

**SAN FRANCISCO DEPARTMENT OF PUBLIC HEALTH
REVISION TO PROGRAM BUDGETS (RPB #1)**

The Department of Public Health, hereby requests a revision to contract number 1000028223, to update Attachment 2 of Appendix B, Appendix D, Appendix E, and add Attachment 2.1a of Appendix B FY24/25 in support of San Mateo County - Ryan White HIV/AIDS Treatment /Extension Act of 2009 Agreement. This revision will be funded using a portion of the pre-approved budget outlined in Attachment 2 of Appendix B Grant Budget Summary.

WHEREAS, the City and County of San Francisco (CCSF), through its Department of Public Health, entered into an Agreement with **San Mateo County** for the period March 1, 2023 through February 29, 2028 (CID#1000028223) hereinafter referred to as the “Original Agreement”; and

WHEREAS, This Revision to the Original Agreement has been entered into this 1st day of March, 2024; and

WHEREAS, The Department of Public Health and **San Mateo County** desire to amend the Original Agreement; and

WHEREAS, This Revision to the Original Agreement will become effective upon certification by the Controller of the availability of funds;

NOW THEREFORE, The parties to the Original Agreement do hereby agree to amend the Original Agreement. Except for these changes, the Original Agreement remains in full force and effect.

Delete Attachment 2 of Appendix B, and replace in its entirety with Attachment 2 of Appendix B, to Agreement as revised. Dated 03/01/2024.

Add Attachment 2.1a, to Agreement as revised. Dated 03/01/2024.

Delete Appendix D, and replace in its entirety with Appendix D SFDPH SAA 11-20-2023, to Agreement as revised. Dated 03/01/2024.

Delete Appendix E and replace in its entirety with Appendix E Dated: OCPA & CAT v1/10/2024, Attestation forms 06-07-2017, and Protected Information Destruction Order Purge Certification 01-10-2024, to Agreement as revised. Dated 03/01/2024.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the day first mentioned above.

CITY:

CONTRACTOR:



SMC Resolution No. 080842

Bill Blum
Contract Administrator
Department of Public Health

Board of Supervisors

San Mateo County

Contractor

225 37th Avenue Pony HI, T324

Address

San Mateo, CA 94403

City, State, Zip

**ATTACHMENT 2 of Appendix B
Grant Budget Summary**

1. Estimated Funding Allocations by Funding Source

| Grant Plan | Grant Plan Term | Funding Source | Estimated Funding Allocation | |
|--|--------------------------|-----------------------|-------------------------------------|--------------|
| Attachment 2.1 STD/HIV Program | 03/01/23-02/29/24 | Federal RWPA | \$1,442,325 | Original |
| Attachment 2.1a STD/HIV Program | 03/01/24-02/28/25 | Federal RWPA | \$1,485,487 | RPB#1 |
| Attachment 2.1b STD/HIV Program | 03/01/25-02/28/26 | Federal RWPA | \$1,550,000* | Original |
| Attachment 2.1c STD/HIV Program | 03/01/26-02/28/27 | Federal RWPA | \$1,550,000* | Original |
| Attachment 2.1d STD/HIV Program | 03/01/27-02/29/28 | Federal RWPA | \$1,550,000* | Original |
| Subtotal Award | | | \$7,577,812 | |
| <i>Grant TBD</i> | | | \$64,513 | |
| Contingency | | | \$917,079 | |
| Total NTE | | | \$8,559,404 | |
| *Actual HRSA award amount will be added by a Revision to Program Budget (RPB). | | | | |

2. Method of Payment

A. Compensation for all SERVICES provided by Grantee shall be paid in the following manner

(1) Direct Payment will be issued to Grantee after approval of each Funding Request by the Director of Health or designee, acting in his or her sole discretion.

(2) Grantee shall submit a Grant Budget in the format attached (*Attachment 2.1 Grant Budget Details*).

(3) Grantee shall submit a Funding Request in the format attached (*Appendix C – Form of Funding Request*).

3. Contingency Amount

A. Grantee understands that, of the maximum dollar obligation listed in Section 5.1 of this Agreement, **\$917,079** is included as a contingency amount and is neither to be used in Program Budgets attached to this Appendix, or available to Contractor without a modification to this Agreement executed in the same manner as this Agreement or a revision to the Grant Budgets of Appendix B, which has been approved by Contract Administrator. Contractor further understands that no payment of any portion of this contingency amount will be made unless and until such modification or budget revision has been fully approved and executed in accordance with applicable City and Department of Public Health laws, regulations and policies/procedures and certification as to the availability of funds by Controller. Contractor agrees to fully comply with these laws, regulations, and policies/procedures.

4. Revisions to the Grant Budget

A. Grantee agrees to comply with its Grant Budgets of Appendix B. Changes to the Grant Budget that do not increase or reduce the Maximum Amount of Grant Funds listed in Section 5.1 of the Agreement are subject to the provisions of the Department of Public Health Policy/Procedure Regarding Contract Budget Changes. Grantee agrees to comply fully with that policy/procedure.

B. Grantee understands that the CITY may need to adjust funding sources and funding allocations and agrees that these needed adjustments will be executed in accordance with Section 19.1 of this Agreement. In event that such funding source or funding allocation is terminated or

reduced, this Agreement shall be terminated or proportionately reduced accordingly. In no event will Grantee be entitled to compensation in excess of these amounts for these periods without there first being a modification as provided for in Section 17.2 of the Agreement or a revision to Grant Budget, as provided for in Section 19.1 section of this Agreement.

C. The amount for each fiscal year, to be used in Grant Budget and available to Grantee for that fiscal year shall conform with the Grant Plan, Grant Budget and Cost Reporting Data Collection form, as approved by the City's Department of Public Health based on the City's allocation of funding for services for that fiscal year.

**Attachment 2.1a of Appendix B
Grant Budget Detail
Federal RWPA Pass-Through Grant Funding**

San Mateo County STD/HIV Program
March 1, 2024 through February 28, 2025

| SERVICE CATEGORY | DIRECT EXP. | IND.COSTS | TOTAL | IND.RATE |
|--|------------------|-----------|------------------|---------------|
| Category I | | | | |
| I. Outpatient/Ambulatory Health Services | 23,794 | 0 | 23,794 | 0.00 |
| II. Oral Health Care | 75,000 | 0 | 75,000 | 0.00 |
| III. Early Intervention Services | 152,770 | 0 | 152,770 | 0.00 |
| IV. Mental Health Services | 125,792 | 0 | 125,792 | 0.00 |
| V. Medical Case Management | 575,631 | 0 | 575,631 | 0.00 |
| Sub-total Category I 75% | | | 952,987 | 64% |
| Category II | | | | |
| VI. Emergency Financial Assistance | 112,500 | 0 | 112,500 | 0.00 |
| VII. Food Bank/Home Delivered Meals | 400,000 | 0 | 400,000 | 0.00 |
| VIII. Housing Services | 20,000 | 0 | 20,000 | 0.00 |
| Sub-total Category II 25% | | | 532,500 | 36% |
| TOTAL RYAN WHITE PART A | 1,485,487 | 0 | 1,485,487 | 0.0000 |

I. SERVICE CATEGORY = OUTPATIENT AMBULATORY
UOS = 650, UDC = 75

| | |
|---------------------------|---------------|
| Personnel | 23,794 |
| Operating Expenses | 0 |
| Contracts | 0 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Primary Care | 23,794 |

II. SERVICE CATEGORY - ORAL HEALTH CARE
UOS = 950, UDC = 40

| | |
|------------------------------|---------------|
| Personnel | 0 |
| Operating Expenses | 0 |
| Contracts | 75,000 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Dental Services | 75,000 |

III. EARLY INTERVENTION SERVICES
UOS = 120, UDC = 20

| | |
|--|----------------|
| Personnel | 152,770 |
| Operating Expenses | 0 |
| Contracts | 0 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Early Intervention Services | 152,770 |

Attachment 2.1a of Appendix B
Grant Budget Detail
Federal RWPA Pass-Through Grant Funding

IV. SERVICE CATEGORY - MENTAL HEALTH

UOS = 1,500, UDC = 65

| | |
|--------------------------------|----------------|
| Personnel | 125,792 |
| Operating Expenses | 0 |
| Contracts | 0 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total for Mental Health | 125,792 |

V. SERVICES CATEGORY - MEDICAL CASE MANAGEMENT

UOS = 13,000; UDC = 470

| | |
|------------------------------|----------------|
| Personnel | 575,631 |
| Operating Expenses | 0 |
| Contracts | 0 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Case Management | 575,631 |

VI. SERVICE CATEGORY - EMERGENCY FINANCIAL ASSISTANCE

UOS = 120, UDC = 75

| | |
|--|----------------|
| Personnel | 0 |
| Operating Expenses | 0 |
| Contracts | 112,500 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Direct Emergency Assistance | 112,500 |

VII. SERVICE CATEGORY - FOOD BANK/HOME DELIVERED MEALS

UOS = 10,000, UDC = 80

| | |
|----------------------------|----------------|
| Personnel | 0 |
| Operating Expenses | 0 |
| Contracts | 400,000 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Food Services | 400,000 |

VIII. SERVICE CATEGORY - HOUSING SERVICES

UOS = 375, UDC = 20

| | |
|-------------------------------------|---------------|
| Personnel | 0 |
| Operating Expenses | 0 |
| Contracts | 20,000 |
| Fixed Assets | 0 |
| Indirect Costs | 0 |
| Total Residential Assistance | 20,000 |

Appendix D

**SAN FRANCISCO DEPARTMENT OF PUBLIC HEALTH
THIRD PARTY COMPUTER SYSTEM ACCESS AGREEMENT
(SAA)**

TABLE OF CONTENTS

SECTION 1 - “THIRD PARTY” CATEGORIES 1
SECTION 2 - DEFINITIONS..... 1
SECTION 3 – GENERAL REQUIREMENTS 1
SECTION 4 – ADDITIONAL REQUIREMENTS FOR TREATMENT PROVIDERS 3
SECTION 5 – ADDITIONAL REQUIREMENTS FOR EDUCATION/TEACHING INSTITUTIONS 4
SECTION 6 – ADDITIONAL REQUIREMENTS FOR HEALTH INSURERS 4
SECTION 7 - DEPARTMENT’S RIGHTS..... 4
SECTION 8 - DATA BREACH; LOSS OF CITY DATA..... 5
Attachment 1 to SAA..... 6

TERMS AND CONDITIONS

The following terms and conditions govern Third Party access to San Francisco Department of Public Health (“Department” and/or “City”) Computer Systems. Third Party access to Department Computer Systems and Department Confidential Information is predicated on compliance with the terms and conditions set forth herein.

SECTION 1 - “THIRD PARTY” CATEGORIES

1. **Third Party In General:** means an entity seeking to access a Department Computer System. Third Party includes, but is not limited to, Contractors (including but not limited to Contractor’s employees, agents, subcontractors), Researchers, and Grantees, as further defined below. Category-specific terms for Treatment Providers, Education Institutions, and Health Insurers are set forth Sections 4 through 6, herein.
2. **Treatment Provider:** means an entity seeking access to Department Computer Systems in order to obtain patient information necessary to provide patient treatment, billing, and healthcare operations, including access for Physician Practices, Hospitals, Long Term Care Facilities, and Nursing Homes.
3. **Education Institution:** means an entity seeking access to Department Computer Systems to support the training of its students while performing education activities at Department facilities.
4. **Health Insurer:** means an entity seeking access to provide health insurance or managed care services for Department patients.

SECTION 2 - DEFINITIONS

1. **“Agreement”** means an Agreement between the Third Party and Department that necessitates Third Party’s access to Department Computer System. Agreement includes, but is not limited to, clinical trial agreements, accreditation agreements, affiliation agreements, professional services agreements, no-cost memoranda of understanding, and insurance network agreements.
2. **“Department Computer System”** means an information technology system used to gather and store information, including Department Confidential Information, for the delivery of services to the Department.
3. **“Department Confidential Information”** means information contained in a Department Computer System, including identifiable protected health information (“PHI”) or personally identifiable information (“PII”) of Department patients.
4. **“Third Party”** and/or **“Contractor”** means a Third Party Treatment Provider, Education Institution, and/or Health Insurer, under contract with the City.
5. **“User”** means an individual who is being provided access to a Department Computer Systems on behalf of Third Party. Third Party Users include, but are not limited to, Third Party’s employees, students/trainees, agents, and subcontractors.

SECTION 3 – GENERAL REQUIREMENTS

1. **Third Party Staff Responsibility.** Third Party is responsible for its work force and each Third Party User’s compliance with these Third Party System Access Terms and Conditions.
2. **Limitations on Access.** User’s access shall be based on the specific roles assigned by Department to ensure that access to Department Computer Systems and Department Confidential Information is limited to the minimum necessary to perform under the Agreement.

3. **Qualified Personnel.** Third Party and Department (i.e., training and onboarding) shall ensure that Third Party Users are qualified to access a Department Computer System.

4. **Remote Access/Multifactor Authentication.** Department may permit Third Party Users to access a Department Computer System remotely. Third Party User shall use Department's multifactor authentication solution when accessing Department systems remotely or whenever prompted.

5. **Issuance of Unique Accounts.** Department will issue a unique user account for each User of a Department Computer System. Third Party User is permitted neither to share such credentials nor use another user's account.

6. **Appropriate Use.** Third Party is responsible for the appropriate use and safeguarding of credentials for Department Computer System access issued to Third Party Users. Third Party shall take the appropriate steps to ensure that their employees, agents, and subcontractors will not intentionally seek out, download, transfer, read, use, or disclose Department Confidential Information other than for the use category described in Section 1 – "Third Party" Categories.

7. **Notification of Change in Account Requirements.** Third Party shall promptly notify Department via Third Party's Report for DPH Service Desk (dph.helpdesk@sfdph.org) in the event that Third Party or a Third Party User no longer has a need to use Department Computer Systems(s), or if the Third Party User access requirements change. Such notification shall be made no later than one (1) business day after determination that use is no longer needed or that access requirements have changed.

8. **Assistance to Administer Accounts.** The Parties shall provide all reasonable assistance and information necessary for the other Party to administer the Third Party User accounts.

9. **Security Controls.** Third Party shall appropriately secure Third Party's computing infrastructure, including but not limited to computer equipment, mobile devices, software applications, and networks, using industry standard tools to reduce the threat that an unauthorized individual could use Third Party's computing infrastructure to gain unauthorized access to a Department Computer System. Third Party shall also take commercially reasonable measures to protect its computing infrastructure against intrusions, viruses, worms, ransomware, or other disabling codes. General security controls include, but are not limited to:

a **Password Policy.** Third Party must maintain a password policy based on information security best practices for password length, complexity, and reuse. Third Party credentials used to access Third Party networks and systems must be configured for a password change no greater than every 90 calendar days.

b **Workstation/Laptop Encryption.** All Third Party-owned or managed workstations, laptops, tablets, smart phones, and similar devices that access a Department Computer System must be configured with full disk encryption using a FIPS 140-2 certified algorithm.

c **Endpoint Protection Tools.** All Third Party-owned or managed workstations, laptops, tablets, smart phones, and similar devices that access a Department Computer System must maintain a current installation of comprehensive anti-virus, anti-malware, anti-ransomware, desktop firewall, and intrusion prevention software with automatic updates scheduled at least daily.

d **Patch Management.** To correct known security vulnerabilities, Third Party shall install security patches and updates in a timely manner on all Third Party-owned workstations, laptops, tablets, smart phones, and similar devices that access Department Computer Systems based on Third Party's risk assessment of such patches and updates, the technical requirements of Third Party's computer systems, and the vendor's written recommendations. If patches and

updates cannot be applied in a timely manner due to hardware or software constraints, mitigating controls must be implemented based upon the results of a risk assessment.

e **Mobile Device Management.** Third Party shall ensure both corporate-owned and personally owned mobile devices have Mobile Device Management (MDM) installed. Given the prevalence of restricted data in Third Party's environment, all mobile devices used for Third Party's business must be encrypted. This applies to both corporate-owned and privately-owned mobile devices. At a minimum, the MDM should: Enforce an entity's security policies and perform real-time compliance checking and reporting; Enforce strong passwords/passcodes for access to mobile devices; Perform on-demand remote wipe if a mobile device is lost or stolen; Mandate device encryption.

10. **Auditing Accounts Issued.** Department reserves the right to audit the issuance and use of Third Party User accounts. To the extent that Department provides Third Party with access to tools or reports to audit what Department Confidential Information a Third Party User has accessed on a Department Computer System, Third Party must perform audits on a regular basis to determine if a Third Party User has inappropriately accessed Department Confidential Information.

11. **Assistance with Investigations.** Third Party must provide all assistance and information reasonably necessary for Department to investigate any suspected inappropriate use of a Department Computer Systems or access to Department Confidential Information. The Department may terminate a Third Party' User's access to a Department Computer System following a determination of inappropriate use of a Department Computer System.

12. **Inappropriate Access, Failure to Comply.** If Third Party suspects that a Third Party User has inappropriately accessed a Department Computer System or Department Confidential Information, Third Party must immediately, and within no more than one (1) business day, notify Department.

13. **Policies and Training.** Third Party must develop and implement appropriate policies and procedures to comply with applicable privacy, security and compliance rules and regulations. Third Party shall provide appropriate training to Third Party Users on such policies. Access will only be provided to Third Party Users once all required training is completed.

14. **Third Party Data User Confidentiality Agreement.** Before Department Computer System access is granted, as part of Department's compliance, privacy, and security training, each Third Party User must complete Department's individual user confidentiality, data security and electronic signature agreement form. The agreement must be renewed annually.

15. **Corrective Action.** Third Party shall take corrective action upon determining that a Third Party User may have violated these Third Party System Access Terms and Conditions.

16. **No Technical or Administrative Support.** Except as provided herein or otherwise agreed, the Department will provide no technical or administrative support to Third Party or Third Party User(s) for Department Computer System access; provided, however, that the foregoing does not apply to technical or administrative support necessary to fulfill Third Party's contractual and/or legal obligations, or as required to comply with the terms of this Agreement.

SECTION 4 – ADDITIONAL REQUIREMENTS FOR TREATMENT PROVIDERS

1. **Permitted Access, Use and Disclosure.** Treatment Providers and Treatment Provider Users shall access Department Confidential Information of a patient/client in accordance with applicable privacy rules and data protection laws. Requests to obtain data for research purposes require approval from an Institutional Review Board (IRB).

2. **Redisclosure Prohibition.** Treatment Providers may not redisclose Department Confidential Information, except as otherwise permitted by law.

3. **HIPAA Security Rule.** Under the HIPAA Security Rule, Treatment Providers must implement safeguards to ensure appropriate protection of protected/electronic health information (PHI/EHI), including but not limited to the following:

- a) Ensure the confidentiality, integrity, and security of all PHI/EHI they create, receive, maintain or transmit when using Department Computer Systems;
- b) Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- c) Protect against reasonably anticipated, impermissible uses or disclosures; and
- d) Ensure compliance by their workforce.

SECTION 5 – ADDITIONAL REQUIREMENTS FOR EDUCATION/TEACHING INSTITUTIONS

1. **Education Institution is Responsible for its Users.** Education Institutions shall inform Education Institution Users (including students, staff, and faculty) of their duty to comply with the terms and conditions herein. Department shall ensure that all Education Institution Users granted access to a Department Computer System shall first successfully complete Department’s standard staff training for privacy and compliance, information security and awareness, and software-application specific training before being provided User accounts and access to Department Computer Systems.

2. **Tracking of Training and Agreements.** Department shall maintain evidence of all Education Institution Users (including students, staff, and faculty) having successfully completed Department’s standard staff training for privacy and compliance and information security and awareness. Such evidence shall be maintained for a period of five (5) years from the date of graduation or termination of the Third Party User’s access.

SECTION 6 – ADDITIONAL REQUIREMENTS FOR HEALTH INSURERS

1. **Permitted Access, Use and Disclosure.** Health Insurers and Health Insurer Users may access Department Confidential Information only as necessary for payment processing and audits, including but not limited to quality assurance activities, wellness activities, care planning activities, and scheduling.

2. **Member / Patient Authorization.** Before accessing, using, or further disclosing Department Confidential Information, Health Insurers must secure all necessary written authorizations from the patient / member or such individuals who have medical decision-making authority for the patient / member.

SECTION 7 - DEPARTMENT’S RIGHTS

1. **Periodic Reviews.** Department reserves the right to perform regular audits to determine if a Third Party’s access to Department Computer Systems complies with these terms and conditions.

2. **Revocation of Accounts for Lack of Use.** Department may revoke any account if it is not used for a period of ninety (90) days.

3. **Revocation of Access for Cause.** Department and Third Party reserves the right to suspend or terminate a Third Party User’s access to Department Computer Systems at any time for cause, i.e., the Parties determined that a Third-Party User has violated the terms of this Agreement and/or Applicable law.

4. **Third Party Responsibility for Cost.** Each Third Party is responsible for its own costs incurred in connection with this Agreement or accessing Department Computer Systems.

SECTION 8 - DATA BREACH; LOSS OF CITY DATA.

1. **Data Breach Discovery.** Following Third Party's discovery of a breach of City Data disclosed to Third Party pursuant to this Agreement, Third Party shall notify City in accordance with applicable laws. Third Party shall:

- i. mitigate, to the extent practicable, any risks or damages involved with the breach or security incident and to protect the operating environment; and
- ii. comply with any requirements of federal and state laws as applicable to Third Party pertaining to the breach of City Data.

2. **Investigation of Breach and Security Incidents.** To the extent a breach or security system is identified within Third Party's System that involves City Data provided under this Agreement, Third Party shall investigate such breach or security incident. For the avoidance of doubt, City shall investigate any breach or security incident identified within the City's Data System. To the extent of Third Party discovery of information that relates to the breach or security incident of City Data, Third Party User shall inform the City of:

- i. the City Data believed to have been the subject of breach;
- ii. a description of the unauthorized persons known or reasonably believed to have improperly used, accessed or acquired the City Data;
- iii. to the extent known, a description of where the City Data is believed to have been improperly used or disclosed; and
- iv. to the extent known, a description of the probable and proximate causes of the breach or security incident;

3. **Written Report.** To the extent a breach is identified within Third Party's System, Third Party shall provide a written report of the investigation to the City as soon as practicable; provided, however, that the report shall not include any information protected under the attorney-client privileged, attorney-work product, peer review laws, and/or other applicable privileges. The report shall include, but not be limited to, the information specified above, as well as information on measures to mitigate the breach or security incident.

4. **Notification to Individuals.** If notification to individuals whose information was breached is required under state or federal law, Third Party shall cooperate with and assist City in its notification (including substitute notification) to the individuals affected by the breach

5. **Sample Notification to Individuals.** If notification to individuals is required, Third Party shall cooperate with and assist City in its submission of a sample copy of the notification to the Attorney General.

6. **Media Communications.** The Parties shall together determine any communications related to a Data Breach.

7. **Protected Health Information.** Third Party and its subcontractors, agents, and employees shall comply with all federal and state laws regarding the transmission, storage and protection of all PHI disclosed to Third Party by City. In the event that City pays a regulatory fine, and/or is assessed civil penalties or damages through private rights of action, based on an impermissible use or disclosure of PHI given to Third Party by City, Third Party shall indemnify City for the amount of such fine or penalties or damages, including costs of notification, but only in proportion to and to the extent that such fine, penalty or damages are caused by or result from the impermissible acts or omissions of Third Party. This section does not apply to the extent fines or penalties or damages were caused by the City or its officers, agents, subcontractors or employees.

Attachment 1 to SAA
System Specific Requirements

I. For Access to Department Epic through Care Link the following terms shall apply:

A. Department Care Link Requirements:

1. Connectivity.
 - a) Third Party must obtain and maintain an Internet connection and equipment in accordance with specifications provided by Epic and/or Department. Technical equipment and software specifications for accessing Department Care Link may change over time. Third Party is responsible for all associated costs. Third Party shall ensure that Third Party Data Users access the System only through equipment owned or leased and maintained by Third Party.
2. Compliance with Epic Terms and Conditions.
 - a) Third Party will at all times access and use the System strictly in accordance with the Epic Terms and Conditions. The following Epic Care Link Terms and Conditions are embedded within the Department Care Link application, and each Data User will need to agree to them electronically upon first sign-in before accessing Department Care Link:
3. Epic-Provided Terms and Conditions
 - a) Some short, basic rules apply to you when you use your EpicCare Link account. Please read them carefully. The Epic customer providing you access to EpicCare Link may require you to accept additional terms, but these are the rules that apply between you and Epic.
 - b) Epic is providing you access to EpicCare Link, so that you can do useful things with data from an Epic customer's system. This includes using the information accessed through your account to help facilitate care to patients shared with an Epic customer, tracking your referral data, or otherwise using your account to further your business interests in connection with data from an Epic customer's system. However, you are not permitted to use your access to EpicCare Link to help you or another organization develop software that is similar to EpicCare Link. Additionally, you agree not to share your account information with anyone outside of your organization.

II. For Access to Department Epic through Epic Hyperspace the following terms shall apply:

A. Department Epic Hyperspace:

1. Connectivity.
 - a) Third Party must obtain and maintain an Internet connection and required equipment in accordance with specifications provided by Epic and Department. Technical equipment and software specifications for accessing Department Epic Hyperspace will change over time. You may request a copy of required browser, system, and connection requirements from the Department IT division. Third Party is responsible for all associated costs. Third Party shall ensure that Third Party Data Users access the System in accordance with the terms of this agreement.
2. Application For Access and Compliance with Epic Terms and Conditions.
 - a) Prior to entering into agreement with Department to access Department Epic Hyperspace, Third Party must first complete an Application For Access with Epic Systems Corporation of Verona, WI. The Application For Access is found at: <https://userweb.epic.com/Forms/AccessApplication>. Epic Systems Corporation notifies Department, in writing, of Third Party's permissions to access Department Epic Hyperspace

prior to completing this agreement. Third Party will at all times access and use the system strictly in accordance with the Epic Terms and Conditions.

III. For Access to Department myAvatar the following terms shall apply:

A. Department myAvatar

1. Connectivity.

- a. Third Party must obtain an Internet connection and required equipment in accordance with specifications provided by Department. Technical equipment and software specifications for accessing Department myAvatar will change over time. You may request a copy of required browser, system, and connection requirements from the Department IT division. Third Party is responsible for all associated costs. Third Party shall ensure that Third Party Data Users access the System only through equipment owned or leased and maintained by Third Party.

2. Information Technology (IT) Support.

- a. Third Party must have qualified and professional IT support who will participate in quarterly CBO Technical Workgroups.

3. Access Control.

- a. Access to the BHS Electronic Health Record is granted based on clinical and business requirements in accordance with the Behavioral Health Services EHR Access Control Policy (6.00-06). The Access Control Policy is found at:
<https://www.sfdph.org/dph/files/CBHSPolProcMnl/6.00-06.pdf>
- b. Applicants must complete the myAvatar Account Request Form found at
https://www.sfdph.org/dph/files/CBHSdocs/BHISdocs/UserDoc/Avatar_Account_Request_Form.pdf
- c. All licensed, waived, registered and/or certified providers must complete the Department credentialing process in accordance with the DHCS MHSUDS Information Notice #18-019.



San Francisco Department of Public Health
Business Associate Agreement

This Business Associate Agreement (“BAA”) supplements and is made a part of the contract by and between the City and County of San Francisco, the Covered Entity (“CE”), and Contractor, the Business Associate (“BA”) (the “Agreement”). To the extent that the terms of the Agreement are inconsistent with the terms of this BAA, the terms of this BAA shall control.

RECITALS

A. CE, by and through the San Francisco Department of Public Health (“SFDPH”), wishes to disclose certain information to BA pursuant to the terms of the Agreement, some of which may constitute Protected Health Information (“PHI”) (defined below).

B. For purposes of the Agreement, CE requires Contractor, even if Contractor is also a covered entity under HIPAA, to comply with the terms and conditions of this BAA as a BA of CE.

C. CE and BA intend to protect the privacy and provide for the security of PHI disclosed to BA pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and regulations promulgated there under by the U.S. Department of Health and Human Services (the “HIPAA Regulations”) and other applicable laws, including, but not limited to, California Civil Code §§ 56, et seq., California Health and Safety Code § 1280.15, California Civil Code §§ 1798, et seq., California Welfare & Institutions Code §§5328, et seq., and the regulations promulgated there under (the “California Regulations”).

D. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(a) and (e) and 164.504(e) of the Code of Federal Regulations (“C.F.R.”) and contained in this BAA.

E. BA enters into agreements with CE that require the CE to disclose certain identifiable health information to BA. The parties desire to enter into this BAA to permit BA to have access to such information and comply with the BA requirements of HIPAA, the HITECH Act, and the corresponding Regulations.

In consideration of the mutual promises below and the exchange of information pursuant to this BAA, the parties agree as follows:

1. Definitions.

a. **Breach** means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information, and shall have the meaning given to such term under the HITECH Act and HIPAA Regulations [42 U.S.C. Section 17921 and 45 C.F.R. Section 164.402], as well as California Civil Code Sections 1798.29 and 1798.82.



San Francisco Department of Public Health
Business Associate Agreement

b. Breach Notification Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and D.

c. Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information received from a covered entity, but other than in the capacity of a member of the workforce of such covered entity or arrangement, and shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including, but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.

d. Covered Entity means a health plan, a health care clearinghouse, or a health care provider who transmits any information in electronic form in connection with a transaction covered under HIPAA Regulations, and shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

e. Data Aggregation means the combining of Protected Information by the BA with the Protected Information received by the BA in its capacity as a BA of another CE, to permit data analyses that relate to the health care operations of the respective covered entities, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

f. Designated Record Set means a group of records maintained by or for a CE, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

g. Electronic Protected Health Information means Protected Health Information that is maintained in or transmitted by electronic media and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to, 45 C.F.R. Section 160.103. For the purposes of this BAA, Electronic PHI includes all computerized data, as defined in California Civil Code Sections 1798.29 and 1798.82.

h. Electronic Health Record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given to such term under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

i. Health Care Operations shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

j. Privacy Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

k. Protected Health Information or PHI means any information, including electronic PHI, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental 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 (ii) that identifies the individual or



San Francisco Department of Public Health
Business Associate Agreement

with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Sections 160.103 and 164.501. For the purposes of this BAA, PHI includes all medical information and health insurance information as defined in California Civil Code Sections 56.05 and 1798.82.

l. Protected Information shall mean PHI provided by CE to BA or created, maintained, received or transmitted by BA on CE's behalf.

m. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, and shall have the meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. Section 164.304.

n. Security Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

o. Unsecured PHI means PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute, and shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h) and 45 C.F.R. Section 164.402.

2. Obligations of Business Associate.

a. Attestations. Except when CE's data privacy officer exempts BA in writing, the BA shall complete the following forms, attached and incorporated by reference as though fully set forth herein, SFDPH Attestations for Privacy (Attachment 1) and Data Security (Attachment 2) within sixty (60) calendar days from the execution of the Agreement. If CE makes substantial changes to any of these forms during the term of the Agreement, the BA will be required to complete CE's updated forms within sixty (60) calendar days from the date that CE provides BA with written notice of such changes. BA shall retain such records for a period of seven years after the Agreement terminates and shall make all such records available to CE within 15 calendar days of a written request by CE.

b. User Training. The BA shall provide, and shall ensure that BA subcontractors, provide, training on PHI privacy and security, including HIPAA and HITECH and its regulations, to each employee or agent that will access, use or disclose Protected Information, upon hire and/or prior to accessing, using or disclosing Protected Information for the first time, and at least annually thereafter during the term of the Agreement. BA shall maintain, and shall ensure that BA subcontractors maintain, records indicating the name of each employee or agent and date on which the PHI privacy and security trainings were completed. BA shall retain, and ensure that BA subcontractors retain, such records for a period of seven years after the Agreement terminates and shall make all such records available to CE within 15 calendar days of a written request by CE.



San Francisco Department of Public Health
Business Associate Agreement

c. Permitted Uses. BA may use, access, and/or disclose Protected Information only for the purpose of performing BA's obligations for, or on behalf of, the City and as permitted or required under the Agreement and BAA, or as required by law. Further, BA shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by CE. However, BA may use Protected Information as necessary (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) as required by law; or (iv) for Data Aggregation purposes relating to the Health Care Operations of CE [45 C.F.R. Sections 164.502, 164.504(e)(2), and 164.504(e)(4)(i)].

d. Permitted Disclosures. BA shall disclose Protected Information only for the purpose of performing BA's obligations for, or on behalf of, the City and as permitted or required under the Agreement and BAA, or as required by law. BA shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by CE. However, BA may disclose Protected Information as necessary (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) as required by law; or (iv) for Data Aggregation purposes relating to the Health Care Operations of CE. If BA discloses Protected Information to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and used or disclosed only as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches, security incidents, or unauthorized uses or disclosures of the Protected Information in accordance with paragraph 2 (n) of this BAA, to the extent it has obtained knowledge of such occurrences [42 U.S.C. Section 17932; 45 C.F.R. Section 164.504(e)]. BA may disclose PHI to a BA that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit Protected Information on its behalf, if the BA obtains satisfactory assurances, in accordance with 45 C.F.R. Section 164.504(e)(1), that the subcontractor will appropriately safeguard the information [45 C.F.R. Section 164.502(e)(1)(ii)].

e. Prohibited Uses and Disclosures. BA shall not use or disclose Protected Information other than as permitted or required by the Agreement and BAA, or as required by law. BA shall not use or disclose Protected Information for fundraising or marketing purposes. BA shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the Protected Information solely relates [42 U.S.C. Section 17935(a) and 45 C.F.R. Section 164.522(a)(1)(vi)]. BA shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of CE and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2), and the HIPAA regulations, 45 C.F.R. Section 164.502(a)(5)(ii); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to the Agreement.

f. Appropriate Safeguards. BA shall take the appropriate security measures to protect the confidentiality, integrity and availability of PHI that it creates, receives, maintains, or transmits on behalf of the CE, and shall prevent any use or disclosure of PHI other than as permitted by the Agreement or this



San Francisco Department of Public Health
Business Associate Agreement

BAA, including, but not limited to, administrative, physical and technical safeguards in accordance with the Security Rule, including, but not limited to, 45 C.F.R. Sections 164.306, 164.308, 164.310, 164.312, 164.314 164.316, and 164.504(e)(2)(ii)(B). BA shall comply with the policies and procedures and documentation requirements of the Security Rule, including, but not limited to, 45 C.F.R. Section 164.316, and 42 U.S.C. Section 17931. BA is responsible for any civil penalties assessed due to an audit or investigation of BA, in accordance with 42 U.S.C. Section 17934(c).

g. Business Associate's Subcontractors and Agents. BA shall ensure that any agents and subcontractors that create, receive, maintain or transmit Protected Information on behalf of BA, agree in writing to the same restrictions and conditions that apply to BA with respect to such PHI and implement the safeguards required by paragraph 2.f. above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2) through (e)(5); 45 C.F.R. Section 164.308(b)]. BA shall mitigate the effects of any such violation.

h. Accounting of Disclosures. Within ten (10) calendar days of a request by CE for an accounting of disclosures of Protected Information or upon any disclosure of Protected Information for which CE is required to account to an individual, BA and its agents and subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935 (c), as determined by CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents and subcontractors for at least seven (7) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an Electronic Health Record. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure [45 C.F.R. 164.528(b)(2)]. If an individual or an individual's representative submits a request for an accounting directly to BA or its agents or subcontractors, BA shall forward the request to CE in writing within five (5) calendar days.

i. Access to Protected Information. BA shall make Protected Information maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within (5) days of request by CE to enable CE to fulfill its obligations under state law [Health and Safety Code Section 123110] and the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 C.F.R. Section 164.504(e)(2)(ii)(E)]. If BA maintains Protected Information in electronic format, BA shall provide such information in electronic format as necessary to enable CE to fulfill its obligations under the HITECH Act and HIPAA Regulations, including, but not limited to, 42 U.S.C. Section 17935(e) and 45 C.F.R. 164.524.



San Francisco Department of Public Health
Business Associate Agreement

j. Amendment of Protected Information. Within ten (10) days of a request by CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, BA and its agents and subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment or other documentation to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R Section 164.526. If an individual requests an amendment of Protected Information directly from BA or its agents or subcontractors, BA must notify CE in writing within five (5) days of the request and of any approval or denial of amendment of Protected Information maintained by BA or its agents or subcontractors [45 C.F.R. Section 164.504(e)(2)(ii)(F)].

k. Governmental Access to Records. BA shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to CE and to the Secretary of the U.S. Department of Health and Human Services (the “Secretary”) for purposes of determining BA’s compliance with HIPAA [45 C.F.R. Section 164.504(e)(2)(ii)(I)]. BA shall provide CE a copy of any Protected Information and other documents and records that BA provides to the Secretary concurrently with providing such Protected Information to the Secretary.

l. Minimum Necessary. BA, its agents and subcontractors shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the intended purpose of such use, disclosure, or request. [42 U.S.C. Section 17935(b); 45 C.F.R. Section 164.514(d)]. BA understands and agrees that the definition of “minimum necessary” is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes “minimum necessary” to accomplish the intended purpose in accordance with HIPAA and HIPAA Regulations.

m. Data Ownership. BA acknowledges that BA has no ownership rights with respect to the Protected Information.

n. Notification of Breach. BA shall notify CE within 5 calendar days of any breach of Protected Information; any use or disclosure of Protected Information not permitted by the BAA; any Security Incident (except as otherwise provided below) related to Protected Information, and any use or disclosure of data in violation of any applicable federal or state laws by BA or its agents or subcontractors. The notification shall include, to the extent possible, the identification of each individual whose unsecured Protected Information has been, or is reasonably believed by the BA to have been, accessed, acquired, used, or disclosed, as well as any other available information that CE is required to include in notification to the individual, the media, the Secretary, and any other entity under the Breach Notification Rule and any other applicable state or federal laws, including, but not limited, to 45 C.F.R. Section 164.404 through 45 C.F.R. Section 164.408, at the time of the notification required by this paragraph or promptly thereafter as information becomes available. BA shall take (i) prompt corrective action to cure any deficiencies and (ii) any action pertaining to unauthorized uses or disclosures required by applicable federal and state laws. [42 U.S.C. Section 17921; 42 U.S.C. Section 17932; 45 C.F.R. 164.410; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)]



San Francisco Department of Public Health
Business Associate Agreement

o. Breach Pattern or Practice by Business Associate's Subcontractors and Agents.

Pursuant to 42 U.S.C. Section 17934(b) and 45 C.F.R. Section 164.504(e)(1)(iii), if the BA knows of a pattern of activity or practice of a subcontractor or agent that constitutes a material breach or violation of the subcontractor or agent's obligations under the Contract or this BAA, the BA must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the BA must terminate the contractual arrangement with its subcontractor or agent, if feasible. BA shall provide written notice to CE of any pattern of activity or practice of a subcontractor or agent that BA believes constitutes a material breach or violation of the subcontractor or agent's obligations under the Contract or this BAA within five (5) calendar days of discovery and shall meet with CE to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

3. Termination.

a. Material Breach. A breach by BA of any provision of this BAA, as determined by CE, shall constitute a material breach of the Agreement and this BAA and shall provide grounds for immediate termination of the Agreement and this BAA, any provision in the AGREEMENT to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii).]

b. Judicial or Administrative Proceedings. CE may terminate the Agreement and this BAA, effective immediately, if (i) BA is named as defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

c. Effect of Termination. Upon termination of the Agreement and this BAA for any reason, BA shall, at the option of CE, return or destroy all Protected Information that BA and its agents and subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by CE, BA shall continue to extend the protections and satisfy the obligations of Section 2 of this BAA to such information, and limit further use and disclosure of such PHI to those purposes that make the return or destruction of the information infeasible [45 C.F.R. Section 164.504(e)(2)(ii)(J)]. If CE elects destruction of the PHI, BA shall certify in writing to CE that such PHI has been destroyed in accordance with the Secretary's guidance regarding proper destruction of PHI. Per the Secretary's guidance, the City will accept destruction of electronic PHI in accordance with the standards enumerated in the NIST SP 800-88, Guidelines for Media Sanitization. The City will accept destruction of PHI contained in paper records by shredding, burning, pulping, or pulverizing the records so that the PHI is rendered unreadable, indecipherable, and otherwise cannot be reconstructed.

d. Civil and Criminal Penalties. BA understands and agrees that it is subject to civil or criminal penalties applicable to BA for unauthorized use, access or disclosure of Protected Information in accordance with the HIPAA Regulations and the HITECH Act including, but not limited to, 42 U.S.C. 17934 (c).



San Francisco Department of Public Health
Business Associate Agreement

e. Disclaimer. CE makes no warranty or representation that compliance by BA with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations or corresponding California law provisions will be adequate or satisfactory for BA's own purposes. BA is solely responsible for all decisions made by BA regarding the safeguarding of PHI.

4. Amendment to Comply with Law.

The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Agreement or this BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable state or federal laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from BA that BA will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this BAA embodying written assurances consistent with the updated standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable state or federal laws. CE may terminate the Agreement upon thirty (30) days written notice in the event (i) BA does not promptly enter into negotiations to amend the Agreement or this BAA when requested by CE pursuant to this section or (ii) BA does not enter into an amendment to the Agreement or this BAA providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

5. Reimbursement for Fines or Penalties.

In the event that CE pays a fine to a state or federal regulatory agency, and/or is assessed civil penalties or damages through private rights of action, based on an impermissible access, use or disclosure of PHI by BA or its subcontractors or agents, then BA shall reimburse CE in the amount of such fine or penalties or damages within thirty (30) calendar days from City's written notice to BA of such fines, penalties or damages.

Attachment 1 – SFDPH Privacy Attestation, version 06-07-2017

Attachment 2 – SFDPH Data Security Attestation, version 06-07-2017

Attachment 3 – Protected Information Destruction Order Purge Certification 01-10-2024

Office of Compliance and Privacy Affairs
San Francisco Department of Public Health
101 Grove Street, Room 330, San Francisco, CA 94102
Email: compliance.privacy@sfdph.org
Hotline (Toll-Free): 1-855-729-6040

| | |
|------------------|---------------------------|
| Contractor Name: | Contractor City Vendor ID |
|------------------|---------------------------|

PRIVACY ATTESTATION

INSTRUCTIONS: Contractors and Partners who receive or have access to health or medical information or electronic health record systems maintained by SFPDH must complete this form. Retain completed Attestations in your files for a period of 7 years. Be prepared to submit completed attestations, along with evidence related to the following items, if requested to do so by SFPDH.

Exceptions: If you believe that a requirement is Not Applicable to you, see instructions below in Section IV on how to request clarification or obtain an exception.

I. All Contractors.

| DOES YOUR ORGANIZATION... | | | Yes | No* |
|---------------------------|---|---------------|-------------------|-----|
| A | Have formal Privacy Policies that comply with the Health Insurance Portability and Accountability Act (HIPAA)? | | | |
| B | Have a Privacy Officer or other individual designated as the person in charge of investigating privacy breaches or related incidents? | | | |
| | If yes: | Name & Title: | Phone # Email: | |
| C | Require health information Privacy Training upon hire and annually thereafter for all employees who have access to health information? [Retain documentation of trainings for a period of 7 years.] [SFPDH privacy training materials are available for use; contact OCPA at 1-855-729-6040.] | | | |
| D | Have proof that employees have signed a form upon hire and annually thereafter, with their name and the date, acknowledging that they have received health information privacy training? [Retain documentation of acknowledgement of trainings for a period of 7 years.] | | | |
| E | Have (or will have if/when applicable) Business Associate Agreements with subcontractors who create, receive, maintain, transmit, or access SFPDH's health information? | | | |
| F | Assure that staff who create, or transfer health information (via laptop, USB/thumb-drive, handheld), have prior supervisory authorization to do so AND that health information is only transferred or created on encrypted devices approved by SFPDH Information Security staff? | | | |

II. Contractors who serve patients/clients and have access to SFPDH PHI, must also complete this section.

| If Applicable: DOES YOUR ORGANIZATION... | | Yes | No* |
|--|---|-----|-----|
| G | Have (or will have if/when applicable) evidence that SFPDH Service Desk (628-206-SERV) was notified to de-provision employees who have access to SFPDH health information record systems within 2 business days for regular terminations and within 24 hours for terminations due to cause? | | |
| H | Have evidence in each patient's / client's chart or electronic file that a Privacy Notice that meets HIPAA regulations was provided in the patient's / client's preferred language? (English, Cantonese, Vietnamese, Tagalog, Spanish, Russian forms may be required and are available from SFPDH.) | | |
| I | Visibly post the Summary of the Notice of Privacy Practices in all six languages in common patient areas of your treatment facility? | | |
| J | Document each disclosure of a patient's/client's health information for purposes <u>other than</u> treatment, payment, or operations? | | |
| K | When required by law, have proof that signed authorization for disclosure forms (that meet the requirements of the HIPAA Privacy Rule) are obtained PRIOR to releasing a patient's/client's health information? | | |

III. ATTEST: Under penalty of perjury, I hereby attest that to the best of my knowledge the information herein is true and correct and that I have authority to sign on behalf of and bind Contractor listed above.

| | | | |
|---|------------------|-----------|------|
| ATTESTED by Privacy Officer or designated person | Name: (print) | Signature | Date |
|---|------------------|-----------|------|

IV. *EXCEPTIONS: If you have answered "NO" to any question or believe a question is Not Applicable, please contact OCPA at **1-855-729-6040** or compliance.privacy@sfdph.org for a consultation. All "No" or "N/A" answers must be reviewed and approved by OCPA below.

| | | | |
|----------------------------------|-----------------|-----------|------|
| EXCEPTION(S) APPROVED by OCPA | Name (print) | Signature | Date |
|----------------------------------|-----------------|-----------|------|

| | |
|------------------|---------------------------|
| Contractor Name: | Contractor City Vendor ID |
|------------------|---------------------------|

DATA SECURITY ATTESTATION

INSTRUCTIONS: Contractors and Partners who receive or have access to health or medical information or electronic health record systems maintained by SFPDH must complete this form. Retain completed Attestations in your files for a period of 7 years. Be prepared to submit completed attestations, along with evidence related to the following items, if requested to do so by SFPDH.

Exceptions: If you believe that a requirement is Not Applicable to you, see instructions in Section III below on how to request clarification or obtain an exception.

I. All Contractors.

| DOES YOUR ORGANIZATION... | Yes | No * |
|--|---------------|---------|
| A Conduct assessments/audits of your data security safeguards to demonstrate and document compliance with your security policies and the requirements of HIPAA/HITECH at least every two years? [Retain documentation for a period of 7 years] | | |
| B Use findings from the assessments/audits to identify and mitigate known risks into documented remediation plans? | | |
| Date of last Data Security Risk Assessment/Audit: | | |
| Name of firm or person(s) who performed the Assessment/Audit and/or authored the final report: | | |
| C Have a formal Data Security Awareness Program? | | |
| D Have formal Data Security Policies and Procedures to detect, contain, and correct security violations that comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)? | | |
| E Have a Data Security Officer or other individual designated as the person in charge of ensuring the security of confidential information? | | |
| If yes: | Name & Title: | Phone # |
| | Email: | |
| F Require Data Security Training upon hire and annually thereafter for all employees who have access to health information? [Retain documentation of trainings for a period of 7 years.] [SFPDH data security training materials are available for use: contact OCPA at 1-855-729-6040.] | | |
| G Have proof that employees have signed a form upon hire and annually, or regularly, thereafter, with their name and the date, acknowledging that they have received data security training? [Retain documentation of acknowledgement of trainings for a period of 7 years.] | | |
| H Have (or will have if/when applicable) Business Associate Agreements with subcontractors who create, receive, maintain, transmit, or access SFPDH's health information? | | |
| I Have (or will have if/when applicable) a diagram of how SFPDH data flows between your organization and subcontractors or vendors (including named users, access methods, on-premise data hosts, processing systems, etc.)? | | |

II. ATTEST: Under penalty of perjury, I hereby attest that to the best of my knowledge the information herein is true and correct and that I have authority to sign on behalf of and bind Contractor listed above.

| | | | |
|--|---------------|-----------|------|
| ATTESTED by Data Security Officer or designated person | Name: (print) | Signature | Date |
|--|---------------|-----------|------|

III. *EXCEPTIONS: If you have answered "NO" to any question or believe a question is Not Applicable, please contact OCPA at 1-855-729-6040 or compliance.privacy@sfdph.org for a consultation. All "No" or "N/A" answers must be reviewed and approved by OCPA below.

| | | | |
|-------------------------------|--------------|-----------|------|
| EXCEPTION(S) APPROVED by OCPA | Name (print) | Signature | Date |
|-------------------------------|--------------|-----------|------|

Attachment 3 to Appendix E

Protected Information Destruction Order

Purge Certification - Contract ID # 1000028223

In accordance with section 3.c (Effect of Termination) of the Business Associate Agreement, attached as Appendix E to the Agreement between the City and Contractor dated March 1, 2023 (“Agreement”), the City hereby directs Contractor to destroy all Protected Information that Contractor and its agents and subcontractors (collectively “Contractor”) still maintain in any form. Contractor may retain no copies of destroyed Protected Information.” Destruction must be in accordance with the guidance of the Secretary of the U.S. Department of Health and Human Services (“Secretary”) regarding proper destruction of PHI.

Electronic Data: Per the Secretary’s guidance, the City will accept destruction of electronic Protected Information in accordance with the standards enumerated in the NIST SP 800-88, Guidelines for Data Sanitization (“NIST”).

Hard-Copy Data: Per the Secretary’s guidance, the City will accept destruction of Protected Information contained in paper records by shredding, burning, pulping, or pulverizing the records so that the Protected Information is rendered unreadable, indecipherable, and otherwise cannot be reconstructed.

Contractor hereby certifies that Contractor has destroyed all Protected Information as directed by the City in accordance with the guidance of the Secretary of the U.S. Department of Health and Human Services (“Secretary”) regarding proper destruction of PHI.

So Certified

Signature

Title:

Date: