

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



**ITEM: 3.23
(ID # 24321)**

MEETING DATE:
Tuesday, April 02, 2024

FROM : PUBLIC SOCIAL SERVICES:

SUBJECT: DEPARTMENT OF PUBLIC SOCIAL SERVICES (DPSS): Approve the California National Data Privacy Agreement (CA-NDPA) from Riverside County Superintendent of Schools (RCSS) to allow for Riverside County Superintendent of Schools to share data in accordance with AB-210 allowing RCSS to participate in Multidisciplinary Teams (MDTs) across multiple County Departments and Agencies; and authorize the Chairman of the Board to sign the Agreement on behalf of the County; All Districts. [Total Cost \$0]

RECOMMENDED MOTION: That the Board of Supervisors:

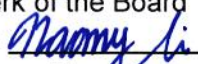
1. Approve the California National Data Privacy Agreement (CA-NDPA) from Riverside County Superintendent of Schools to share data;
2. Authorize the Chair of the Board to sign the Agreement on behalf of the County.

ACTION:Policy

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Spiegel, seconded by Supervisor Gutierrez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Jeffries, Spiegel, Washington, Perez and Gutierrez
Nays: None
Absent: None
Date: April 2, 2024
xc: DPSS

Kimberly A. Rector
Clerk of the Board
By: 
Deputy

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

| FINANCIAL DATA | Current Fiscal Year: | Next Fiscal Year: | Total Cost: | Ongoing Cost |
|-----------------------------|-----------------------------|--------------------------|-------------------------------|---------------------|
| COST | \$0 | \$0 | \$0 | \$0 |
| NET COUNTY COST | \$0 | \$0 | \$0 | \$0 |
| SOURCE OF FUNDS: N/A | | | Budget Adjustment: N/A | |
| | | | For Fiscal Year: 23/24 | |

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

On December 7, 2021 (item 3.34), the Board authorized the County Executive Office to lead the initiative to fully develop the Integrated and Comprehensive County Health and Human Services System. The initiative aims to incorporate the work, service provision and data of multiple County departments and various community-based organizations into an integrated system aimed at serving vulnerable, high needs residents. The system provides guidelines regarding access to processing and sharing of client data for the purpose of increasing operational efficiencies, leveraging strategic partnerships, streamlining application and case management processes, and developing a client-centered service delivery model. The goal is to improve health, self-sufficiency, recovery, and well-being services, and develop holistic, effective and efficient models of person-centered coordinated services among participating agencies.

California Assembly Bill 210 (AB-210) became effective on January 1, 2018, and created section 18999.8 of the Welfare and Institutions Code. This bill permits multidisciplinary personnel teams (MDTs) of Participating Agencies to share and exchange information made confidential by State law to facilitate the expedited identification, assessment, and linkage of homeless individuals and families to housing and supportive services within the County.

AB-210 authorizes counties to establish homeless individuals and family multidisciplinary teams (MDTs) to facilitate the expedited identification, assessment, and linkage of homeless individuals and families to housing and supportive services. While state laws generally prohibit the sharing of an individual's confidential health, mental health, criminal history, and social services information, AB-210 authorizes MDT members to share such information to improve coordination of housing and supportive services, increase continuity of care, and decrease duplication of services.

In accordance with AB-210, and as part of the Integrated Services Delivery (ISD) Initiative, MDTs are being established to include a wide range of staff from County Departments, affiliated agencies such as housing authorities or contracted homeless service providers, other governmental agencies, and non-governmental agencies that have as one of their purposes the identification, assessment, and linkage of homeless individuals to housing and services.

The Riverside County Superintendent of Schools (RCSS) is requesting that the County execute the California National Data Privacy Agreement (CA-NDPA) prior to participation in MDTs. Approval of this document will allow RCSS to participate in the data exchange and provide information such as Demographic Information; Service and Program History; Nutrition Data; Benefits History and Status; Housing and Homeless History and Status; and other relevant information as needed for identification.

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

Impact on Residents and Businesses

The Integrated Services Delivery Initiative is a collaborative partnership that ensures effective evidence-based services in a comprehensive and culturally responsive manner. It provides better quality service delivery to homeless individuals and families; an increased ability to match homeless clients to appropriate services and housing; and reduced costs to County systems by decreasing duplication of services to homeless clients and improving targeting of interventions.

ATTACHMENTS

Attachment A: California National Data Privacy Agreement (CA-NDPA)

Attachment B: AB 210 Participating Agency Agreement

Attachment C: AB 210 Employee Confidentiality Statement

Attachment D: AB 210 Protocol for MDT's

Attachment E: AB 210 Policies and Procedures


Erianna Lontajo, Principal Management Analyst

3/26/2024


Katherine Wilkins, Deputy County Counsel

3/12/2024


Gregg Gu, Chief of Deputy County Counsel

3/13/2024

STANDARD STUDENT DATA PRIVACY AGREEMENT

**CA-NDPA Standard
Version 1.0 (10.25.20)**

Riverside County Superintendent of Schools

and

Riverside County

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

Riverside County Superintendent of Schools located at PO Box 868 Riverside, CA 92501
(the "**Local Education Agency**" or "**LEA**") and
Riverside County, located at 4060 County Circle Dr, Riverside, CA 92503
(the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
D if Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the **ffServices**).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: _____ Attn: Contracts & Purchasing Title: Administrator

Address: _____ PO Box 868 Riverside, CA 92501

Phone: 951-826-6892 Email: purchasing@rcoe.us

The designated representative for the Provider for this DPA is:

Name: Joan Danfifer Title: Administrative Services Manager II

Address: 4060 County Circle Drive, Riverside, CA 92503

Phone: 951-358-4536 Email: dpsscontracts@rivco.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Riverside County Superintendent of Schools

By: *Parvina M. Ashor*

Date: 7 LJJJ 11 Y

Printed Name: Cuxm-u-. μ.DcAwt Title/Position: M...14y-r | Lol.-+rc.c-b -cchw1

PROVIDER: Riverside County

By: cluu:k, wt>.,1,m Af-r-n,, vv, vvr 'Y Date: A_p_r_4_,_2_0_24

Printed Name: C_h_u_c_k_W_a_s_h_i_n_g_t_o_n Title/Position: Chairman of the Board

Approval as to
form Minh C. Tran
County Counsel
Kathen11e W1k111s
i.1y: _____
Katherine Wilkins
Deputy County Counsel IV
Date: Mar 14, 2024

ATTEST:
KIMBERLY A. RECTOR, Clerk
Naomy .Sicra
By: _____
DEPUTY

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **DISPOSITION of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section 113. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider **will** allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any auditor investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular Instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a *waiver* of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.
IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST
EACH PRODUCT (RESOURCE) HERE]

EXHIBIT "B"
SCHEDULE OF DATA

| Category of Data | Elements | Check if Used by Your System | | |
|-------------------------------------|--|------------------------------|-------------------------------------|--------------------------|
| Application Technology Meta Data | IP Addresses of users, Use of cookies, etc. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Other application technology meta data-Please specify: | | | |
| Application Use Statistics | Meta data on user interaction with application | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Assessment | Standardized test scores | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Observation data | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Other assessment data-Please specify: | | | |
| Attendance | Student school (daily) attendance data | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Student class attendance data | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Communications | Online communications captured (emails, blog entries) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Conduct | Conduct or behavioral data | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Demographics | Date of Birth | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Place of Birth | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Gender | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Ethnicity or race | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Language Information (native, or primary language spoken by student) | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | Other demographic information-Please specify: | | | |
| Enrollment | Student school enrollment | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Student grade level | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Homeroom | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Guidance counselor | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Specific curriculum programs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Year of graduation | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Other enrollment information-Please specify: | | | |
| Parent/Guardian Contact Information | Address | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Email | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| | Phone | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Category of Data | Elements | Check If Used by Your System | | |
|-----------------------------|--|------------------------------|--|--|
| Parent/Guardian ID | Parent ID number (created to link parents to students) | | | |
| Parent/Guardian Name | First and/or Last | | | |
| Schedule | Student scheduled courses | | | |
| | Teacher names | | | |
| Special Indicator | English language learner information | | | |
| | Low income status | | | |
| | Medical alerts/ health data | | | |
| | Student disability information | | | |
| | Specialized education services (IEP or 504) | | | |
| | living situations (homeless/foster care) | | | |
| | Other indicator information-Please specify: | | | |
| Student Contact Information | Address | | | |
| | Email | | | |
| | Phone | | | |
| Student Identifiers | Local (School district) ID number | | | |
| | State ID number | | | |
| | Provider/App assigned student ID number | | | |
| | Student app username | | | |
| | Student app passwords | | | |
| Student Name | First and/or Last | | | |
| Student In App Performance | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | |
| Student Program Membership | Academic or extracurricular activities a student may belong to or participate in | | <input type="checkbox"/> | |
| Student Survey Responses | Student responses to surveys or questionnaires | | | |
| Student work | Student generated content; writing, pictures, etc. | | | |
| | Other student work data -Please specify: | | | |
| Transcript | Student course grades | | | |
| | Student course data | | | |
| | Student course grades/ performance scores | | | |

| Category of Data | Elements | Check if Used by Your System |
|------------------|---|--|
| | Other transcript data - Please specify: | |
| Transportation | Student bus assignment | <input type="checkbox"/> |
| | Student pick up and/or drop off location | <input type="checkbox"/> |
| | Student bus card ID number | <input type="checkbox"/> |
| | Other transportation data - Please specify: | |
| Other | Please list each additional data element used, stored, or collected by your application: | <ul style="list-style-type: none"> • Demographic Information • Contact Information • Income, Assets, and Resources • Citizenship/Immigration • Service and Program History • Medical History • Mental Health History • Nutrition Data • Disability Status • Housing and Homelessness History and Status • Benefit History and Status • Criminal History and Status • Probation Status • Domestic Violence Status in accordance with Pen. Code, §§ 13752 subds. (a)-(b) & 13753 subds. (a)-(b) and Pan. Code, §§ 13752 subds. (e) & 13753 subds. (e), • Veteran Status • Employment and Educational History and Status • High Risk Behavior, Violence, or Aggression History <p>This list is not exclusive. Members of homeless adult and family multidisciplinary personnel teams (MDTs) may share other information if they believe it is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services, provided that no information may be shared in a manner prohibited by federal law or regulations.</p> |
| None | No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable. | <input type="checkbox"/> |

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K--12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests overtime for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Riverside County Superintendent of Schools Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

 D Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

 Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and
Riverside County Superintendent of Schools

("Originating LEA") which is dated _____, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA, The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

PROVIDER EXHIBIT E NOTIFICATION EMAIL ADDRESS

PROVIDER: Riverside County

BY: _____ Date: **Apr 4, 2024**

Printed Name: Chuck Washington Title/Position: Chairman of the Board

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Riverside County Superintendent of Schools and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

LEA: INSERT SUBSCRIBING SCHOOL DISTRICT OR LOCAL EDUCATION AGENCY

BY: _____ Date: _____
SUBSCRIBING LEA AUTHORIZED SIGNER PRINT NAME SUBSCRIBING LEA AUTHORIZED SIGNER TITLE

Printed Name: _____ Title/Position: _____
SCHOOL DISTRICT NAME: INSERT SUBSCRIBING SCHOOL DISTRICT OR LOCAL EDUCATION AGENCY

DESIGNATED REPRESENTATIVE OF LEA:
Name: _____
Title: _____
Address: _____
Telephone Number: _____
Email: _____
DESIGNATED REPRESENTATIVE OF SUBSCRIBING LEA NAME
DESIGNATED REPRESENTATIVE OF SUBSCRIBING LEA TITLE
DESIGNATED REPRESENTATIVE OF SUBSCRIBING LEA ADDRESS
DESIGNATED REPRESENTATIVE OF SUBSCRIBING LEA PHONE NUMBER
DESIGNATED REPRESENTATIVE OF SUBSCRIBING LEA EMAIL

EXHIBIT "E"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

| | MAINTAINING ORGANIZATION/GROUP | FRAMEWORK(S) |
|--------------------------|--|--|
| <input type="checkbox"/> | National Institute of Standards and Technology | NIST Cybersecurity Framework Version 1.1 |
| <input type="checkbox"/> | National Institute of Standards and Technology | NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171 |
| <input type="checkbox"/> | International Standards Organization | Information technology - Security techniques - Information security management systems (ISO 27000 series) |
| <input type="checkbox"/> | Secure Controls Framework Council, LLC | Security Controls Framework (SCF) |
| <input type="checkbox"/> | Center for Internet Security | CIS Critical Security Controls (CSC, CIS Top 20) |
| | Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) | Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR) |

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"

Supplemental SDPC State Terms for California

Version 1.0

This Amendment for SDPC State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

Riverside County Superintendent of Schools, located at PO Box 868 Riverside, CA 92501
(the "**Local Education Agency**" or "**LEA**") and
Riverside County, located at 4060 County Circle Dr, Riverside, CA 92503
(the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. § 1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. **Term.** The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.
2. **Modification to Article IV, Section 7 of the DPA.** Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data if for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

[SIGNATURES BELOW]

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Riverside County Superintendent 31/f/, l;) U/
 By: [Signature] Date: (o...fntc fs ;)
 Printed Name: William M. O'Connell Title/Position: Superintendent of Schools

Provider: Riverside County
 By: [Signature] Date: Apr 4, 2024
 Printed Name: Chuck Washington Title/Position: Chairman of the Board

**PARTICIPATING AGENCY AGREEMENT FOR RIVERSIDE COUNTY HOMELESS
ADULT AND FAMILY MULTIDISCIPLINARY PERSONNEL TEAMS**

BACKGROUND:

Assembly Bill 210 (January 1, 2018) created section 18999.8 of the Welfare and Institutions Code. That new section permits multidisciplinary personnel teams (MDTs) of Participating Agencies to share and exchange information made confidential by State law in order to facilitate the expedited identification, assessment, and linkage of homeless adults and families to housing and supportive services within the County.

PARTICIPATING AGENCY DEFINITION:

Riverside County departments, their contracted agency providers, other governmental agency partners, and any other agencies/organizations that have, as one of their purposes, the identification, assessment, and linkage of homeless families and/or individuals to housing and supportive services to homeless adults or families within the County, may become a “Participating Agency.”

PROTOCOL:

WIC 18999.8 requires that a Countywide protocol be developed as part of implementation of the MDTs. Attached is a copy of the County’s Protocol.

POLICIES AND PROCEDURES:

WIC 18999.8 requires Participating Agencies to have uniform written policies and procedures that include security and privacy awareness training for employees who have access to information pursuant to WIC 18999.8. Attached is a copy of the Uniform County Policies and Procedures, which apply to all Participating Agencies.

CONFIDENTIALITY:

WIC 18999.8 requires all persons that have access to confidential information pursuant to the MDT to sign a confidentiality statement that includes, at minimum, general use, security safeguards, acceptable use, and enforcement policies. Further, every MDT member shall be under the same privacy and confidentiality obligations and subject to the same confidentiality penalties as the person disclosing or providing the information or records. Information and records must be maintained in a manner that ensures the maximum protection of privacy and confidentiality rights. Attached is a copy of the County’s Confidentiality Statement.

SECURITY CONTROLS:

WIC 18999.8 requires that Participating Agencies have security controls that meet applicable State and federal standards, including reasonable administrative, technical, and physical safeguards to ensure data confidentiality, integrity, and availability to prevent unauthorized or inappropriate access, use, or disclosure. Security controls are required by the County’s Protocol and Uniform County Policies and Procedures.

COMPLETE AND ACCURATE INFORMATION:

WIC 18999.8 requires that Participating Agencies take reasonable steps to ensure information provided is complete, accurate, and up to date to the extent necessary for the agency’s intended purposes and that the information has not been altered or destroyed in an unauthorized manner.

ACKNOWLEDGEMENT AND AGREEMENT:

By your signature below, you are certifying:

- Your department or agency will be a Participating Agency;
- Your department or agency has received a copy of and will abide by the County Protocol;
- Your department or agency has received a copy of and will abide by the Uniform County Policies and Procedures; and
- Your department or agency will ensure that all employees participating in information-sharing under a homeless adult and family MDT have signed the required Confidentiality Statement.

Department/Agency Name: _____

Name, Title, and Contact Information of Individual Signing on Department/Agency’s behalf:

Signature: _____

Date: _____

Please email the completed document to DPSScontracts@rivco.org and AB210@rivco.org .

AB 210 EMPLOYEE CONFIDENTIALITY STATEMENT
RIVERSIDE COUNTY HOMELESS ADULT AND FAMILY MDTs

I. Background

The passage of Assembly Bill 210 created Section 18999.8 of the Welfare and Institutions Code which permits multi-disciplinary personnel teams (MDTs) comprised of employees of Participating Agencies to share and exchange information made confidential by State law in order to facilitate the expedited identification, assessment, and linkage of homeless adults and families to housing and supportive services within the County.

MDT members may disclose and exchange with one another, otherwise confidential information if the team member possessing that information, reasonably believes it is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services, provided that no information may be shared in a manner prohibited by federal law or regulations.

Ensuring the confidentiality of information regarding homeless adults and families is of critical importance. All information shared between AB 210 MDT members is private and confidential. WIC 18999.8 requires all persons who have access to confidential information pursuant to the MDT to sign a confidentiality statement.

II. Use and Confidentiality of Information

As a Participating Employee, you must: 1) abide by the Riverside County Uniform Policies and Procedures governing the use, disclosure, sharing and maintenance of confidential information; 2) uphold all privacy protection standards established by Riverside County and your department/agency; and 3) comply with all federal and State laws and regulations that protect client records and are not superseded by AB 210.

The following documents set forth the Riverside County requirements for Participating Agencies and their employees governing information sharing and maintenance of the confidentiality of information:

- *Riverside County AB 210 Protocol Governing Information Sharing By Homeless Adult And Family Multidisciplinary Personnel Teams (“Riverside County Protocol”)*
- *Riverside County Uniform Policies and Procedures AB 210 Homeless Adult and Family Multidisciplinary Teams (“Riverside County Uniform Policies and Procedures”)*
- *Riverside County Board Policy A-58 Enterprise Information Systems Security Policy*
- *Riverside County Board Policy B-23 (Health Privacy Policy) and respective Department specific policies*

- *Riverside County Board Policy A-43, county Records Management and Archives*

Additionally, your employing Participating Agency may promulgate its own policies and procedures governing security, privacy, and information sharing.

III. Acknowledgement and Agreement:

By your signature below, you are certifying that:

- You have received a copy of, reviewed, and will abide by the Riverside County Protocol and Riverside County Uniform Policies and Procedures;
- You agree that you will only share/disclose information that you reasonably believe is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services;
- You understand that no confidential information or writings shall be disclosed to persons who are not members of the MDT, except to the extent required or permitted under applicable law;
- You agree that information and/or records you obtain as a MDT member will be maintained in a manner that ensures the maximum protection of privacy and confidentiality rights;
- You have completed the County's AB 210 training; and
- You understand that any violation of this Participation and Confidentiality Statement is grounds for discipline, including but not limited to the immediate suspension or revocation of your current and future authorization to disclose or receive confidential information as a member of any MDT.

Name: _____

Department/Agency Name:

Job Title: _____

Email: _____

Telephone: _____

Signature: _____ Date: _____

**RIVERSIDE COUNTY AB 210 PROTOCOL
GOVERNING INFORMATION SHARING BY HOMELESS ADULT AND FAMILY
MULTIDISCIPLINARY PERSONNEL TEAMS**

The State Legislature has recognized that the exchange of otherwise confidential information within multidisciplinary personnel teams is critically important to facilitating the expedited identification, assessment, and linkage of homeless adults and families to housing and supportive services within Riverside County.

The County and each of the agencies participating in this protocol are committed to preserving and maintaining the confidentiality of the information to be exchanged under this protocol by limiting the disclosure of such information to that which has been determined to be generally relevant to the identification, assessment, and linkage of homeless individuals and families to housing and supportive services; by preventing unauthorized access to or disclosure of such information; and by ensuring safeguards are in place to protect the confidentiality and security of such information.

1.0 Purpose of this Protocol

This protocol is drafted and implemented in accordance with Welfare and Institutions Code (WIC) section 18999.8 and is specifically intended to apply to the sharing of confidential information by the homeless adult and family multidisciplinary personnel teams established pursuant to that section. The sharing of confidential information pursuant to this protocol is intended to facilitate the expedited identification, assessment, and linkage of homeless individuals to housing and supportive services within the County and to allow provider agencies to share confidential information for the purpose of coordinating housing and supportive services to ensure continuity of care. This protocol is also intended to ensure that confidential information gathered by the team is not disclosed in violation of State or federal law.

2.0 Definitions

Unless otherwise indicated, the terms used in this protocol shall have the same meaning as in Welfare and Institutions Code section 18999.8.

3.0 Participating Agencies

- 3.1 Riverside County Departments, their contracted agency providers, other governmental agency partners, and any other agencies/organizations that has, as one of its purposes, the identification, assessment, and linkage of homeless individuals to housing and supportive services to homeless adults or families within the County, may become “Participating Agencies” subject to this protocol. Participating Agencies are identified in Attachment B, which may be updated from time to time.
- 3.2 Additional County Departments, Contracted Agencies, Governmental Agencies, and Partner Agencies may be added as a Participating Agency

upon approval by Department Public Social Services – Director or his/her designee and compliance with applicable terms herein.

- 3.3 Agencies will sign a Participating Agency Agreement to certify their participation and commitment to abide by all requirements in the Agreement.
- 3.4 All Participating County Departments will receive notice if a Participating County Department elects to cease participation or when an additional County Department becomes a Participating Agency.

4.0 Establishment of the Multidisciplinary Personnel Teams

- 4.1 Personnel of any Participating Agency shall be eligible to participate as members of a homeless adult and family multidisciplinary team if they are trained in the identification and treatment of homeless adults and families and are qualified to provide services related to homelessness. The multidisciplinary personnel team may include, but is not limited to, the following categories of persons:
 - 4.1.1 Mental health and substance abuse services personnel and practitioners or other trained counseling personnel, in accordance with 42 U.S.C. 290dd-2(g).
 - 4.1.2 Police officers, probation officers, or other law enforcement agents.
 - 4.1.3 Legal counsel for the adult or family representing them in a criminal matter.
 - 4.1.4 Medical personnel with sufficient training to provide health services.
 - 4.1.5 Case managers or case coordinators responsible for referral, linkage, or coordination of care and services to adults or families.
 - 4.1.6 Social services workers with experience or training in the provision of services to homeless adults or families or funding and eligibility for services.
 - 4.1.7 Veterans services providers and counselors.
 - 4.1.8 Domestic violence victim service organizations, as defined in subdivision (b) of Section 1037.1 of the Evidence Code and Pen. Code, §§ 13752 subds. (a)-(b) & 13753 subds. (a)-(b).
 - 4.1.9 Any public or private school teacher, administrative officer, or certified pupil personnel employee.

4.1.10 Housing or homeless services provider agencies and designated personnel.

4.2 Personnel may be designated as a member of a homeless adult and family multidisciplinary team for a particular case, and in such capacity may receive and disclose relevant information and records, within the MDT, subject to the requirements of this Protocol.

5.0 Information/Data Items that May be Disclosed and Exchanged among Members of the Homeless Adult and Family Multidisciplinary Personnel Team

5.1 The members of the homeless adult and family multidisciplinary personnel team may disclose to and exchange with one another, information that may be designated as confidential under State law, if the members of the homeless adult and family multidisciplinary personnel team possessing that information reasonably believe it is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services, provided that no information may be shared in a manner prohibited by federal law or regulations.

5.1.1 “Relevant” information shall include any information that has any tendency to assist a homeless adult and family multidisciplinary personnel team to identify, assess, and link homeless adults and families to housing and supportive services. Examples of relevant information that would be deemed shareable by and between MDTs, include but are not limited to those items of information listed on Attachment A.

5.1.2 Representatives of domestic violence victim service organizations, as defined in subdivision (b) of Section 1037.1 of the Evidence Code, shall obtain a domestic violence victim’s informed consent, in accordance with all applicable state and federal confidentiality laws, before disclosing information regarding a domestic violence victim or the victim’s family.

5.1.3 Unless there is written authorization from the patient, in accordance with all applicable laws, RUHS Behavioral Health and its contractors shall not provide any information related to Part II substance use disorder treatment programs, pursuant to 42 U.S.C. 290dd–2(g).

5.2 Participating Agencies shall take reasonable steps to ensure information is complete, accurate, and up to date to the extent necessary for the agency’s intended purposes and that the information has not been altered or destroyed in an unauthorized manner.

- 5.3 No confidential information or writings shall be disclosed to persons who are not members of the homeless adult and family multidisciplinary personnel team, except to the extent required or permitted under applicable law.
- 5.4 Information and writings shared pursuant to this protocol are confidential. Testimony concerning the information and writings shared pursuant to this protocol is not admissible in any criminal, civil, or juvenile court proceeding. Further, information and writings shared pursuant to this protocol shall be protected from discovery and disclosure by all applicable statutory and common law protections. In addition, law enforcement shall not use any information obtained via AB 210 for purposes other than to identify, assist, and link homeless individuals and families with housing and supportive services.

6.0 How Information May be Shared

- 6.1 Information may be shared by and between MDT members in person, as well as telephonically and electronically with adequate verification of the personnel involved in the exchange of information.
- 6.2 Electronic sharing of information/data under this Protocol will be facilitated by existing electronic data systems and electronic data systems that are under development (Data Systems).
- 6.3 Participating Agencies shall comply with the applicable information retention schedule established by County Policy A-43 in accordance with applicable laws.

7.0 Use of Shared Information

Information shared pursuant to this protocol will be used to facilitate the identification and assessment of homeless adults and families and their linkage to the most appropriate housing and supportive services. The information will be used to keep Participating Agencies informed about the services homeless adults and families are currently receiving or have received in the past. Shared information will be used to coordinate care, ensure continuity of care, and reduce duplication and fragmentation of services.

8.0 Policies and Procedures Addressing Security and Privacy Training

- 8.1 The County shall maintain written Uniform Policies and Procedures that require security and privacy awareness training for employees who will have access to information pursuant to this protocol.
- 8.2 The Uniform Policies and Procedures shall include a requirement that all persons who have access to information shared by Participating Agencies, sign a confidentiality statement that includes, at a minimum, general use, security safeguards, acceptable use, and enforcement policies.

- 8.3 The Uniform Policies and Procedures shall require that all Participating Agencies employ security controls that meet applicable federal and state standards, including reasonable administrative, technical, and physical safeguards to ensure data confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- 8.4 All Participating Agencies shall certify their agreement to abide by the Uniform Policies and Procedures in the Participating Agency Agreement.

9.0 Ensuring Confidentiality

- 9.1 As required by the Uniform Policies and Procedures, Participating Agencies shall employ security controls that meet applicable federal and state standards, including reasonable administrative, technical, and physical safeguards to ensure data confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- 9.2 Every member of the homeless adult and family multidisciplinary personnel team who receives information or records regarding adults and families in his or her capacity as a member of the team shall be under the same privacy and confidentiality obligations and subject to the same confidentiality penalties as the person disclosing or providing the information or records. The information or records obtained shall be maintained in a manner that ensures the maximum protection of privacy and confidentiality rights.
- 9.3 Every member of the homeless adult and family multidisciplinary personnel team represent and warrant that it has implemented and will maintain during the term of this MDT administrative, physical, and technical safeguards to reasonably protect private and confidential information, to protect against anticipated threats to the security or integrity of County data, and to protect against unauthorized physical or electronic access to or use of County data. Such safeguards and controls shall include at a minimum:
 - 9.3.1 Storage of confidential paper files that ensures records are secured, handled, transported, and destroyed in a manner that prevents unauthorized access.
 - 9.3.2 Control of access to physical and electronic records to ensure County data is accessed only by individuals with a need to know for the delivery of MDT services.
 - 9.3.3 Control to prevent unauthorized access and to prevent members of the homeless adult and family multidisciplinary personnel team

employees from providing County data to unauthorized individuals.

9.3.4 Firewall protection.

9.3.5 Use of encryption methods of electronic County data while in transit from the County networks to external networks, when applicable.

9.3.6 Measures to securely store all County data, including, but not be limited to, encryption at rest and multiple levels of authentication and measures to ensure County data shall not be altered or corrupted without County's prior written consent. The member of the homeless adult and family multidisciplinary personnel team further represent and warrant that it has implemented and will maintain during the term of this MDT administrative, technical, and physical safeguards and controls consistent with State and federal security requirements.

9.4 Information and records communicated or provided to the team members by all providers and agencies shall be deemed private and confidential and shall be protected from discovery and disclosure by all applicable statutory and common law protections. Existing civil and criminal penalties shall apply to the inappropriate disclosure of information held by the team members.

10.0 Implementation and Oversight

Department Public Social Services, Adult Services Division, will provide oversight and coordination of activities under this protocol and the development and implementation that supports this protocol, in addition to serving as a Participating Agency.

Riverside County Information Technology (RCIT) will assist in the development and implementation of any new County government information system that directly supports the exchange of information under this protocol.

Relevant Categories of Information to be Shared*

- Demographic Information
- Contact Information
- Income, Assets, and Resources
- Citizenship/Immigration Data
- Service and Program History
- Medical History
- Mental Health History
- Nutrition Data
- Disability Status
- Housing and Homeless History and Status
- Benefit History and Status
- Criminal History and Status
- Probation Status
- Domestic Violence Status in accordance with Pen. Code, §§ 13752 subds. (a)-(b) & 13753 subds. (a)-(b) and Pen. Code, §§ 13752 subds. (e) & 13753 subds. (e).
- Veteran Status
- Employment and Educational History and Status
- High Risk Behavior, Violence, or Aggression History

*This list is not exclusive. Members of homeless adult and family multidisciplinary personnel teams (MDTs) may share other information if they believe it is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services, provided that no information may be shared in a manner prohibited by federal law or regulations.

Participating Agencies

Participating Agencies may include any governmental or other agency that has, as one of its purposes, the identification, assessment, and linkage of housing or supportive services to homeless adults or families.

Participating Agencies in Riverside County include:

- Department of Public Social Services (DPSS)
- Child Support Services (CSS)
- First 5
- Housing and Workforce Solutions (HWS)
- Office on Aging (OoA)
- Veterans' Services Office (VSO)
- Riverside University Health System (RUHS)
- Contracted Agencies of any of the above-listed Participating Agencies (Contracted Agencies)
- Governmental agencies working in partnership with any of the above- listed Participating Agencies (Governmental Agencies)
- Non-Governmental agencies working in partnership any of the above listed Participating Agencies (Partner Agencies)

Riverside County Uniform Policies and Procedures
AB 210 Homeless Adult and Family Multidisciplinary Teams

AB 210 authorizes counties to establish homeless adult and family multidisciplinary teams (MDTs) to facilitate the expedited identification, assessment, and linkage of homeless individuals and families to housing and supportive services within the County. It allows provider agencies to share otherwise confidential information in order to coordinate services, ensure continuity of care, and reduce duplication of services. The following policies and procedures are intended to ensure that all agencies participating in AB 210 MDTs comply with the AB 210 statute and protocol.

1.0 Purpose

The purpose of AB 210 is to allow for sharing of confidential information in order to facilitate the expedited identification, assessment, and linkage of homeless individuals and families to housing and supportive services within the County and to allow provider agencies to share confidential information for the purpose of coordinating housing and supportive services to ensure continuity of care.

2.0 Protocol and Participating Agency Agreement

AB 210 requires each county wishing to implement AB 210 to establish a protocol, which governs the information sharing authorized under the law. Agencies wishing to participate in Riverside County AB 210 MDTs must sign a Participating Agency Agreement, and thereby commit to abide by the Riverside County AB 210 Protocol. All Participating Agency staff should review the Protocol carefully.

3.0 Agency Supplemental Policies and Procedures

In addition to these Countywide Policies and Procedures, Participating Agencies may establish their own Supplemental Policies and Procedures, which shall not conflict with the Uniform Policies and Procedures. Participating Agencies must share any Supplemental Policies and Procedures they create with Department Public Social Services – Director or his/her designee.

4.0 Formation of team

- 4.1 AB 210 MDTs are comprised of two or more team members. Teams may exist on an ongoing basis (Ongoing AB 210 MDTs) or be formed in order to serve a particular client or clients (Client-specific MDTs).
- 4.2 Ongoing AB 210 MDTs may consist of personnel who are eligible to participate in AB 210 MDTs who work together on an ongoing basis and need to regularly share information in order to effectively serve their clients. For example, outreach teams may form ongoing AB 210 MDTs.
- 4.3 Ongoing AB 210 MDTs may also be engaged in broader data sharing efforts, such as generating a list of high utilizers of County services in order to prioritize serving

such individuals and/or families, or aggregating data to track progress of County efforts to serve homeless individuals and families.

- 4.4 Client-specific AB 210 MDTs may form when authorized individuals establish contact with one another, verify their eligibility to participate in an MDT, and engage in information sharing. For MDT members who are not familiar with one another, verification of eligibility to participate in an MDT will be established through either an automated data system or by contacting designated point persons at each agency who are able to assess eligibility and facilitate information sharing. Teams are disbanded when information sharing about a client is no longer necessary.

5.0 Information that can be shared under AB 210

- 5.1 The members of AB 210 MDTs may share information that may be designated as confidential under State law, policy, or regulations, if they believe it is generally relevant to the identification, assessment, and linkage of homeless adults and families to housing and supportive services, provided that no information may be shared in a manner prohibited by federal law or regulations.
- 5.2 Homeless is defined as any recorded instance of an adult or family self-identifying as homeless within the most recent 12 months, or any element contained in service utilization records indicating that an adult or family experienced homelessness within the most recent 12 months.
- 5.3 The categories of information to be shared under AB 210 are identified in Attachment A of the Protocol. There may be information that falls outside of the categories that is permissible to share. Moreover, no Participating Agency is required to share any information simply because it falls into one of the categories.
- 5.4 Participating Agencies are expected to make reasonable efforts to share the minimum necessary information. Agencies may decide to share different information depending on the method of information sharing or may determine that different information may be shared by different personnel.
- 5.5 Regardless of the type of information to be shared, personnel participating in an AB 210 MDT are required to ensure to the best of their abilities that information shared is complete, accurate, and up to date.

6.0 Restrictions on information sharing and information uses

- 6.1 AB 210 does not supersede any federally mandated restrictions on information sharing. All personnel participating in MDTs must be familiar with the laws affecting their ability to share information under AB 210 and must comply with the letter and intent of these laws.
- 6.2 Testimony concerning information shared under AB 210 is not admissible in any criminal, civil, or juvenile court proceeding, notwithstanding any other law.

Further, information and writings shared pursuant to this protocol shall be protected from discovery and disclosure by all applicable statutory and common law protections.

- 6.3 Representatives of domestic violence service organizations must obtain clients' consent in order to share confidential information regarding a domestic violence victim or the victim's family.
 - 6.3.1 Domestic violence service organizations must establish a policy delineating how they will obtain clients' consent, how frequently consent will be renewed, how consent will be tracked, and any other pertinent issues necessary to ensure appropriate consent has been secured prior to information sharing under AB 210.
 - 6.3.2 Records of Consent shall be maintained by the client's respective MDT Participating Agency.
- 6.4 Unless there is written authorization from the patient, in accordance with all applicable laws, RUHS Behavioral Health and its contractors shall not provide any information related to Part II substance use disorder treatment programs.
- 6.5 If a law enforcement official contacts an MDT member to request PII and/or PHI about a client who is not in the custody of the law enforcement agency, the MDT member shall direct the official to contact DPSS ASD Liaison, who shall coordinate the request with County Counsel.

7.0 How information can be shared

- 7.1 AB 210 MDTs may share information through "person-to-person" mechanisms, including one-on-one telephone or in-person conversations, electronic communications, and other modes of communication.
- 7.2 AB 210 MDTs may share information through the use of automated systems that facilitate exchange of data and other information.
- 7.3 AB 210 MDTs may share information through the exchange of data files in order to aggregate data to enhance service provision quality and efficiency, and to monitor system outcomes.

8.0 Confidentiality

- 8.1 Ensuring confidentiality of information regarding homeless individuals and families is of critical importance. All Participating Agency personnel will be subject to the same confidentiality requirements as one another. All information shared between AB 210 MDT participants is private and confidential.
- 8.2 All Participating Agency personnel must sign a confidentiality statement prior to participating in AB 210 MDTs.

- 8.3 Participating Agencies must keep all personnel members' signed confidentiality statements on file for the duration of each personnel member's participation in AB 210 MDTs.
- 8.4 If a personnel member changes employer, and the new employer is also a Participating Agency, the personnel members must sign a new confidentiality statement.

9.0 Breaches

- 9.1 The follow definitions apply to this section:
 - 9.1.1 Breach: The term "breach" means the unauthorized acquisition, access, use, or disclosure of PII and/or PHI which compromises the security, privacy or integrity of such information.
 - 9.1.2 Personally Identifiable Information (PII): PII is any information that identifies or describes an individual, including, but not limited to, names Social Security number, date of birth, physical description, home address, telephone number, education, financial matters, medical, or employment history. PII applies to all Multidisciplinary Teams who maintain such information.
 - 9.1.3 Protected Health Information (PHI): PHI is information that relates to the past, present, or future of health, or payment for the health care that is individually identifiable health information, such as a person's name, physical description, medical record number, Social Security number that is transmitted or maintained in any form or medium, including electronic, written, or verbal. (Note that the term PHI is not applicable to all medical information and it applies only to HIPPA-covered entities and their business associates.)
- 9.2 The following procedures apply in the event of a breach or potential breach.
 - 9.2.1 If a Multidisciplinary Team (MDT) member discovers or becomes aware of a Breach or potential Breach of PII or PHI, they must immediately (same business day) report the Breach to their department's respective privacy security liaison.
 - 9.2.2 Following the initial notice of the discovery of a potential Breach, the respective Department's privacy liaison will coordinate efforts with their respective Compliance and Privacy representative and/or Riverside County Chief Compliance and Privacy Officer to investigate and mitigate the Breach.
- 9.3 For further information on Riverside County policies regarding breaches, please see: Riverside County Board Policy B-23 (Health Privacy Policy) and respective Department specific policies.

10.0 Training

- 10.1 All Participating Agency personnel must complete an AB 210 training prior to participating in AB 210 MDTs. AB 210 training must be completed annually for ongoing participation.
- 10.2 Participating Agencies must keep verification of all personnel members' successful completion of an AB 210 training on file for the duration of the personnel member's participation in AB 210 MDTs.
- 10.3 If a personnel member changes employer, and the new employer is also a Participating Agency, training does not need to be repeated if the personnel member completed an AB 210 training while in the position occupied immediately prior to taking a new position. However, the personnel member must obtain verification of successful training completion from the previous employer and the new employer must keep this verification on file.
- 10.4 AB 210 trainings will be presented via webinar and made widely available through County and other learning management systems.

11.0 Information security

- 11.1 Information shared electronically by County Departments under AB 210 is subject to Riverside County Board Policy B-23 – Health Privacy Policy in addition to respective Department specific policies and applicable State and Federal regulations.

12.0 Inquiries about and changes to Policies and Procedures

- 12.1 Any inquiries about these Policies and Procedures should be directed to Department of Public Social Services – Director or his/her designee.
- 12.2 Any changes to these Policies and Procedures will be approved by Department of Public Social Services – Director or his/her designee, in close collaboration with the participating agencies and the Integrated Service Delivery planning team. All Participating Agencies will receive a copy of revised Policies and Procedures upon such approval.