AGENDA # _____, September 28, 2021

ALAMEDA COUNTY PROBATION DEPARTMENT

P.O. Box 2059
1111 Jackson Street
Oakland, CA 94604-2059

Marcus Dawal
Interim Chief Probation Officer

August 30, 2021

Honorable Board of Supervisors
County of Alameda
1221 Oak Street, Suite 536
Oakland, California 94612-4305

SUBJECT: APPROVE A DATA SHARING AGREEMENT WITH THE UNIVERSITY SYSTEM OF GEORGIA, GEORGIA STATE UNIVERSITY, TO PROVIDE THE SHARING OF INFORMATION FOR ALAMEDA COUNTY'S PILOT TO POSITIVE REENTRY PROGRAM

Dear Board Members:

RECOMMENDATIONS:

A. Approve a Data Sharing Agreement with the Regents of the University System of Georgia, Georgia State University to provide Second Chance Act Reentry Initiative Evaluation Services for the period 10/1/2020-9/30/2024 at no cost to the County; and

B. Delegate authority to the Interim Chief Probation Officer, or designee, to negotiate and execute a Data Sharing Agreement, subject to review and approval as to form by County Counsel and return an executed copy to the Clerk of the Board for filing.

DISCUSSION/SUMMARY:

On November 17, 2020 (Item No. 36), your board accepted the Fiscal Year 2020-21 Second Chance Act Evaluation Participation Support grant from the Bureau of Justice Assistance (BJA) to fund a randomized controlled trial of Alameda County Probation Department's Pathways Home initiative for the period 10/1/20 – 9/30/24, in the amount of $800,000. This grant requires that researchers from Georgia State University, led by Dr. William Sabol, lead this evaluation as part of the National Institute of Justice's national multi-site evaluation of the Second Chance Act (SCA) program. As a stipulation of BJA funding, the Alameda County Probation Department (ACPD) has agreed to facilitate access to the necessary information to support the multi-site evaluation that begins in 2021 and is intended to end in 2024. Your board is requested to approve the addition of a data sharing agreement to this grant.

ACPD will share data related to individuals who are now or have been under the supervision of ACPD. Data will include all relevant variables retained by ACPD that, by mutual agreement of ACPD and the Georgia State University research team, are necessary for the successful completion of the evaluation project. Data used in this research evaluation includes the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code § 13202. This shared data is highly sensitive and will be protected by all parties. The data sharing agreement is the tool that addresses how and when the data will be used and the protocols for storage and destruction of data.

SELECTION CRITERIA/PROCESS:

On September 20, 2020, the Alameda County Probation Department (ACPD) received notice from the Office of Justice Programs of a grant award from the Fiscal Year (FY) 2020-21 Second Chance Act Evaluation Participation Support grant program. This grant provides $800,000 to support a randomized controlled trial of ACPD's Pathways Home initiative, which involves four innovative components designed to improve the reentry experience for individuals returning to Alameda County from state prison on Post-Release Community Supervision:

(1) Case-planning and service referrals initiated before clients are released from state prison;
(2) Virtual reality simulations available pre- and post-release to help clients practice appropriate responses to challenging situations;
(3) A mobile application, Vergil, that supports successful goal-based community supervision using insights from behavioral science; and
(4) Reentry workbooks specific to Alameda County that are disseminated to clients who will return to Alameda County prior to their release.

Georgia State University was selected by the National Institute of Justice as the independent evaluation partner that will oversee this evaluation. ACPD is therefore required to work with Georgia State University as a condition of its FY20 Second Chance Act Evaluation Participation Support grant award.

FINANCING:

There is no cost associated with this data sharing agreement. Therefore, there is no impact in net County cost as a result of approving the above recommendations.

VISION 2026 GOAL:

The Pathways Home Pilot meets the 10X goal pathway of a **Crime Free County** in support of our shared visions of a **Thriving and Resilient Population** and **Safe and Livable Communities**.

August 30, 2021

Respectfully submitted,

DocuSigned by:
Marcus Dawal
436902B1EF8A47A...

Marcus Dawal
Interim Chief Probation Officer

Md:cd

Data Sharing Agreement

This Data Sharing Agreement (DSA) is entered into by and between the County of Alameda, acting by and through its Probation Department ("ACPD") and The Board of Regents of the University System of Georgia by and on the behalf of Georgia State University ("University") on behalf of its researchers in the Andrew Young School of Policy Studies ("Researchers"). As a site chosen by the Bureau of Justice Assistance ("BJA"), ACPD received grant funding ("the Grant") to support participation in a multi-site evaluation of the Pathways Home project on behalf of the National Institute of Justice ("NIJ"). The Researchers have been engaged by the NIJ to conduct the multi-site evaluation. As a stipulation of BJA funding, ACPD has agreed to facilitate access by the Researchers to the necessary information to support the multi-site evaluation, beginning in 2021 and intended to end in 2024.

1. RECITALS

A. Whereas the Researchers have been engaged to conduct an evaluation of Bureau of Justice selected Second Chance Act ("SCA") grantee sites as part of a multi-site evaluation funded by the NIJ. As a grant recipient, ACPD agrees to provide the Researchers with data needed to support the Researchers' evaluation to examine program implementation processes, outcomes, impact, and costs, pursuant to the Grant requirements, and this DSA.

2. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this DSA is to outline the terms and conditions agreed to by the University and ACPD regarding the transfer and analysis of all necessary data related to the Pathways Home program, criminal offender record information pursuant to the authority granted in California Penal Code § 13202.

3. DEFINITIONS

"DSA" 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). The Researchers will only request Criminal Offender Record Information necessary to conduct the evaluation of the SCA Pathways Home program.

4. DESCRIPTION OF DATA TO BE SHARED

ACPD will share relevant data and materials related to creation, implementation, daily operation, and any assessments of its SCA-related Pathways Home program retained by ACPD that, by mutual agreement of ACPD and the Researchers, are necessary conducting both the process and outcome components of the Pathways project evaluation in accordance with the Grant and the University's SCA evaluation. Information

will include data and materials The following will be provided to the extent that they are available and accessible by ACPD.

- Individual-level data for clients under active Post Release Community Supervision (PRCS), Mandatory Supervision (MS), and Formal Probation supervision between January 2019 and December 2025. These data will be used to examine implementation and outcomes for both Pathways participants and a non-participant, comparison population. Individual-level data will include the following to the extent they are available in the case management system:
  - Full name (Last, First, Middle)
  - Personal File Number (PFN)
  - Date of Birth
  - Demographic characteristics (e.g., race, ethnicity, gender)
  - Client referral status history (date and status)
  - Program/Service referral and enrollment status and date, with other pertinent program data, as available
  - Associated offense history, where available (e.g., conviction date, conviction offense, sentence date)
  - COMPAS assessment score, supervision level, and domain scores
  - Caseload assignment
  - Pathways-related activity (e.g., pre-release video conference participation, virtual reality program enrollment)
- Finalized internal reports documenting local Pathways program implementation and evaluation.
- Pathways-specific expenditure and revenue data on sources of support for program implementation and maintenance. Pathways-specific funding sources and expenses incurred. The purpose of this information is to examine the effectiveness of the program in relation to its cost. These data may include:
  - ACPD Pathways-dedicated staffing
  - Contract vendor costs
- Approved internal procedures and policies related to the Pathways program including information of participant outreach and recruiting.

5. DESCRIPTION OF INTENDED USE

Data will be used to describe and evaluate the Pathways Home program, as outlined in the DSA.

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 email transmission.

7. DATA SECURITY

All data provided by ACPD shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this DSA. The secure environment where all data will be stored is Alameda County Secure FTP (SFTP). This SFTP meets the University's Institutional Review Board, and HIPAA security and confidentiality requirements.

a. Protection of Data

The Researchers agree to store data on one or more of the following media and protect the data as described:

1) Data Analysis. All data analysis of identifiable data will be conducted on the secured network and subject to applicable requirements below. All individual-level data transferred to or analyzed on any portable devices will de-identified prior to transfer and analysis from the secured network.

2) 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 and will require multi-factor authentication. If the workstation is located in an unsecured physical location the hard drive will be encrypted to protect ACPD data in the event the device is stolen.

3) 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 and a multi-factor authentication process. Backup copies for disaster recovery purposes will be encrypted if recorded to removable media.

4) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by ACPD 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 DSA, 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 ACPD 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 ACPD 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) ACPD data shall not be stored by the Researchers on portable devices or media unless specifically authorized within this DSA. If so authorized, the data shall be given the following protections by the Researchers:

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 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 ACPD data will be under the physical control of the Researchers' 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**

The Researchers 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 DSA:

1) Access to the information provided by ACPD 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 DSA.

2) The Researchers 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 DSA, the Researchers will not store any confidential or sensitive ACPD 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) The Researchers 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) The Researchers shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

6) The Researchers 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 DSA, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this DSA.

7) The Researchers shall take due care and take reasonable precautions to protect ACPD's data from unauthorized physical and electronic access.

8) The Researchers 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**

The Researchers shall comply with the following requirements:

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

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

3) When stored on electronic media, ACPD data will be stored in a logical container on electronic media, such as a partition or folder dedicated to ACPD data.

4) When stored in a database, ACPD data will be stored in a database which will contain no non-ACPD data.

5) When stored within a database, ACPD data will be stored within a database and will be distinguishable from non-ACPD data by the value of a specific field or fields within database records.

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

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

If the Researchers, University, 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, the Researchers shall give notice to ACPD within three (3) business days of discovering the compromise or potential compromise.

The Researchers 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. ACPD retains ownership of all data provided pursuant to this DSA including, but not limited to, any subsets generated from the raw data, individual-level subsets derived from the raw data, and any data from ACPD that becomes part of data sets generated by addition to or combination with other any other data.

b. The Researchers may not relinquish, or transfer ownership or physical custody of the data provided pursuant to this DSA to any entity.

9. DATA SHARING AGREEMENT COMPLETION/TERMINATION

a. This Agreement shall terminate on the following date: December 31, 2025

b. Upon completion or termination of this DSA, the data provided pursuant to the terms of this DSA shall be destroyed or returned to ACPD with certification by the Researchers that the original and all copies of the data on all systems and media have been destroyed.

c. This DSA 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.

d. Upon execution of this DSA, all Researchers' staff with access to, or that have accessed the data provided pursuant to the terms of this DSA will be notified of the non-disclosure provisions of this DSA.

e. ACPD may terminate this DSA with a prior written notice to the Researchers, with approval form the NIJ, or in accordance with the Grant requirements with the BJA.

10. DATA CONFIDENTIALITY

a. Regulations Governing Confidentiality of Data

   i. The Researchers acknowledge the confidential nature of the data received from ACPD and agree that personnel with access shall comply with all laws, regulations, and policies that apply to the protection of the confidentiality of the data.

   ii. Any willful, malicious, negligent, or knowing disclosure of the data received pursuant to this DSA to unauthorized persons may be punishable by applicable state and federal laws.

b. Limited Access to Data

   i. Only staff assigned by the Researchers 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 DSA will access the data received pursuant to this DSA.

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

c. Safety and Security

   The Researchers acknowledge and agree 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 DSA may be used ONLY for the purpose described in the Grant and this DSA and only for the term of the Grant and DSA.

b. This DSA 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 the Grant, and this DSA. Any ad hoc analysis or other use of the data, not expressly specified in

the Grant, and this DSA, is not permitted without the prior written authorization of ACPD.

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 ACPD pursuant to this DSA to any individual or agency, unless the Grant and DSA 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 and provisions of the Grant, and within this DSA and that have received approval from ACPD.

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

iii. Non-disclosure requirements should not be interpreted to limit Researchers' ability to present, distribute, or publish summaries of data or evaluation results that do not include individual-level and/or identifiable data, to the extent consistent with applicable laws and regulations.

b. Any exceptions to these limitations must be approved in writing by ACPD.

c. Penalties for Unauthorized Disclosure of Information:

Should the Researchers fail to comply with any terms of this DSA, ACPD 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

The Researchers shall ensure that all staff with access to the data provided pursuant to this DSA are aware of the use and disclosure requirements of this DSA and will advise all staff of the provisions of this DSA. This notification shall include all IT support staff as well as staff who will manipulate and/or analyze the data. All staff will receive probation administered Live Scans at ACPD’s expense.

SIGNATURES

The parties have executed this Data Sharing Agreement by and through their duly authorized representatives. By signing below, signatory warrants and represents that he/she executed this Data Sharing Agreement in his/her authorized capacity and that by his/her signature on this Data Sharing Agreement, he/she or the entity upon behalf of which he/she acted, executed this Data Sharing Agreement.

Alameda County Probation Department

By: _____ Date:_____

Marcus Dawal
Interim Chief Probation Officer

xxx (xxx)

By: _____ Date:_____

The Board of Regents of the University System of Georgia by and on behalf of Georgia State University

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff

By:_____ Date:_____
Project Staff