



**UNITED
WAY**

**SMART REFERRAL
NETWORK**

**Smart Referral Network
Memorandum of Understanding**

BACKGROUND

As a United Way Monterey County initiative, the SRN is designed to strengthen community connections, streamline referrals, and provide measurable outcomes to support impactful services.

What the SRN Offers:

- The SRN is an innovative platform that enables “closed loop” bi-directional referrals between agencies, ensuring clients are connected to the services they need. Here's how it works:
- Powerful Search Capabilities: Frontline workers can search the County 211 health and human service database for programs and services tailored to clients’ demographics and eligibility.
- Streamlined Referrals: Users can send and track electronic referrals while receiving timely updates when referrals lead to services.
- Intelligent Matching: Prioritized search results based on client data ensure more effective connections.
- Robust Agency Participation: Over 90 agencies offering more than 160 services are committed to responding to and documenting referrals.

Additional Features:

- Public-Facing Chatbot: A tool for community members to self-refer using non-stigmatizing language, with integrated crisis support features.
- Special Projects Integration: Supports initiatives like emergency rent and utility assistance, CalAIM Whole Person Care, and the Hope and Help mental and behavioral health network.

- Outcome Measurement: Tracks 15 social determinants of health to demonstrate the impact of referrals.

Data Sharing

The SRN is a resource, information and referral hub that connects residents with health and human services; services in the SRN include but are not limited to financial assistance, debt and tax preparation, counseling, housing, food, transportation, employment and job training, and disaster relief. Partners work with their Clients make “closed loop” referrals. Case Managers use the SRN to search for services in the 211 database and/or SRN and generate a prioritized list of complementary services that address the need and would accept the client. Case Managers electronically send referrals and document when referrals lead to services, including the economic mobility and social determinants of health outcomes of those services. Partners have access to client dashboards where they can respond to referrals received, monitor the services their clients receive, keep track of their clients’ outcome improvements, and run reports. This program helps inform any additional services clients might need and allows service providers to work together to ensure Clients have access to the most appropriate services.

In order to generate the list of prioritized services, the SRN matches client demographic information with service eligibility requirements. The SRN collects the following client demographic information: name, date of birth, education, access to health insurance, race, ethnicity, income, address, veteran status, and disability status.

Cyber Security, Access, Permissions, and Infrastructure:

Each Partner receives personalized onboarding, training, and ongoing technical assistance. Partners are assigned user levels, roles and permissions. Access is web based and controlled by login with user names and unique passwords.

Before referrals can be made, clients must sign or indicate referral consent. This form is available in English and Spanish on the SRN and can be signed online, on a hard copy or via text message, and attached to the client profile. Clients can provide verbal approval after a Case Manager reads the forms to their Clients. SRN program and client rights information are included in the Referral Authorization & Consent to Release of Information form. See Attachment B for a copy. Clients have the right to access and verify their personal information, to receive a list of Partners belonging to the SRN, to revoke their referral authorization and consent to release of information at any time.

Partners can see client level demographic information only if they have created a client or received a client’s smart referral. Additional consent is required if a user wants to access a client’s profile and they did not create the client or receive a referral. All referral outcomes including health services will not include Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA). Users who send referrals to health

services cannot see if a referral resulted in a service. Users who send referrals from health service agencies, have the option to obfuscate the “agency from” information in the referral inbox or reports.

United Way Monterey County staff with administrative access credential have access to all partners SRN activity and client level demographic information, referral history, and social determinants of health outcomes.

The SRN is covered with Cybersecurity Insurance protection that includes Security Breach Response Coverage. The policy covers costs to notify individuals affected or reasonably believed to be affected by such “Security Breach”, including printing costs, publishing costs, postage expenses, call center costs or costs of notification via phone or e-mail, including “voluntary notification.”

Client level data is stored on Amazon Web Services Cloud that is infinitely scalable. Data is secured and encrypted at rest and in transit. Data is redundantly stored for disaster recovery. The SRN benefits from Amazon security oversight, regular penetration testing, and 100% approved audits at Federal government level.

See Data Sharing Agreement Attachment A for more details, information, and requirements.

Confidentiality and Privacy

Each party recognizes the importance of the other’s Confidential Information. In particular, each party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither party would enter into this agreement without assurance that such information and the value thereof will be distributed only on a need to know basis and will be protected at least at the same level the organization uses to protect its own confidential information. By signing this agreement, each party agrees to only use personal information for the express purpose of making referrals and providing services and comply with Health Insurance Portability & Accountability Act (HIPAA) Certification. Please refer to Attachment C for HIPAA compliance certification.

PARTNER RESPONSIBILITIES UNDER THIS MOU

- Agree to develop workflow to use SRN.
- Own and maintain its Client data that will be located in Amazon Web Services in the SRN System.
- Respond to its Clients’ personal information requests.
- Identify the case managers and team members to be provided access to the SRN System for collaboration purposes.
- Ensure effective onboarding and Client hand over when case managers and/or team members assigned to the SRN system leave the organization.
- Create and maintain users belonging to agency including deletion of users no longer with the organization or who no longer need access to the software.

- Implement reasonable administrative, physical, and technical safeguards to protect confidential or Protected Health Information (PHI) Client information.
 - Report to United Way any use or disclosure of confidential or Protected Health Information (PHI) which is not in compliance with terms.
 - To mitigate, to the extent practicable, any harmful effect that is known to grantee of a use or disclosure of confidential or Protected Health Information (PHI) by grantee.

Referrals:

- Participate in SRN orientation to learn how to access the SRN software.
- Regularly participate in monthly ARN meetings and quarterly SRN Meetings.
- Commit to making Smart Referrals aligned with their business operations and capacity.
- Follow up on all Smart Referrals to ensure referral leads to a service.
- Respond to referrals received and indicate that they are “received” in their Smart Referral Network inbox.

Services:

- Complete 211 SRN intake form to ensure services are in 211 ICarol database.
- Update service information as needed.
 - 211 will send automatic notifications and links to update once per year

Partners’ Clients:

- Review Client Referral Authorization & Consent to Release of Information document with clients and answer any questions to ensure informed consent.
- Collect and input client consent into the SRN.

UNITED WAY MONTEREY COUNTY RESPONSIBILITIES UNDER THIS MOU

Software

- Facilitate, coordinate, and support access to the SRN platform for partner agency noted on this MOU.
- Train Partners on software use, privacy policies, and outcome evaluation.

Reporting

- Grant Partners access to run reports on:
 - # and type of referrals received and made by individual staff members
 - # and type of referrals that lead to services

- # and % of their Clients that improve in economic mobility and determinants of health (as a result of active referrals or of Partner's services if used as an outcome measurement tool)

TERM AND TERMINATION

Term. The term of this MOU shall commence on the date signed and continue indefinitely. Partners will be required to sign a new MOU if the SRN MOU is updated.

Termination of MOU

Either party may terminate this MOU without stating a cause or reason upon fifteen (15) days prior written notice to the other party.

Consent to the terms of this MOU is indicated by the authorized signatures affixed and dated below.

United Way Monterey County

Partner Organization

Signature:

Organization:

Signature:

Name: Josh Madfis

Name:

Title: VP Community Investments

Title:

Date:

Date:

Attachment A

Data Sharing Memorandum of Understanding

In consideration of the mutual covenants and promises hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties do hereby mutually agree as follows:

Use of Data

Each party recognizes the importance of the other's Confidential Information. In particular, each party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither party would enter into this MOU without assurance that such information and the value thereof will be distributed only on a need to know basis and will be protected at least at the same level the organization uses to protect its own confidential information. Information gleaned from the SRN has to be stored on a password protected computer and hard copies need to be locked up when stored.

By signing this MOU, each party agrees to only use personal information for the express purpose of making referrals and determining the outcomes of referrals.

1. **Obligations of United Way Monterey County (UWMC).** To ensure safe and secure warehousing of data UWMC will implement the following actions:
 - a. **Security Breach Notification.** UWMC shall comply with all applicable laws that require the notification of effected individuals and appropriate authorities in the event of unauthorized release of Personally Identifiable Information (PII) or other event requiring notification. In the event of a breach of any of UWMCs obligations herein related to PII or other event requiring notification under applicable law, UWMC shall:
 - i. Notify Partners and Clients of such event within twenty-four (24) hours of discovery.
 - ii. To the extent UWMC has an independent legal obligation, assume direct responsibility for informing and notifying affected individuals and appropriate authorities in accordance with applicable law;
 - iii. Provide Partners with a copy of any notification(s) to affected individuals and appropriate authorities ("Notification of PII Event").
2. **Authorized User Training.** Partner will, at its own expense, provide to all persons who will be accessing Data ("Authorized Users"), appropriate training regarding, without limitation, proper use of the SRN Platform, Data exchanged and/or, viewed, accessed, or downloaded to the Partners electronic system from the SRN. Partner will maintain users with designated access to the SRN for their agency in the SRN. If Partner has an issue maintaining their own

users they will notify UWMC promptly if any Authorized User's access is terminated, compromised or Data Access Privileges have changed. UWMC may require Partners to demonstrate compliance with these provisions from time to time upon UWMC's written request.

3. **Design and Implementation:** The primary contact for each Party shall be designated below. The primary contact will have the primary authority and serve as the central point of communication for all Partner onboarding tasks and the issuance of Authorized User accounts. In the event a primary contact becomes unavailable or unresponsive, the primary contact shall be replaced by another individual with the same or better qualifications and availability within ten (10) days of receipt of a reasonable written request.
4. **Onboarding:** The parties shall meet and mutually agree to an onboarding and implementation schedule within thirty (30) days of execution of this MOU, or other agreed upon date. The following persons shall have primary responsibility and shall serve as the central point of contact for each of the parties. Each of the parties shall promptly notify the other in writing (e.g. email) of any substitutes to the persons named below.

<u>Grantee</u>	<u>Name</u>	<u>Contact Information</u>
UWMC Onboarding Mgr.	Josh Madfis	Josh.madfis@unitedwaymcca.org
Authorized User Administrator	Josh Madfis	Josh.madfis@unitedwaymcca.org
Partner Onboarding Mgr.		
Authorized User Administrator		

Data To Be Uploaded to the Smart Referral Network: The value of Data depends on its completeness, accuracy, and timeliness. Partner and UWMC will ensure that the Data shared in the SRN is accurate and complete. Partner or UWMC or both (as indicated in the Attachment A Addendum) will provide access to and/or transmit the Data indicated on the Attachment A Addendum hereto, and provide updated Data as and when new information is available. Neither Party will withhold Data unless; (i) the individual who is the subject of the Data has not consented (or authorized) Partner or UWMC to share Data, or (ii) sharing the Data with the Partner or UWMC would violate the individual's written authorization or the revocation of an authorization to share or, (iii) if disclosing the particular Data would violate Applicable Privacy Laws or the MOU.

Attachment A - Addendum

Data to be Uploaded to the Smart Referral Software

DATA ACCESS: Partner shall be granted the following Data Access privileges:

[X BE] View, Download and Enter Data in the SRN: View, Download and Enter Data, permits the Partner to retrieve Data from and enter Data into the SRN Platform

DATA ELEMENTS: [X BE] Partner, [] UWMC shall transmit or exchange the following Data Elements about its Clients (if available):

*Indicates required fields to prevent duplicate records	
Identifiers	Name: First, Last, * Cell Phone* Email Birthdate*
Demographics	Residential Address City Zip Code Ethnicity Culture Group Race Gender Non-Binary/Gender non-conforming LGBTQ2S+ Primary Language Income
Family	Child's Name: First, Last
Youth	Child's Name: First, Last Foster Care Status System Impacted Youth (Juvenile/Legal)
Health Insurance	Medi-Cal Medi-Cal ID: Private
Education	Highest Level
Disability	Status:
Veteran	Status:

Attachment B

UNITED WAY SMART REFERRAL NETWORK (SRN) **Referral Authorization & Consent to Release of Information** *(Covering Monterey, Kings, Tulare Counties, and future participating counties)*

The purpose of this Referral Authorization & Consent to Release of Information is to obtain your permission to refer you to partner organizations who are members of the United Way Smart Referral Network (SRN) and to obtain your consent to the release of certain personal information to partner organizations to which you are referred. The SRN covers Monterey, Kings, and Tulare Counties. Your privacy is important to us. The collection, storage, and sharing of your personal data complies with all applicable federal and California privacy laws, including HIPAA, CCPA, and other relevant statutes.

Partner organizations to whom you are referred may forward your referral only to another SRN-approved agency that provides services relevant to your needs. Any such forwarding is subject to the same confidentiality and privacy protections. You have the right to be notified before your personal information is forwarded to an agency outside of the SRN.

Your information may include your name, age, gender, ethnicity, race, income category, city or county of residence, access to healthcare, language, disability, veteran status, education, contact information, services you have received, progress made in your economic mobility, protected health information (PHI), mental health information, substance use disorder information (if consented), school-based services, Medi-Cal eligibility, housing status, and limited criminal justice information. Sensitive data will only be shared if necessary to determine eligibility for specific services.

Your information will be shared solely with SRN partner organizations to help determine and provide your eligible services. You may expect to be contacted by one or more SRN organizations to receive services tailored to your needs. Some partners may report anonymized data to their funders; no personally identifiable information will be disclosed without your explicit written consent. All SRN member organizations must protect your information using industry-standard security measures, including encryption and secure data transmission protocols.

In the event of a data breach affecting your personal information, you will be notified in accordance with California law. The responsible party must provide a detailed report and corrective actions.

Your Rights:

- You may request a list of SRN member organizations.
- You have the right to limit or revoke your consent at any time by contacting your county representative (see contacts below).
- Revocation requests will be processed within 10 business days. Upon revocation, your data will be removed from the SRN system unless retention is legally required.

- You may request to verify or correct your personal information.

Revoking Consent (Contact Information):

- Monterey County: Jessica Sousa
Jessica.Sousa@unitedwaymcca.org | (831) 318-1998
- Kings County: Daray Jones
darayj@kingsunitedway.org | (559) 584-1536
- Tulare County: Fedieson Landicho
fedieson@unitedwaytc.org | (Phone # coming soon)

This consent is valid for 12 months from the date signed. Prior to expiration, you will have the option to renew or revoke your consent. Unless renewed in writing, your personal data will be permanently deleted unless required by law to be retained.

By signing below, I authorize referrals to SRN member organizations and consent to releasing my personal information to such organizations so I can access services to meet my specific needs.

Referring Agency:

Client Name (Printed):

Date:

Client Signature:

RED DE DERIVACIÓN INTELIGENTE DE UNITED WAY (SRN)
Autorización de Referencia y Consentimiento para la Divulgación de Información
(Cubre los condados de Monterey, Kings, Tulare y futuros condados participantes)

El propósito de esta Autorización de Referencia y Consentimiento para la Divulgación de Información es obtener su permiso para referirlo a organizaciones asociadas que son miembros de la Red de Referencia Inteligente (SRN) de United Way y obtener su consentimiento para divulgar cierta información personal a las organizaciones a las que se le refiere. La SRN cubre los condados de Monterey, Kings y Tulare. Su privacidad es importante para nosotros. La recopilación, almacenamiento y divulgación de su información personal cumple con todas las leyes federales y de California sobre privacidad, incluidas HIPAA, CCPA y otras leyes relevantes.

Las organizaciones asociadas a las que se le refiere solo podrán reenviar su referencia a otra agencia aprobada por SRN que ofrezca servicios relevantes para sus necesidades. Cualquier reenvío estará sujeto a las mismas protecciones de confidencialidad y privacidad. Usted tiene derecho a ser notificado antes de que su información personal sea enviada a una agencia fuera de la SRN.

Su información puede incluir su nombre, edad, género, nacionalidad, ~~raza~~, categoría de ingresos, ciudad o condado de residencia, acceso a atención médica, idioma, discapacidad, estado de veterano, educación, información de contacto, servicios que ha recibido, progreso financiero, información de salud protegida (PHI), información de salud mental, información sobre trastornos por uso de sustancias (si da su consentimiento), servicios escolares, elegibilidad de Medi-Cal, estado de vivienda e información limitada del sistema de justicia penal. Los datos sensibles solo se compartirán si es necesario para determinar su elegibilidad para servicios específicos.

Su información se compartirá únicamente con organizaciones asociadas de SRN para ayudar a determinar y proporcionar los servicios a los que es elegible. Puede esperar ser contactado por una o más organizaciones de SRN para recibir servicios adaptados a sus necesidades. Algunas organizaciones pueden informar datos anónimos a sus financiadores; no se divulgará ninguna información personal identificable sin su consentimiento escrito explícito. Todas las organizaciones miembros de SRN deben proteger su información utilizando medidas de seguridad estándar de la industria, incluido el cifrado y protocolos seguros de transmisión de datos.

En caso de una violación de datos que afecte su información personal, se le notificará de acuerdo con la ley de California. La parte responsable debe proporcionar un informe detallado y acciones correctivas.

Sus Derechos:

- Puede solicitar una lista de las organizaciones miembros de SRN.
- Tiene derecho a limitar o revocar su consentimiento en cualquier momento contactando a su representante del condado (ver contactos abajo).
- Las solicitudes de revocación se procesarán en un plazo de 10 días hábiles. Al revocar, sus datos serán eliminados del sistema SRN a menos que la ley exija su retención.
- Puede solicitar verificación o corregir su información personal.

Revocar Consentimiento (Información de Contacto):

- Condado de Monterey: Jessica Sousa
Jessica.Sousa@unitedwaymcca.org | (831) 318-1998
- Condado de Kings: Daray Jones
darayj@kingsunitedway.org | (559) 584-1536
- Condado de Tulare: Fedieson Landicho
fedieson@unitedwaytc.org | (Número de teléfono próximamente)

Este consentimiento es válido por 12 meses a partir de la fecha de firma. Antes de que expire, tendrá la opción de renovar o revocar su consentimiento. A menos que se renueve por escrito, sus datos personales se eliminarán permanentemente a menos que la ley requiera su conservación.

Al firmar a continuación, autorizo referencias a organizaciones miembros de SRN y doy mi consentimiento para divulgar mi información personal a dichas organizaciones para poder acceder a los servicios que satisfagan mis necesidades.

Agencia de referencia: _____

Nombre del cliente (escrito): _____

Fecha: _____

Firma del cliente: _____

Attachment C

Health Insurance Portability & Accountability Act (HIPAA) Certification

A. Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as “the Administrative Simplification provisions,” direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information, and pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services has issued regulations modifying 45 CFR Parts 160 and 164 (“HIPAA Privacy Rule”).

B. Partner and United Way Monterey County have entered into an Agreement (“Agreement”) to which this Certification is an attachment whereby Grantee will provide certain services to United Way Monterey County, pursuant to which Grantee may have access

to Protected Health Information (as defined below) in fulfilling its responsibilities under the Agreement.

C. In consideration of the Parties' continuing obligations under the Agreement, compliance with the HIPAA Privacy Rule, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Partner agrees to the provisions of this Certification and of the HIPAA Privacy Rule and to protect the interests of United Way.

I. DEFINITIONS

Except as otherwise defined herein, any and all capitalized terms in this Section shall have the definitions set forth in the HIPAA Privacy Rule. In the event of an inconsistency between the provisions of this Certification and mandatory provisions of the HIPAA Privacy Rule, as amended, the HIPAA Privacy Rule shall control. Where provisions of this Certification are different than those mandated in the HIPAA Privacy Rule, but are nonetheless permitted by the HIPAA Privacy Rule, the provisions of this Certification shall control.

The term "Protected Health Information" means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Partner acknowledges and agrees that all Protected Health Information that is created or received by United Way Monterey County and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by United Way Monterey County, or its operating units, to Partner or is created or received by grantee on United Way Monterey County's behalf shall be subject to this Certification.

II. CONFIDENTIALITY REQUIREMENTS

(a) Partner agrees:

(i) to use or disclose any Protected Health Information solely: (1) for meeting its obligations as set forth in any agreements between the Parties evidencing their business relationship or (2) as required by applicable law, rule or regulation, or by accrediting or credentialing organization to whom United Way Monterey County is required to disclose such information, or as otherwise permitted under this Certification, or the underlying Agreement, (if consistent with this Certification and the HIPAA Privacy Rule), or the HIPAA Privacy Rule, and (3) as would be permitted by the HIPAA Privacy Rule if such use or disclosure were made by United Way Monterey County; and

(ii) at termination of the Agreement, (or any similar documentation of the business relationship of the Parties), or upon request of United Way, whichever occurs first, if feasible grantee will return or destroy all Protected Health Information received from or created or received by Partner on behalf of United Way Monterey County that grantee still maintains in any form, and retain no copies of such information, or if such return or destruction is not feasible, grantee will extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible; and

(iii) to ensure that its agents, including a subcontractor(s), to whom it provides Protected Health Information received from or created by grantee on behalf of United Way Monterey County, agrees to the same restrictions and conditions that apply to grantee with respect to such information. In addition, grantee agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause grantee to breach the terms of the Agreement.

(b) Notwithstanding the prohibitions set forth in this Certification or the Agreement, grantee may use and disclose Protected Health Information as follows:

(i) if necessary, for the proper management and administration of grantee or to carry out the legal responsibilities of grantee, provided that as to any such disclosure, the following requirements are met:

(A) the disclosure is required by law; or

(B) Partner obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law, or for the purpose for which it was disclosed to the person, and the person notifies grantee of any instances of which it is aware in which the confidentiality of the information has been breached;

(ii) for data aggregation services, if to be provided by grantee for the health care operations of United Way pursuant to any agreements between the Parties evidencing their business relationship. For purposes of this Certification and the Agreement, data aggregation services means the combining of Protected Health Information by Partner with the protected health information received by grantee in its capacity as grantee of another United Way Monterey County, to permit data analyses that relate to the health care operations of the respective covered entities.

(c) Partner will implement appropriate administrative, physical, and technical safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Certification. The Secretary of Health and Human Services shall have the right to audit grantee's records and practices related to use and disclosure of Protected Health Information to ensure United Way Monterey County's compliance with the terms of the HIPAA Privacy Rule. Partner shall report to United Way any use or disclosure of Protected Health Information which

is not in compliance with the terms of this Certification of which it becomes aware. In addition, Partner agrees to mitigate, to the extent practicable, any harmful effect that is known to grantee of a use or disclosure of Protected Health Information by grantee in violation of the requirements of this Certification or the Agreement.

III. AVAILABILITY OF PHI

Partner agrees to make available Protected Health Information to the extent and in the manner required by Section 164.524 of the HIPAA Privacy Rule. Partner agrees to make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information in accordance with the requirements of Section 164.526 of the HIPAA Privacy Rule. In addition, Partner agrees to make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Privacy Rule.

IV. TERMINATION

Notwithstanding anything in this Certification or the Agreement to the contrary, United Way shall have the right to terminate the Agreement immediately if United Way Monterey County determines that grantee has violated any material term of this Certification and/or the Agreement. If United Way Monterey County reasonably believes that grantee will violate a material term of this Certification and/or the Agreement and, where practicable, United Way Monterey County gives written notice to grantee of such belief within a reasonable time after forming such belief, and grantee fails to provide adequate written assurances to United Way Monterey County that it will not breach the cited term of this Certification and/or the Agreement within a reasonable period of time given the specific circumstances, but in any event, before the threatened breach is to occur, then United Way Monterey County shall have the right to terminate the Agreement immediately.

V. MISCELLANEOUS

Except as expressly stated herein or the HIPAA Privacy Rule, the parties to the Agreement do not intend to create any rights in any third parties. The obligations of grantee under this Section shall survive the expiration, termination, or cancellation of this Certification and/or the Agreement, and/or the business relationship of the parties, and shall continue to bind grantee, its agents, employees, contractors, successors, and assigns as set forth herein.

The parties agree that, in the event that any documentation of the arrangement pursuant to which Partner provides services to United Way Monterey County contains provisions relating to the use or disclosure of Protected Health Information which are more restrictive than the provisions of this Certification or the Agreement, the provisions of the more restrictive documentation will control. The provisions of this Certification and the Agreement are

intended to establish the minimum requirements regarding grantee use and disclosure of Protected Health Information.

In the event that either party believes in good faith that any provision of this Certification and/or the Agreement fails to comply with the then current requirements of the HIPAA Privacy Rule, such party shall notify the other party in writing. For a period of up to thirty (30) days, the parties shall address in good faith such concern and amend the terms of this Certification and/or the Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Certification and/or the Agreement fails to comply with the HIPAA Privacy Rule, then either party has the right to terminate upon written notice to the other party.

Partner:

By:

Title:

Date:

Attachment D

Smart Referral Network Compliance with FERPA

This attachment provides an overview of how the Smart Referral Network (SRN) complies with the Family Educational Rights and Privacy Act (FERPA), ensuring student education records and related information are handled lawfully, securely, and with respect for student and family rights.

1. Consent and Authorization

FERPA requires written consent from parents (or eligible students) before disclosing personally identifiable education records. The SRN aligns with this by requiring signed or indicated referral consent before referrals are made. Clients (or their guardians, when applicable) must complete the Referral Authorization & Consent to Release of Information form, which specifies what data may be shared, with whom, and for what purpose.

2. Limited Scope of Data Use

FERPA restricts use of education records to authorized educational purposes. The SRN ensures that personal information is used only for the express purpose of making referrals and providing services. Partner agencies agree to use client information solely for these purposes and not for unrelated activities.

Additionally:

- Partners can only see client-level data if they created the client profile or received a referral.
- Additional consent is required to access a profile if neither condition applies.
- Sensitive data (such as education, disability, or school-based services) is only shared if necessary for service eligibility.

This 'need-to-know' principle parallels FERPA's requirement that access to records be limited to legitimate educational interests.

3. Student and Family Rights

FERPA guarantees students and parents the right to review, correct, and revoke consent regarding education records. The SRN incorporates these rights by allowing clients to:

- Access and verify their personal information.
- Request a list of partner organizations that may access their data.
- Revoke consent at any time, which results in removal of their data from the SRN unless legally required to retain it.

This mirrors FERPA's protections for inspection, amendment, and control over disclosure.

4. Data Security and Confidentiality

FERPA requires reasonable methods to safeguard education records from unauthorized disclosure. The SRN enforces this through:

- Role-based access, unique logins, and permissions.
- Encryption of data at rest and in transit, securely stored on Amazon Web Services.
- Administrative, technical, and physical safeguards maintained by United Way and partner agencies.
- Cybersecurity insurance and breach response protocols.

These protections align with FERPA's mandate for secure handling of education records.

5. Alignment with Other Privacy Laws

While FERPA is specific to education records, the SRN's framework also addresses HIPAA and California privacy laws (CCPA), ensuring compliance across education, healthcare, and social service contexts. This layered compliance reinforces FERPA standards by applying the strictest privacy protections across domains.

Conclusion

The Smart Referral Network complies with FERPA by requiring explicit consent, restricting access on a need-to-know basis, upholding student and family rights to review and revoke consent, securing data with robust technical measures, and embedding these commitments into its legal agreements with partner agencies.