively as the "Agencies" or "Parties".

2. PURPOSE

This MOU memorializes the Parties' understanding of each Agency's access to an Integrated Justice Information System (IJIS), a platform that will allow the Parties to share, analyze, and report data pertaining to shared clients as agreed among MOU Parties.

This MOU does not directly authorize any data to be shared among Parties, but describes a uniform process and framework for Parties to participate in such data sharing agreements that will define the allowable internal and/or external uses of data shared through the IJIS platform.

3. ADMINISTRATION OF MOU

3.1 Notices. Any notice or consent required or permitted to be given under this MOU shall be given to all other Parties in writing. Notices shall be sent to the individuals identified in **Attachment A** as an authorized administrative representative of this MOU for their respective Agency.

3.2 Changing Agency Designated Representatives. Any Party may change its administrative representative by providing written notice of the change to all other Parties. Any such change will become effective upon receipt of such notice by the other Parties to this MOU.

4. TERM AND TERMINATION

4.1 Term. This MOU is effective on the date all of the Parties have signed and shall continue in force through June 30, 2020, renewing for a one-year term beginning each July 1st thereafter, unless terminated in writing by all Parties.

4.2 Termination. Any Agency may terminate its participation in the MOU immediately in the event of a material breach (e.g., unauthorized disclosure of data, use of data by any party for purposes not authorized by this MOU). Any Agency may terminate its participation in this MOU for any reason upon 45 days written notice to the other Parties.

Upon termination any Agency, the IJIS Administrator shall terminate IJIS access to send or receive further data to or from that Agency. Additionally, to the extent applicable, the IJIS Administrator shall delete, destroy, and/or deliver back to the terminating Agency all of that Agency's data, estimates, graphs, summaries, reports, and all other property, records, documents or papers as may have been accumulated or produced by the terminating Agency under this MOU, except such items as the Agency may, by written permission, permit the IJIS to retain.

4.3 Suspension. Each Agency contributing data under this MOU reserves the right to immediately suspend data sharing of that Agency's own data elements, without prior notice, upon reasonable belief by the suspending Agency that this MOU has been violated or to protect its systems, personnel, or the public in the event of a suspected or actual security breach or unauthorized use or disclosure of data. As needed for maintenance purposes, any Agency may suspend data sharing with advance notice to all other Parties in accordance with Section 11 (Required Notifications). The suspending Agency may reinstate suspended data sharing services upon verification that any violations have been investigated, and if verified, corrected, and that appropriate measures have been taken to prevent future violations.

5. ENTIRE AGREEMENT AND AMENDMENT

This MOU contains the entire and complete understanding of the parties hereto concerning the IJIS platform, and supersedes any and all other previous or contemporaneous agreements, representations, and warranties, whether oral or written, regarding data sharing through the IJIS. This MOU may be altered, amended, or modified only by a written instrument executed by all Parties to this MOU, and by no other means, except as follows:

5.1 Attachments. This MOU includes the following Attachments:

5.1.1. Attachment A: MOU Agency Designated Representatives

Any Party may change its Designated Representative as set forth in Section 3.2 above, without requiring a formal amendment to this MOU. The IJIS Administrator shall maintain the current list of Participating Agency Representatives.

5.1.2. Attachment B: Conceptual Overview of IJIS Data Sharing

This flowchart is provided and maintained by the IJIS Administrator, and is attached hereto for illustrative purposes only.

5.1.3. Attachment C: Conceptual Guide to IJIS Data Request and Review Process

This summary is provided and maintained by the IJIS Administrator, and is attached hereto for illustrative purposes only.

5.2 Separate Agreements between Parties. Any data sharing agreements entered between participating Parties according to the process set forth in Section 6.2 (Data Elements Shared) shall not require the consent of unaffected MOU Parties.

6. PARTIES' RESPONSIBILITIES

6.1 Data Sharing Infrastructure: Probation shall provide the following:

- a. Database Services to host the application and data integration structure.
- b. Internet Information Server to host web applications such as API (Application Program Interface).
- c. To the extent that funding is available, one EDP Systems Programming Analyst position to serve as IJIS Administrator, providing database administration and integration assistance to partner Agencies.

6.2 Data Elements Shared through Separate Written Agreement: A Party shall enter a separate written agreement with one or more participating Parties, subject to the general terms of this MOU, to specify the data elements to be shared as well any other necessary terms agreed upon between those Parties (e.g., data format, frequency of updates, authorized uses). Any Party shall only access data of another Agency through the IJIS to the extent authorized by the foregoing separate agreement. Prior to the execution of the foregoing separate agreement, a Party shall not access data from another Party through the IJIS.

To the extent set forth in each separate data sharing agreement approved by the participating Parties' Administrations, each participating Party shall share data as permitted under applicable confidentiality restrictions for use in reports about the provision of services by the Law and Justice community. Each Party receiving a request to share data under this MOU is responsible for determining whether any of the data elements it maintains originated from another Agency, and if so, to obtain written consent from the owning Agency, prior to sharing that data.

Parties further anticipate that there may be opportunities to use one or more Agencies' data to enhance the effectiveness or efficiency of other Law and Justice partners who are not Parties to this MOU, through the process set out for third-party access (Section 7.4).

6.3 Periodic Review: Each Party agrees to review this MOU and any related Integrated Justice Information System policies and procedures for accuracy at least every three years, beginning in July 2021.

7. AUTHORIZED ACCESS

7.1 CORI and HIPAA Requirements. Anyone including any Party Agency, who has been authorized by a participating Agency to view data in the Integrated Justice Information System that could be used to associate criminal history, criminal offender record information, or HIPAA-protected information with an individual must meet the legal requirements for such access, including Penal Code section 13300 requirements. De-identified, aggregate data that meets the standard set forth at 45 C.F.R. § 164.514 does not have this restriction and is subject to the other sections of this MOU governing use of data.

7.2 System User Accounts. Each Agency is responsible for creating individual System User accounts for any Agency employees authorized to request data reports through the Integrated Justice Information System. Each Agency is responsible for ensuring user accounts are current and to deactivate or terminate user accounts promptly when users leave the Agency or no longer meet the Agency's qualifications for a System User account.

7.3 Clearance Requirements. Each Agency shall assign a clearance level to each individual System User account for that Agency's employees, based on an employee's background and training, which will control what data elements are available to or restricted from access by that user. Each Agency is responsible for ensuring its System User account clearance levels are accurate at all times.

7.4 Third-party Access to Data:

Requests for data from the Integrated Justice Information System may come from third parties (e.g., external policy stakeholders, Law and Justice Community partners, requests under public records laws including the Public Records Act and California Rule of Court 10.500) that are not parties to this MOU. All third-party requests shall be sponsored by a Party Agency, and shall proceed through an authorized System User of the sponsor Agency with the appropriate clearance level. Disclosure of the data shall only occur if permitted by applicable law.

For any Public Records Act request to an Agency for information that may include data of the Probation, DA, PD or the Sheriff, an agency shall treat this as a multi-departmental Public Records Act request and shall coordinate through the County's Executive's Office, in accordance with County Policy.

For any public records request to a Party for information that may include data of the Court, each Party shall treat this as a public records request to the Court and shall coordinate through the Court's Executive Office in accordance with Court policy.

Neither a County Agency nor the Court shall disclose the other's confidential data in response to a public records request without the prior written consent of all Parties, whose data elements are included in the request.

8. IJIS PLATFORM TERMS OF USE

- 8.1 Data Security Controls. Each Agency making its data accessible through the Integrated Justice Information System maintains full responsibility to ensure the security of its own data, including that protected elements are disseminated only to authorized System Users with appropriate clearance levels or in de-identified aggregate form as permitted by applicable laws, regulations, and Agency policies and procedures.

Since the IJIS does not store data, the security of any data once shared is the responsibility of the sharing Parties to set forth under their separate data sharing agreement (see Section 6.2). At minimum, each Agency sharing or receiving data through the IJIS shall comply with and implement industry-standard safeguards against the loss, misuse, or unauthorized disclosure of data. Any data shared or accessed under this MOU shall not be stored or transmitted outside the continental United States; the physical location of the equipment where such data is stored shall be within the continental United States.

- 8.2 Enforcement Rights. Each party has the responsibility and authority to monitor and enforce the implementation of this MOU. Parties agree to cooperate with each other in the implementation of this MOU and to accomplish the purposes of this MOU.

- 8.3 Integrated Justice Information System MOU Training. Each Agency agrees to appropriately educate its authorized System Users and IT personnel who will engage with the Integrated Justice Information System regarding the terms of use set forth in this MOU.

- 8.4 Penalties for Misuse: If an individual System User or Agency misuses data governed by this MOU:

- 8.4.1 They take upon themselves full legal responsibility for such misuse and hold harmless the Agency (ies) that may have contributed the data.
- 8.4.2 They are subject to being barred from further access to data. The Integrated Justice Information System Administrator shall make that determination in consultation with any affected Agency system administrator.

- 8.4.3 If any Agency contributing data believes its data is not being used in accordance with this MOU, they may request the IJIS Administrator to immediately suspend an offending individual System User account. Such requests will be honored by the IJIS Administrator, to ensure that the offending individual has no further access to Agency data while investigation occurs.
- 8.4.4 An Agency may request that the IJIS administrator suspend all data sharing from that Agency according to the process set forth in Section 4.3.
- 8.4.5 Parties may include additional enforcement language, subject to IJIS Administrator's confirmation, within their separate data sharing agreements established under Section 6.2 to this MOU.

8.5 Data Uses: Parties may use Agency data accessible through the IJIS to the extent authorized by the contributing Agency, whether for internal purposes, for coordination with Participating Agencies, or for external publication. Any use of data in a publication or report for uses including, but not limited to, budget hearings, grant applications, news stories, etc., must first be approved as to content by each Agency whose data is included in the release.

8.6 Accuracy Disclaimer: None of the Agencies contributing data make any warranty as to the accuracy or availability of data contributed. Although each Agency strives for its data to be correct, it is understood that there may be discrepancies.

9. PRIVACY AND CONFIDENTIALITY

Each Agency acknowledges that information accessed or shared through the Integrated Justice Information System is restricted and may be confidential. Access to Agency data through the Integrated Justice Information System shall be governed by the most stringent of all applicable laws, statutes, rules, and regulations, including those related to privacy. Each Agency will disclose IJIS data only to its officers and employees who have the right to know and a legitimate need to know such data, and who have executed a confidentiality agreement with such Agency that is at least as protective of the data as the provisions of this MOU. An Agency or third party shall use the information and data received under this MOU only to perform official duties, for internal statistical and research purposes as permitted by law, or other use approved by the affected MOU Parties.

10. COMPLIANCE WITH LAW.

Each Party shall, at its sole cost and expense, comply with all County, State and Federal ordinances and statutes, and any other applicable laws now in force or which may hereafter be in force with regard to this MOU.

11. REQUIRED NOTICES

- 11.1 **Breach Notification.** Each Agency shall promptly notify all Parties when a network incident or data breach is suspected or has occurred and immediately suspend access to its data while the incident is investigated. The suspending Agency shall promptly notify all Parties when service is restored.
- 11.2 **Unplanned Outage Notification.** Each Agency shall promptly notify all Parties when access to its data is suspended due to an unplanned network outage. The suspending Agency shall promptly notify all Parties when service is restored.
- 11.3 **Scheduled Outage Notification.** Each Agency experiencing a scheduled maintenance outage or other planned outage resulting in suspended access to its data shall provide 72 hours advance notice to all other Parties. The suspending Agency shall promptly notify all Parties when service is restored.
- 11.4 **Notification of Legal Action.** Each Agency shall promptly notify the other Agencies upon notification or receipt of any civil or criminal action, demand, cause of action, lawsuit, or governmental enforcement action (collectively "actions") arising out of or related to this MOU, regardless of whether any other Agency is specifically named in the action.

12. INDEMNIFICATION & INSURANCE

- 12.1 **Indemnification.** Each Party (the "Indemnifying Party") agrees to defend, indemnify, and hold harmless each other Party and its officers, officials, employees, volunteers or agents (the "Indemnitee") against any and all claims, damages, costs, liabilities, and expenses, including attorneys' fees, arising from or attributable to the Indemnifying Party's negligent acts or omissions and intentional misconduct which is brought against an Indemnitee in connection with the activities, related services or the Indemnifying Party's breach of its responsibilities under this MOU.

The Parties waive the per capita risk allocation set forth in Government Code section 895.6. Instead, the Parties agree that if one of them is held liable upon any judgment for damages caused by a negligent or wrongful act or omission occurring in the performance of this MOU, the Parties' respective pro-rata shares in satisfaction of the judgment will be determined by applying principles of comparative fault.

- 12.2 **Insurance.** Each party shall maintain its own insurance coverage, through commercial insurance, self-insurance or a combination thereof, against any claim, expense, cost, damage, or liability arising out of the performance of its responsibilities pursuant to this MOU.

13. PARTY PROPERTY AND INFORMATION

Each Party's property, documents, and information provided for IJIS use under this MOU shall remain that Party's property, and all other Parties shall return any such items

whenever requested by a Party and whenever required according to the Termination section of this MOU. Other Parties may use such items only in connection with the stated purpose of this MOU. Other Parties shall not disseminate any Party property, documents, or information without that Party's prior written consent.

14. NONDISCRIMINATION.

The County's Unlawful Discrimination Ordinance (Article XIII of Chapter 2 of the Santa Barbara County Code) applies to this MOU and is incorporated into the MOU by this reference with the same force and effect as if the ordinance were specifically set out herein, and Court agrees to comply with that ordinance.

15. NON-ASSIGNMENT

An Agency may not assign, subcontract, delegate, or otherwise transfer its rights, duties, or obligations under this MOU without the prior written consent of the other Agencies.

16. AUTHORITY

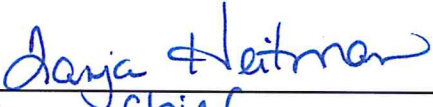
Each Agency represents and warrants that it has full power and authority to enter into this MOU, and that its representative who signs this MOU has the authority to bind such Party to this MOU.

MEMORANDUM OF UNDERSTANDING
Regarding the Integrated Justice Information System

IN WITNESS WHEREOF, the Parties hereby execute this Memorandum of Understanding, effective on the date all of the Parties have signed.

SANTA BARBARA COUNTY:

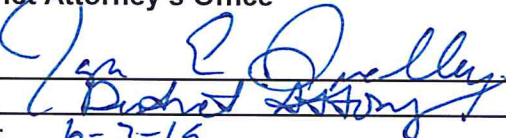
Probation Department

By: 
Title: Chief
Date: 6.3.19

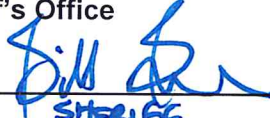
Public Defender's Office

By: 
Title: Chief
Date: 6/12/19

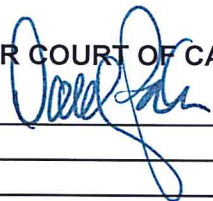
District Attorney's Office

By: 
Title: District Attorney
Date: 6-3-19

Sheriff's Office

By: 
Title: Sheriff
Date: 6/17/19

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA BARBARA:

By: 
Title: CEO
Date: 5/23/19

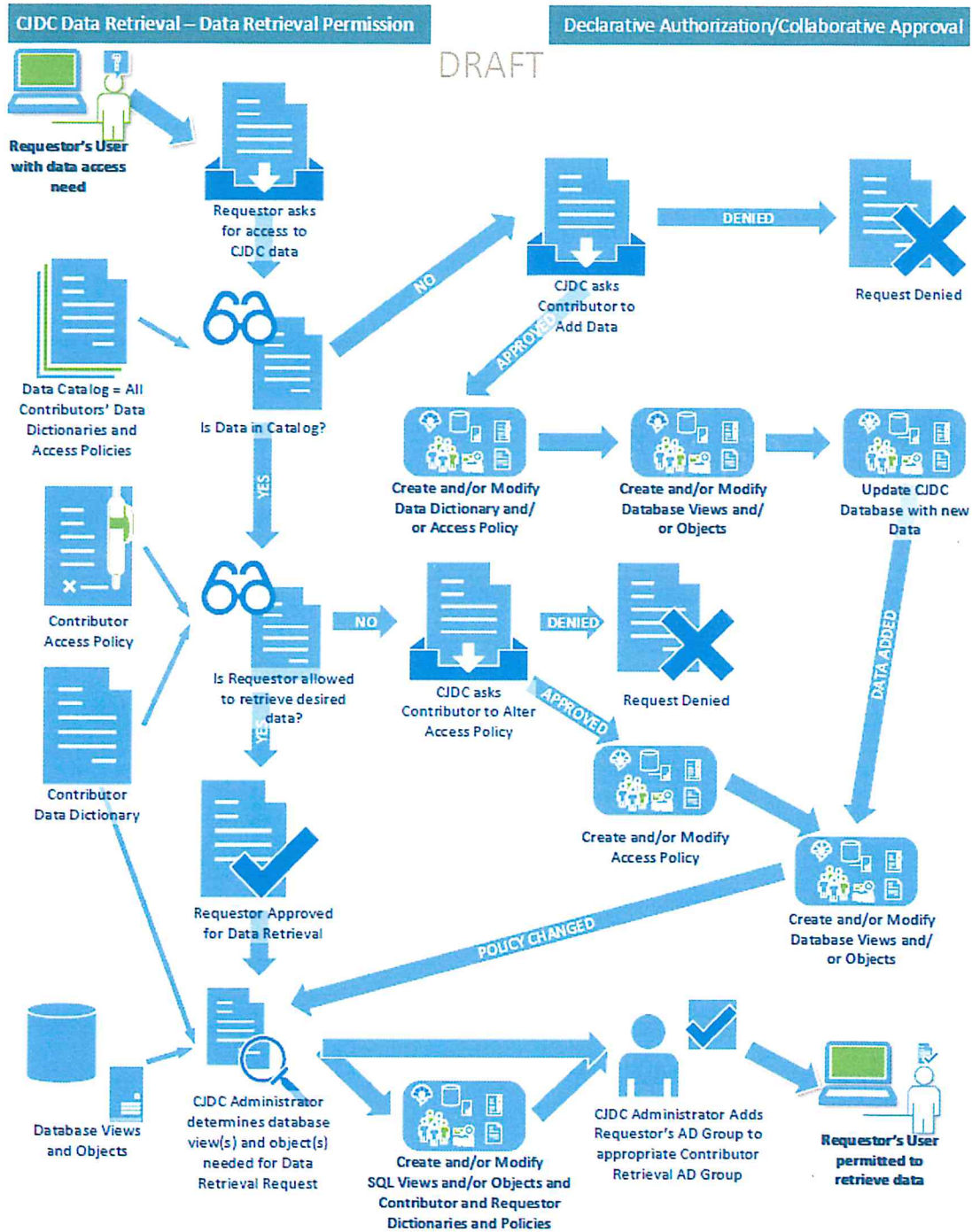
Attachment A

MOU Agency Designated Representatives

<u>Probation Department</u> Damon Fletcher Administrative Deputy Director 117 E. Carrillo St. Santa Barbara, CA 93101 (805) 882-3654 dfletch@co.santa-barbara.ca.us <u>IJIS Administrator</u> John Kuo	<u>Sheriff's Office</u> Nemie Holman Chief Information Officer Santa Barbara Sheriff's Headquarters 4434 Calle Real Santa Barbara CA 93110 (805) 681-4722 nfh3573@sbsheriff.org
<u>District Attorney's Office</u> Michael Soderman Chief Financial and Administrative Officer 1112 Santa Barbara St. Santa Barbara, CA 93101 (805) 568-2303 mdsoderman@co.santa-barbara.ca.us	<u>Santa Barbara Superior Court</u> Darrel Parker Court Executive Officer 1100 Anacapa Street Santa Barbara, CA 93101 (805) 614-6594 dparker@sbcourts.org
<u>Public Defender's Office</u> Deepak Budwani Chief Financial and Administrative Officer 1100 Anacapa Street Santa Barbara, CA 93101 (805) 568-3589 dbudwani@publicdefendersb.org	

Attachment B

IJIS Data Sharing Flowchart



Attachment C

IJIS Data Request and Review Process

Request

Requestor, on behalf of a user in their department, submits a request to the System Administrator that itemizes the data requested. The request must provide the following:

- Describe how the information being requested will be used and for what purpose.
- Specify in detail the data elements needed and any processing to be performed (filtering and/or aggregation) – see following section.
- How the data will be retrieved (Linked Server, SSRS, export, etc.) and frequency.

Data Element Specification

The request may specify the following to identify the data desired:

- Existing Requestor Data Dictionary View/Query (these contain multiple data elements and optionally filters).
- Individual data elements such as Gender, Race, DOB, etc. present in one or more existing Requestor Data Dictionary View/Query.
- Individual data elements not already found in any existing Requestor Data Dictionary View/Query.

Processing Specification

The request may also specify the following options:

- Data summarization and/or other aggregation
- Data Filtering

Review

The System Administrator reviews the request to determine the availability of the data elements, and assist parties to determine the appropriate data permissions for those elements. Both Contributors and Requestors may be consulted multiple times during this step to refine and possibly revise the original request.

This review facilitates the determination by a Party that the data can or cannot be provided by a Contributor in response to the request. If it cannot, the request is rejected.