Appendix F – Confidentiality and Privacy of Participant Information

1. In addition to the terms included in Section 12.1 of the Agreement, **Proprietary or Confidential Information of City**, Grantee agrees to further take the following steps to protect the confidentiality and privacy of information it obtains in the course of providing services under this Agreement:

   1.1. **Safeguards for Participant Information**. In the course of providing services to members of the public as set forth in this Agreement, Grantee may at times have access to and may collect or retain various kinds of information about people who are participating in and/or receiving services provided by Grantee based on funds received pursuant to this Agreement. Such information includes any information about a person that allows Grantee or would allow anyone else to identify that person by name or other personal characteristics, and it includes but is not limited to the following information about each program participant: name and any aliases; contact information; demographic information; physical description information; photo, video, or audio recordings of the person; medical information; employment information; financial information; and/or any information about services or benefits that person receives from any City, state, or other governmental department or program. To the extent that Grantee keeps any such information associated with people who participate in and/or receive services funded by this Agreement, Grantee must take appropriate steps to protect the confidentiality of such information and to safeguard such information from unauthorized access, use, or disclosure. Such protections must include but are not limited to administrative, physical, and technical safeguards.

   1.2. **Assessment of Use of Participant Information**. Grantee agrees to assess how it maintains and uses the program participant information described in Subsection 1.1 above. This assessment should include consideration of all of the following:

      1.2.1. How such information is protected;

      1.2.2. How use of such information is limited to appropriate purposes;

      1.2.3. How such information is stored, including how computer systems are encrypted, how cloud storage or other online services are used, and whether it is stored in data center locations outside the United States of America;

      1.2.4. How Grantee's employees, agents, or subcontractors are allowed to use and share such information;

      1.2.5. What rules apply to the distribution, sharing, or use of such information outside the services provided under this Agreement;

      1.2.6. How Grantee will ensure compliance with any applicable federal, state, and local laws and regulations relating to services funded by this Agreement and participant information kept by Grantee; and

      1.2.7. How a participant is allowed to access information held by Grantee about that participant.

   1.3. **Notification to City of Loss or Unauthorized Access to Participant Information; Security Breach Notification**. Grantee must comply with all applicable laws that require the notification to individuals in the event of unauthorized release of participant information or other event requiring notification. Regardless of all other such laws and obligations, Grantee

must notify City of any actual, suspected, or potential exposure or misappropriation of participant information (any "Leak") within seventy-two (72) hours of the discovery of such. Grantee, at its own expense, will reasonably cooperate with law enforcement authorities to investigate any such Leak and to notify injured or potentially injured parties. The obligation to notify the City expressly includes any suspected or potential Leak and not just a confirmed Leak. City retains the sole right to conduct media communications related to such Leak on its own behalf, and Grantee may not communicate with the media on behalf of the City in relation to such Leak. Grantee is also required to use all reasonable efforts to coordinate its response to such Leak with City.

Notifications to City must be made via email to:

San Francisco Human Services Agency Privacy Office: HSAPrivacyOffice@sfgov.org

Information Security Office: HSA.IT.Information.Security@sfgov.org