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

September 1, 2021

Honorable Board of Supervisors
County Administrator Building
1221 Oak Street, Suite 536
Oakland, CA 94612-4305

Dear Board Members:

SUBJECT: AUTHORIZE A FIRST AMENDMENT WITH BRIGHT RESEARCH GROUP TO ADD A DATA SHARING AGREEMENT TO PROVIDE EVALUATION SERVICES FOR THE WE RISE PROJECT; PROCUREMENT CONTRACT NO. 22084

RECOMMENDATIONS:

A. Approve a First Amendment (Procurement Contract No. 22084) with Bright Research Group to add a Data Sharing Agreement to the contract to provide evaluation services for the WE RISE project, with no change in the current term of 5/1/2021 – 09/30/2022, and no change in the contract amount of $129,150; and

B. Delegate authority to the Interim Chief Probation Officer, or designee, to execute the Amendment upon review and approval as to form by County Counsel, and to submit an executed copy to the Clerk of the Board for filing.

DISCUSSION/SUMMARY:

On May 18, 2021 your Board approved (Item No.58) a contract with Bright Research Group to provide evaluation services for the WE RISE project, which delivers intensive case management and life coaching support to gang-affiliated youth returning to Oakland following detention in Alameda County's Juvenile Hall. Your Board is requested to approve an amendment to add a data sharing agreement to the contract.

The Alameda County Probation Department (ACPD) will share state and local Criminal Offender Record Information related to participants in the WE RISE program who are now or have been under the jurisdiction of ACPD. Data will include all relevant variables retained by ACPD that, by mutual agreement of ACPD and Bright Research Group, are necessary for the successful completion of the evaluation project. This shared data is highly sensitive and must 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.

Delegation of authority to the Interim Chief Probation Officer is being requested to add the Data Sharing Agreement to the existing contract. There are no changes to the contract term or amount as a result of this action.

SELECTION CRITERIA/PROCESS:

Bright Research Group is named in the Alameda County Probation Department's Second Chance Act grant from the OJJDP as a subrecipient of funds to conduct a process and outcome evaluation of program activities and is therefore mandated by the federal grant funding.

GSA approved Sole Source #7387 and issued a Finding Memo of Non-Competition on 4/15/2021. Bright Research Group is a certified small, local, and emerging business (Certificate No.13-00098) expires on 7/31/2022.

FINANCING:

There will be no increase in net County cost as result of approving the above recommendation.

VISION 2026 GOAL:

The awareness and strategic prevention and intervention services that work to reduce juvenile cannabis use meets the County's 10X goal pathways of a **Crime Free County** in support of the County's shared visions of a **Thriving and Resilient Population** and **Safe and Livable Communities**.

Respectfully submitted,

Marcus Dawal
Interim Chief Probation Officer

MD/ss

FIRST AMENDMENT TO AGREEMENT

This First Amendment to Agreement ("First Amendment") is made by the County of Alameda ("County") and Bright Research Group, ("Contractor") with respect to that certain agreement entered by them on March 18, 2021 (referred to herein as the "Contract") pursuant to which Contractor provides evaluation services for the WE RISE project to County.

County and Contractor agree as follows:

1. Except as otherwise stated in this First Amendment, the terms and provisions of this Amendment will be effective as of the date this First Amendment is executed by the County.

2. The attached Exhibit G, Data Sharing Agreement, is incorporated into this Agreement by this reference.

3. DEBARMENT AND SUSPENSION CERTIFICATION:

   a. By signing this First Amendment and Exhibit D-1, Debarment and Suspension Certification, which is attached and incorporated into this Agreement by this reference, Contractor/Grantee agrees to comply with applicable federal suspension and debarment regulations, including but not limited to 7 Code of Federal Regulations (CFR) 3016.35, 28 CFR 66.35, 29 CFR 97.35, 34 CFR 80.35, 45 CFR 92.35 and Executive Order 12549.

   b. By signing this First Amendment, Contractor certifies to the best of its knowledge and belief, that it and its principals:

      (1) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntary excluded by any federal department

or agency;

(2) Shall not knowingly enter into any covered transaction with a person who is proposed for debarment under federal regulations, debarred, suspended, declared ineligible, or voluntarily excluded from participation in such transaction.

4. Except as expressly modified by this First Amendment all of the terms and conditions of the contract are and remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this First Amendment to the Agreement as of the day and year this First Amendment is executed by the County below.

COUNTY OF ALAMEDA

By:_____
Signature

Name: Marcus Dawal
(Printed)

Title: Interim Chief Probation Officer

Date:_____

BRIGHT RESEARCH GROUP

By:_____
Signature

Name:_____
(Printed)

Title:_____

Date:_____

Approved as to Form:
Donna R. Ziegler, County Counsel

By:_____
K. Joon Oh, Deputy County Counsel

By signing above, signatory warrants and represents that he/she executed this First Amendment in his/her authorized capacity and that by his/her signature on this First Amendment, he/she or the entity upon behalf of which he/she acted, executed this First Amendment

EXHIBIT D-1

COUNTY OF ALAMEDA
DEBARMENT AND SUSPENSION CERTIFICATION

The contractor, under penalty of perjury, certifies that, except as noted below, contractor, its principals, and any named or unnamed subcontractor:

- **Is not currently under suspension, debarment, voluntary exclusion, or determination of ineligibility by any federal agency;**
- **Has not been suspended, debarred, voluntarily excluded or determined ineligible by any federal agency within the past three years;**
- **Does not have a proposed debarment pending; and**
- **Has not been indicted, convicted, or had a civil judgment rendered against it by a court of competent jurisdiction in any matter involving fraud or official misconduct within the past three years.**

If there are any exceptions to this certification, insert the exceptions in the following space.

Exceptions will not necessary result in denial of award, but will be considered in determining contractor responsibility. For any exception noted above, indicate below to whom it applies, initiating agency, and dates of action.

Notes: Providing false information may result in criminal prosecution or administrative sanctions. The above certification is part of the Standard Services Agreement. Signing this Standard Services Agreement on the signature portion thereof shall also constitute signature of this Certification.

CONTRACTOR: _____

PRINCIPAL: _____ TITLE: _____

SIGNATURE: _____ DATE: _____

Exhibit G
Data Sharing Agreement

This Data Sharing Agreement has been incorporated into the Standard Service Agreement, Procurement Contract No. 22084 dated May 18, 2021, by and between the County of Alameda, acting by and through its Probation Department (Probation) and Bright Research Group ("Contractor").

1. RECITALS

A. **WHEREAS,** Probation received a Second Chance Act grant through the Office of Justice Programs' Office of Juvenile Justice and Delinquency Prevention (OJJDP) to deliver intensive case management and life coaching to gang-affiliated youth returning to Oakland from Alameda County's Juvenile Hall for the term of October 1, 2018 through September 30, 2021; and

WHEREAS, the grant required Probation to contract with Bright Research Group to conduct a process and outcome evaluation of the program, which is known as WE RISE; and

WHEREAS, Probation has entered into an agreement with Bright Research Group to conduct a process and outcome evaluation of WE RISE to determine its impact on youth participants and their families and fully describe operational elements of the program for replication by other jurisdictions, for a contract term of 5/1/21 to 9/30/22 and a contract amount of $129,150; and

WHEREAS, Bright Research Group requires data from Probation on WE RISE participants in order to conduct an adequate process and outcome evaluation

NOW, THEREFORE, BE IT RESOLVED as follows:

1. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement is to outline the terms and conditions agreed to by Bright Research Group and Probation regarding the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code § 13202.

2. 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)

3. DESCRIPTION OF DATA TO BE SHARED

Probation will provide the following information for clients who participated in the WE RISE program between 1/1/2020, when the WE RISE program began, and 9/30/2022.

- Client Name (Last, First)
- Client demographic characteristics (Date of Birth, Race, Ethnicity, Gender)
- Violations filed by DPOs (not violations filed by the District Attorney)
- Client referral statuses with dates
- Results from all YLS-CMI assessments

Probation will also provide the above deidentified data (without Client Name) for those probation clients meeting the eligibility criteria for the WE RISE program who did not participate in the program but were active during this time period. These data may be used by Bright Research Group to derive a comparison population.

Probation will also share data on client participation in the WE RISE program and results from Social Embeddedness Tool assessments conducted with WE RISE participants at four times during the program: (1) within 3 months of program enrollment; (2) Approximately 9 months after program enrollment; (3) when probation term is completed; (4) 6-12 months following program completion.

4. DESCRIPTION OF INTENDED USE

Data will be used to evaluate the impact of the WE RISE program on probation completion, recidivism, and gang affiliation for program youth, as described in the Agreement.

5. 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 HIPAA protected data will be encrypted prior to email transmission.

6. DATA SECURITY

All data provided by Probation 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**

Bright Research Group 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 Probation 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 disaster recovery 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 Probation 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 Probation 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 Probation 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) Probation data shall not be stored by Bright Research Group on portable devices or media unless specifically authorized within this DSA. If so authorized, the data shall be given the following protections by Bright Research Group:

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.

Passwords must be changed every 90 days

Passwords should be at least 8 characters and include upper case, lower case, number and special character

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 Probation data will be under the physical control of Bright Research Group 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**

Bright Research Group 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 Probation 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) Bright Research Group 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, Bright Research Group will not store any confidential or sensitive Probation 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) Bright Research Group 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) Bright Research Group shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

6) Bright Research Group 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) Bright Research Group shall take due care and take reasonable precautions to protect Probation's data from unauthorized physical and electronic access.

8) Bright Research Group 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**

Contractor shall comply with the following requirements:

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

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

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

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

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

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

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

If Bright Research Group 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, Bright Research Group shall give notice to Probation within one (1) business day of discovering the compromise or potential compromise.

Bright Research Group 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.

7. DATA OWNERSHIP

a. Probation 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 sets generated by addition to or combination with other any other data.

b. Bright Research Group may not relinquish or transfer ownership or physical custody of the data provided pursuant to this Agreement to any entity.

8. DATA SHARING AGREEMENT COMPLETION/TERMINATION

a. This Agreement shall terminate on the following date: 9/30/2022.

b. Upon completion or termination of this Agreement or DSA, the data provided pursuant to the terms of this DSA shall be destroyed or returned to Probation with certification by

Contractor 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 Data Sharing Agreement, all Contractor 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. Probation may terminate, suspend, or abandon this Data Sharing Agreement with a prior written notice to Bright Research Group as provided for in paragraph 20 of the Agreement.

9. DATA CONFIDENTIALITY

a. Regulations Governing Confidentiality of Data

i. Bright Research Group acknowledges the confidential nature of the data received from Probation 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 Bright Research Group shall have access to review, manipulate, and maintain the data received for their organization. Bright Research Group is responsible for ensuring that only authorized staff with a business need directly related to the purpose of the Agreement and DSA will access the data received pursuant to this DSA. 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 Probation on request.

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

c. Safety and Security

Bright Research Group 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.

10. CONSTRAINTS ON USES OF THE DATA RECEIVED

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

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 this Agreement and DSA. Any ad hoc analysis or other use of the data, not expressly specified in this Agreement and DSA, is not permitted without the prior written authorization of Probation.

11. NON-DISCLOSURE OF DATA

a. Non-Disclosure of Data Requirements:

i. No person shall disclose, in whole or in part, the data provided by Probation pursuant to this Agreement to any individual or agency, unless this Agreement 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 of this Agreement and DSA and that have received approval from Probation.

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 Probation.

c. Penalties for Unauthorized Disclosure of Information:

Should Bright Research Group fail to comply with any terms of this Agreement or DSA, Probation 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

Bright Research Group 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

Bright Research Group

By: _____ Date:_____

Brightstar Ohlson
Chief Executive Officer & Principal

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

Bright Research Group Staff:

By:_____ Date:_____

[Moira De Nike]

By:_____ Date:_____

[Carrie Oliver]

By:_____ Date:_____

[Alice Hu-Nguyen]

By:_____ Date:_____

[Chantiri Resendiz]

Data Sharing Agreement

This Data Sharing Agreement has been incorporated into the Standard Service Agreement dated May 18, 2021, by and between the County of Alameda, acting by and through its Probation Department (Probation) and Bright Research Group.

1. RECITALS

A. **WHEREAS,** Probation received a Second Chance Act grant through the Office of Justice Programs' Office of Juvenile Justice and Delinquency Prevention (OJJDP) to deliver intensive case management and life coaching to gang-affiliated youth returning to Oakland from Alameda County's Juvenile Hall for the term of October 1, 2018 through September 30, 2021; and

WHEREAS, the grant required Probation to contract with Bright Research Group to conduct a process and outcome evaluation of the program, which is known as WE RISE; and

WHEREAS, Probation has entered into an agreement with Bright Research Group to conduct a process and outcome evaluation of WE RISE to determine its impact on youth participants and their families and fully describe operational elements of the program for replication by other jurisdictions, for a contract term of 5/1/21 to 9/30/22 and a contract amount of $129,150; and

WHEREAS, Bright Research Group requires data from Probation on WE RISE participants in order to conduct an adequate process and outcome evaluation

NOW, THEREFORE, BE IT RESOLVED as follows:

1. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement is to outline the terms and conditions agreed to by Bright Research Group and Probation regarding the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code § 13202.

2. 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)

3. DESCRIPTION OF DATA TO BE SHARED

Probation will provide the following information for clients who participated in the WE RISE program between 1/1/2020, when the WE RISE program began, and 9/30/2022.

- Client Name (Last, First)
- Client demographic characteristics (Date of Birth, Race, Ethnicity, Gender)
- Violations filed by DPOs (not violations filed by the District Attorney)
- Client referral statuses with dates
- Results from all YLS-CMI assessments

Probation will also provide the above deidentified data (without Client Name) for those probation clients meeting the eligibility criteria for the WE RISE program who did not participate in the program but were active during this time period. These data may be used by Bright Research Group to derive a comparison population.

Probation will also share data on client participation in the WE RISE program and results from Social Embeddedness Tool assessments conducted with WE RISE participants at four times during the program: (1) within 3 months of program enrollment; (2) Approximately 9 months after program enrollment; (3) when probation term is completed; (4) 6-12 months following program completion.

4. DESCRIPTION OF INTENDED USE

Data will be used to evaluate the impact of the WE RISE program on probation completion, recidivism, and gang affiliation for program youth, as described in the Agreement.

5. 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.

6. DATA SECURITY

All data provided by Probation 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**

Bright Research Group 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 Probation 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 Probation 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 Probation 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 Probation 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) Probation data shall not be stored by Bright Research Group on portable devices or media unless specifically authorized within this Agreement. If so authorized, the data shall be given the following protections by Bright Research Group:

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.

Passwords must be changed every 90 days

Passwords should be at least 8 characters and include upper case, lower case, number and special character

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 Probation data will be under the physical control of Bright Research Group 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**

Bright Research Group 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 Probation 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) Bright Research Group 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, Bright Research Group will not store any confidential or sensitive Probation 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) Bright Research Group 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) Bright Research Group shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

6) Bright Research Group 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) Bright Research Group shall take due care and take reasonable precautions to protect Probation's data from unauthorized physical and electronic access.

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

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

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

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

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

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

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

If Bright Research Group 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, Bright Research Group shall give notice to Probation within one (1) business day of discovering the compromise or potential compromise.

Bright Research Group 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.

7. DATA OWNERSHIP

a. Probation 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 Probation nor Bright Research Group may relinquish or transfer ownership or physical custody of the data provided pursuant to this Agreement to any entity.

8. DATA SHARING AGREEMENT COMPLETION/TERMINATION

a. This Agreement shall terminate on the following date: 9/30/2022.

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

c. 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.

d. 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.

e. Probation may terminate this Data Sharing Agreement with a prior written notice to Bright Research Group as provided for in paragraph 20 of the Agreement.

9. DATA CONFIDENTIALITY

a. Regulations Governing Confidentiality of Data

i. Bright Research Group acknowledges the confidential nature of the data received from Probation 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 Bright Research Group shall have access to review, manipulate, and maintain the data received for their organization. Bright Research Group 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 Probation on request.

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

c. Safety and Security

Bright Research Group 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.

10. 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 Probation.

11. NON-DISCLOSURE OF DATA

a. Non-Disclosure of Data Requirements:

i. No person shall disclose, in whole or in part, the data provided by Probation 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 Probation.

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 Probation.

c. Penalties for Unauthorized Disclosure of Information:

Should Bright Research Group fail to comply with any terms of this Agreement, Probation 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

Bright Research Group 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 probation administered Live Scans at ACPD's expense.

SIGNATURES

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

Alameda County Probation Department

By: _____ Date:_____
Marcus Dawal
Interim Chief Probation Officer

Bright Research Group
By: _____ Date:_____

Brightstar Ohlson
Chief Executive Officer & Principal

All individuals who are part of Bright Research Group ’s team and who will have access to the confidential individual-level data must sign this agreement.

Bright Research Group Staff:

By:_____ Date:_____
[Moira De Nike]

By:_____ Date:_____
[Carrie Oliver]

By:_____ Date:_____
[Alice Hu-Nguyen]

By:_____ Date:_____
[Chantiri Resendiz]