Data Sharing Agreement

This Data Sharing Agreement has been incorporated into the Standard Service Agreement dated -_____[YEAR], by and between the County of [Insert county], acting by and through its [Insert Agency] and [xxx (xxx)] for [xxx] to _____.

1. RECITALS

A. Whereas, [xxx] ; and;

B. Whereas, [xxx] and [Name of County] County have entered into an agreement for [xxx] to provide _____.

2. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement is to outline the terms and conditions agreed to by [xxx] and [County Agency] regarding the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code §13202.

3. DEFINITIONS

"Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

"Data Encryption" refers to 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 Storage" refers to the state data is in when at rest. Data shall be stored on secured environments.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

"Criminal Offender Record Information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of 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)

4. DESCRIPTION OF DATA TO BE SHARED

[County Agency] will share state and local Criminal Offender Record Information related to individuals who are part of the County's realigned population.

5. DESCRIPTION OF INTENDED USE

[Insert description of project and data use]

6. DATA TRANSMISSON

a. Transmittal Method:

☐	FTP	☐	Hardcopy	☐	Tape
☐	CD	☐	Removable Media (flash drive)	☐	Database View
☐	E-mail	☐	Other (please describe)		

b. Transmittal Frequency:

☐	Weekly	☐	Monthly	☐	Quarterly
☐	Annually	☐	As Needed/On request	☐	One-time
☐	Other_____	☐	Data will not be transmitted, users will access data.		

c. Transmittal security: All HIPPA protected data will be encrypted prior to any email transmission.

7. DATA SECURITY

All data provided by [County Agency] shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement.

a. Protection of Data

RDA agrees to store data on one or more of the following media and protect the data as described:

1) Workstation Hard disk drives. Access to 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 [County Agency] data in the event the device is stolen.

2) Network server disks. Access to 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 DR purposes will be encrypted if recorded to removable media.

3) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by [County Agency] 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 [County Agency] 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.

4) Optical discs (e.g., CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. Access to data provided by [County Agency] 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. 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.

5) 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.

6) Data storage on portable devices or media.

a) [County Agency] data shall not be stored by [xxx] on portable devices or media unless specifically authorized within this Agreement. If so authorized, the data shall be given the following protections by [xxx]:

i. Encrypt the data with a key length of at least 128 bits.

ii. Control access to devices with a unique user ID and password or stronger authentication method.

iii. 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 twenty (20) minutes.

iv. Physically protect the portable device(s) and/or media by:

- Keeping them in locked storage when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

b) When being transported outside of a secure area, portable devices and media with confidential [County Agency] data will be under the physical control of [xxx] staff with authorization to access the 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).

b. **Safeguards Against Unauthorized Access and Re-disclosure**

[xxx] shall exercise due care to protect all Criminal Offender Record Information data from unauthorized physical and electronic access. Both parties shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information provided by either party pursuant to this Agreement:

1) Access to the information provided by [County Agency] will be restricted to only those authorized staff who need it to perform their official duties in the performance of the work requiring access to the information as detailed in the Purpose of this Agreement.

2) [xxx] will store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

3) Unless specifically authorized in this Agreement, the [xxx] will not store any confidential or sensitive [County Agency] data on portable electronic devices or media, including, but not limited to laptops,

handhelds/PDAs, Ultramobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), and portable hard disks.

4) [xxx] will protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

5) [xxx] shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

6) [xxx] shall instruct all individuals with access to the Criminal Offender Record Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Agreement.

7) [xxx] shall take due care and take reasonable precautions to protect [County Agency]'s data from unauthorized physical and electronic access.

8) [xxx] shall ensure that any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived therefrom do not identify specific individuals.

c. **Data Segregation**

1) [County Agency] data must be segregated or otherwise distinguishable from non- [County Agency] data. This is to ensure that when no longer needed by [xxx], all [County Agency] data can be identified for return or destruction. It also aids in determining whether [County Agency] data has or may have been compromised in the event of a security breach.

2) [County Agency] data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-[County Agency] data. Or,

3) [County Agency] data will be stored in a logical container on electronic media, such as a partition or folder dedicated to [County Agency] data. Or,

4) [County Agency] data will be stored in a database which will contain no non- [County Agency] data. Or,

5) [County Agency] data will be stored within a database and will be distinguishable from non- [County Agency] data by the value of a specific field or fields within database records. Or,

6) When stored as physical paper documents, [County Agency] data will be physically segregated from non- [County Agency] data in a drawer, folder, or other container.

7) When it is not feasible or practical to segregate [County Agency] data from non- [County Agency] data, then both [County Agency] data and the non- [County Agency] data with which it is commingled must be protected as described in this Agreement.

If [xxx] or its agents detect a compromise or potential compromise in the IT security for this data such that personal information may have been accessed or disclosed without proper authorization, [xxx] shall give notice to [County Agency] within one (1) business day of discovering the compromise or potential compromise.

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

8. DATA OWNERSHIP

a. [County Agency] retains ownership of all data provided pursuant to this Agreement including, but not limited to, any subsets generated from the raw data, individual-level subsets derived from the raw data, and any data sets generated by addition to or combination with other any other data.

b. Neither [County Agency] nor [xxx] may relinquish or transfer ownership or physical custody of the data provided pursuant to this Agreement to any entity.

9. DATA SHARING AGREEMENT COMPLETION/TERMINATION

a. Upon completion or termination of this contract, the data provided pursuant to the terms of this Agreement shall be destroyed or returned to [County Agency] with certification [xxx] that the original and all copies of the data on all systems and media have been destroyed.

b. This Agreement is binding as to the confidentiality, use of the data, and disposition of all data received as a result of this access, unless otherwise amended by the mutual agreement of both parties.

c. Upon execution of this Data Sharing Agreement, all staff with access to, or that have accessed the data provided pursuant to the terms of this Agreement will be notified of the non-disclosure provisions of this Agreement.

d. [County Agency] may terminate this Data Sharing Agreement with a prior written notice to [xxx] as provided for in paragraph 20 of the Agreement.

10. DATA CONFIDENTIALITY

a. Regulations Governing Confidentiality of Data

i. [xxx] acknowledges the confidential nature of the data received from [County Agency] and agrees that personnel with access shall comply with all laws, regulations, and policies that apply to the protection of the confidentiality of the data. This compliance includes, but is not limited to, submitting an application as required by the CALIFORNIA DEPARTMENT OF JUSTICE, CRIMINAL JUSTICE INFORMATION SERVICES DATA ANALYSIS PROGRAM RESEARCH AND DATA REQUEST

(https://www.oag.ca.gov/sites/all/files/agweb/pdfs/corp/research-request-packet.pdf).

ii. Any willful, malicious, negligent, or knowing disclosure of the data received pursuant to this Agreement to unauthorized persons may be punishable by applicable state and federal laws, including California Penal Code §§11142 , 13302. Any staff that unlawfully discloses confidential data that has been determined to incur any economic, bodily, or psychological harm as a result of the disclosure may also be liable for the damages incurred.

b. Limited Access to Data

i. Only staff assigned by xxx shall have access to review, manipulate, and maintain the data received for their organization. [xxx] is responsible for ensuring that only authorized staff with a business need directly related to the purpose of the

Agreement will access the data received pursuant to this Agreement. Signed confidentiality agreements for all staff that will have access to the data shall be obtained, maintained for the duration of the Agreement, and copies provided to [County Agency] on request.

ii. Protected Health Information: If the dataset includes healthcare information, appropriate HIPAA safeguards shall be in place and followed by [xxx].

c. Safety and Security

[xxx] acknowledges and agrees to fully comply with the necessary strict disclosure provisions that minimize directly or indirectly revealing offender level information which could jeopardize the safety or security of offenders and correctional staff, as well as the public at large.

11. CONSTRAINTS ON USES OF THE DATA RECEIVED

a. The dataset received pursuant to this Agreement may be used ONLY for the purpose described in this Agreement and only for the term of the Agreement.

b. This Agreement does not authorize a release of the data to any organization for discretionary use, but allows access to the data only to carry out the purposes described in this Agreement. Any ad hoc analysis or other use of the data, not expressly specified in this Agreement, is not permitted without the prior written authorization of [County Agency].

12. NON-DISCLOSURE OF DATA

a. Non-Disclosure of Data Requirements:

i. No person shall disclose, in whole or in part, the data provided by [County Agency] pursuant to this Agreement to any individual or agency, unless this Agreement specifically authorizes the disclosure.

i. Data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement and that have received approval from [County Agency].

ii. Staff shall not access or use the data for any commercial or personal purposes.

b. Any exceptions to these limitations must be approved in writing by [County Agency].

c. Penalties for Unauthorized Disclosure of Information:

Should [xxx] fail to comply with any terms of this Agreement, [County Agency] shall have the right to take such action as it deems lawfully appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties harmed or injured by unauthorized disclosure.

d. Employee Awareness of Use/Non-disclosure Requirements

[xxx] shall ensure that all staff with access to the data provided pursuant to this agreement are aware of the use and disclosure requirements of this agreement and will advise all staff of the provisions of this agreement. This notification shall include all IT support staff as well as staff who will manipulate and/or analyze the data. All staff will receive [County Agency] administered Live Scans at [X]'s expense.

SIGNATURES

The parties have executed this Data Sharing Agreement by and through their duly authorized representatives.

[County] [County Agency] Department

By: _____ Date:_____
[Name]
[Title] [County Agency] Officer

[xxx (xxx)]

By: _____ Date:_____
[Name]
[Title] [County Agency] Officer

All individuals who are part of [xxx]'s team and who will have access to the confidential individual-level data must sign this agreement.

[xxx (xxx)] Staff:

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff