United Way Monterey County CalAim
Privacy and Security Program

I. PERSONNEL CONTROLS

A. Security Officer Designation: United Way Monterey County (UWMC) has designated Josh Madfis at the Security Office he will oversee all Personnel Controls. He oversees Smart Referral Network (SRN) Personal Health Information (PHI) and Personally Identifiable Information (PII) data security.

Responsibilities and Duties:

Annual Employee Training: Trains on SRN information privacy and security to all workforce members who:

- Assist in the performance of Smart Referral Network functions or activities
- Access or disclose CCAH PHI or PII

Staff Management and Supervision: Provides management support to all UWMC workforce members who assist in the performance of Smart Referral Network functions or activities or workforce members who access or disclose PHI or PII. This includes ensuring these work-force members receive background checks, criminal history record checks, and that they sign confidentiality statements, and comply with a security and privacy safeguards.

II. TECHNICAL SECURITY CONTROLS

The following security and privacy safeguards are in place. All UWMC staff work in a password protected virtual office. The virtual office enforces appropriate encryption on local workstations. Within the virtual office environment, all systems employ data encryption in transit. Enterprise level anti-virus software is on all virtual office managed workstations and hosts within the virtual office hosted environment. All are updated daily. When in the virtual environment, UWMC work-stations benefit from critical security patches. Patching for virtual office managed workstations is configured to push daily. Patching for hosts within the virtual office hosted environment are applied weekly.

In addition, the Smart Referral Network software has encrypted S3 buckets in transit and at rest, and developed an API interface to unencrypt S3 data on access.

The following technical security controls have been developed:

Auto-logout users after 20 minutes of inactivity

Multi Factor Authentication to log credentials

- Confirm identity via email code

Password restrictions for new users

- Block commonly used blacklist passwords
- 1 Upper case, 1 Lower case, 1 special character,
- Minimum length of 8 characters,
- Prevent password from being the same as username

- MediCal ID Access Restrictions: All Referrals and social determinants of health (SDOH) Reports made for clients referred to health services are restricted. Only users with granted access will be able to see protected information. The protected information, access controls, and historical data are outlined below:

  Any information regarding the source of the referral. This includes:
  - Program Name
  - Agency From
  - Referring User Contact Info

  Any information regarding the outcome of the referral. This includes:
  - Enrolled / Accepted / Declined

Client outcomes that show developments on the range of social determinants of health domains: Employment, Education, Training, Job Retention, Income, Budgeting and Saving, Access to Financial Services, Debt Management, Credit, Housing, Child Care and Food Security

UWMC Admin level users may grant "Protected Access" to Smart Referral Network users that can view protected information.

- For users without access:
  - Protected referral information will be presented as "PROTECTED" in Referral Inbox and Referral Summary Report
  - Protected Referrals will only be visible in Incoming inbox. Protected Referrals will not be visible once moved to Enrolled / Accepted / Declined inboxes.
  - Protected Client Reports will not appear in Client Summary Report or SDOH Report Summary Export.
- For users with access:
  - All referral information will be presented in Referral Inbox and Referral Summary Report
  - Referral will be visible in Enrolled / Accepted / Declined inboxes
  - Protected Client Reports will appear in Client Summary Report and SDOH Report Summary Export.

Historical Data:

- All Referrals for a client to services that are not related to health services will not be protected.
- All SDOH Reports for a client that has not been referred to health services will not be protected. Only SDOH Reports made after having a referral to a health serivce will be protected.

The following Warning Banner now appears upon logging on the SRN. Users cannot access the SRN without agreeing:

> Smart Referral user recognizes the importance of the client and partners’ confidential information. In particular, Smart Referral users agree that the confidential information of clients and other referral partner organizations is critical to client privacy and partners respective businesses. By clicking the box below, the Smart Referral user agrees that such information and the value thereof will be accessed and utilized only on a need to know basis and will be protected at least at the same level the organization uses to project its own confidential information.

In addition, the Smart Referral user agrees to only use personal information for the express purpose of making referrals and determining the outcomes of referrals.

The Smart Referral user also agrees to not include any clients' protected health information including case notes when making referrals.
All access to Smart Referral Network reports and client personally identifiable information is logged.

Please exist the Smart Referrals Network, if you do not agree with the terms of the Confidentiality and Privacy Agreement
Check here to indicate that you have read and agree to the terms of the Confidentiality and Privacy Agreement

All UWMC Smart Referral Network users with access to PHI and PII have agreed:

- To only login and access the Smart Referral Network only in the virtual office.
- To train, monitor and oversee partner users on security and privacy safeguards with access to Covered Entity PHI or PII.
- Download Medi-Cal client information (Covered Entity PHI or PII) only inside the UPIC virtual office.
- Not to download or store any PHI or PII on removable devices.
- Not to share username and password information.
- Not to share Medi-Cal client information (Covered Entity PHI or PII) with partners who do not have access level privileges. Data must be encrypted or password protected before being emailed.

III. AUDIT CONTROLS

A. **System Security Review*.*** UWMC will conduct an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews will include vulnerability scanning tools.

B. **Log Reviews*.*** UWMC has enabled CloudTrail on the Amazon Web Services database to store logs of Smart Referral reports run and downloaded for view at any time.

C. **Change Control*.*** UWMC has a system processing and/or storing PHI or PII and a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. **Emergency Mode Operation Plan** UWMC has established a documented plan to enable continuation of critical business processes and protection of the security of electronic PHI or PII in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours*.*

B. **Data Backup Plan*.*** UWMC has established procedures to backup PHI to maintain retrievable exact copies of PHI or PII. The plan includes a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore PHI or PII should it be lost. At a minimum, the schedule is a weekly full backup and monthly offsite storage of data.

V. PAPER DOCUMENT CONTROLS

A. Supervision of Data. PHI or PII in paper form will not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. PHI or PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. Escorting Visitors. Visitors to areas where PHI or PII is contained shall be escorted and CCAH PHI or PII shall be kept out of sight while visitors are in the area.

C. Confidential Destruction. PHI or PII will be disposed of through confidential means, such as crosscut shredding and pulverizing.

D. Removal of Data. PHI or PII will not be removed from the premises of Business Associate except with express written permission of Covered Entity.

E. Faxing. Faxes containing PHI or PII will not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. Mailing. Mailings of PHI or PII shall be sealed and secured from damage or inappropriate viewing of PHI or PII to the extent possible. Mailings which include 500 or more individually identifiable records of Covered Entity PHI or PII in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of Covered Entity to use another method is obtained.