

|                  |  |                           |  |
|------------------|--|---------------------------|--|
| 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 SFDPH 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 SFDPH.

**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.] [SFDPH 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 SFDPH's health information?  |               |         |        |  |     |     |
| I                         | Have (or will have if/when applicable) a diagram of how SFDPH 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](mailto: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 |
|-------------------------------|--------------|--|-----------|------|