Business Associate Agreement (BAA)

At DPH, we utilize the services of a variety of CBOs, suppliers, vendors, and service providers to carry out our activities, services, and functions. In these relationships, DPH is considered a Covered Entity. When these outside entities require access, creation, maintenance, or storage of protected health information (PHI) a Business Associate (BA) relationship exists. With all business associates, a Business Associate Agreement (BAA) is required.

### Things you need to know about a BAA:

- Prior to allowing a Business Associate (BA) access to DPH’s Protected Health Information (PHI), San Francisco Department of Public Health (SFDPH) must execute a BAA with the Business Associate (ex. CBO or suppliers).
- The HIPAA Omnibus Final Rule defines business associate expectations. It contains recommended guidelines for compliance, and outlines consequences for noncompliance for Covered Entities and Business Associates.
- When DPH has a Business Associate relationship with an individual or entity, a SFDPH Business Associate Agreement (BAA) that complies with HIPAA and the Health Information Technology Act (HITECH Act) must be executed between the parties.
- Typically, vendors going through the SFDPH contracting process will have BAAs within their contract. Services procured through purchase orders, or via the UCSF contracting process will not have a SFDPH BAA in place. The absence of a BAA when it is legally required puts our patients’ privacy, and SFDPH’s reputation, at risk.
- The BAA defines the authorized uses of PHI, the safeguards required to protect the information, and steps to take in the event of breach of PHI.

#### Examples of activities that require a BAA:

| Claims processing or administrative services | Research functions (if 3rd party vendor is analyzing our data) |
| Data analysis                              | Consulting |
| Billing                                    | Software maintenance or support that includes access to PHI |
| Clinical Services                          | Financial Services |

### Steps to take to obtain a BAA contract:

The DPH Office of Compliance and Privacy Affairs (OCPA) maintains the approved standard forms for the Business Associate Agreements. Any variance from the standard form for use in a particular BA relationship must be approved by the office of OCPA.

#### Guidance:

- The SFDPH BAA template is available on the [DPH Privacy website (SFDPH BAA)](https://www.sfdph.org/). Note that this template is not a “standalone” agreement; it must be modified by OCPA or appended to an existing agreement. Contact OCPA at (855) 729-6040 or compliance.privacy@sfdph.org for details.
- The DPH contracting party is responsible for working with the BA and OCPA to complete a fully executed Business Associate Agreement. Such as:
  - Provide a Summary of scope of work or purpose (i.e., how will PHI be used?)
  - Provide Copies of any existing agreements, MOUs, or purchase orders with documentation of completed SFDPH IT security vendor evaluation (i.e., how do we know PHI is adequately protected?)
- Known or suspected violations of a BAA are to be reported to the OCPA Privacy Officer. Subcontractors of the BA are held to the same standards as the BA.

#### Report a Privacy Breach:

- Report every potential breach of protected health information
  - Privacy & Compliance Hotline: (855) 729-6040
  - Email: Compliance.Privacy@sfdph.org
  - Refer to [Policy B1.1 Reporting of Unlawful or Unauthorized Access to PHI](https://www.sfdph.org/)

The Privacy Office also provides consultation on all privacy related questions. Please feel free to contact us.