City and County of San Francisco Department of Public Health

User Agreement for Confidentiality, Data Security and Electronic Signature

Individuals with access to SFDPH confidential information and data systems have a legal and ethical responsibility to protect the security and confidentiality of personal, medical, financial, personnel and protected health information, and to use that information and those systems only as permitted in the performance of their jobs. The following applies to confidential, restricted, or protected SFDPH information and assets that are accessed, received or sent in any format, including digital, paper, voice, facsimile, photos, electronic signatures, etc.

By signing this document, I understand and hereby agree to the following terms and conditions:

1. **Violations:**
    a. **Employees**: Non-adherence to this Agreement may result in termination of employment.
    b. **Non-City Employees**: Non-adherence to this Agreement may result in termination of access to SFDPH confidential information and data systems, and/or termination of contractual or affiliated relationship with SFDPH.
    c. **Everyone:** Violation of state and federal laws regarding patient privacy may subject me to substantial monetary penalties and/or make me the subject of a civil or criminal action pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Medical Information Act, the LPS Act, the Welfare and Institutions Code Section 14100.2, and other federal and state privacy laws.

2. **Policies:** I have access to and I agree to abide by SFDPH Privacy and Data Security Policies found at http://www.sfdph.org/DPH/privacy

3. **Patient Protections:** I understand that patient information is protected in every form, such as written records and correspondence, oral communications and computer programs, applications and data. I will only access, discuss, or divulge confidential SFDPH information as required for the performance of my job duties. I agree not to use, copy, make notes regarding, remove, release or disclose patient Information unless it is permitted by SFDPH policy and local, state, and/or Federal Law.

4. **Releasing Information:** I agree to take all reasonable precautions to assure that SFDPH information or information entrusted to SFDPH by third parties (such as patients) will not be disclosed to unauthorized persons. I understand I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the SFDPH Program Director. I agree not to publish or otherwise make public any information regarding persons receiving services without prior authorization or as required by law. Providers may need to use all of an individual's health information in the provision of patient care.

5. **Accessing Systems:** I agree not to access or attempt to access any system, nor allow access by another person or group, without specific authorization from a local Information System Director. I agree not to demonstrate the operation of systems to anyone without express authorization of a local Information System Director. SFDPH information systems maintain internal logs of applications and data accessed, indicating who viewed, added, edited, printed or deleted information. I may be asked to justify my use of specific information contained in or managed by SFDPH information systems.

6. **Information Assets:** In order to ensure the integrity and security of SFDPH systems, I agree not to disclose any portion of the organization's information assets to any unauthorized person. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens, documentation or intellectual capital created, licensed or owned by SFDPH. I agree to forward any request for such information to my supervisor and/or the SFDPH Public Information Officer.

7. **Devices:** I will not download or maintain patient information on my privately-owned portable devices. If using a SFDPH- or UCSF-provided and password-protected device, I will delete patient information (and empty it from my device's recycle bin) promptly when it is no longer needed to fulfill my job responsibilities. I understand that the risk of privacy being breached increases with the mobility of that data and I recognize extra precautions must be used when using handheld computers and/or smart phones to store or transmit sensitive information.

8. **User IDs and Passwords:** Individuals requiring access to SFDPH information systems will be given a user ID and password. It is my responsibility to maintain the confidentiality of patient and other information to which I have access. I agree to keep my user IDs and passwords secret and secure by taking reasonable security measures to prevent them from being lost or inappropriately acquired, modified or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of them, or of any media on which information about them are stored. If I suspect that my user ID or password has been stolen or inappropriately acquired, lost, used by an unauthorized party, or otherwise compromised, I will immediately notify the appropriate Information Systems Help Desk and request that my electronic signature be revoked. I agree to choose a difficult-to-guess password, not to share this password with any other person and not to write this password down as described in SFDPH Data Security Policies.

9. **Property Rights**: The hardware, software, data and outputs of SFDPH information system are the property of the SFDPH and must be appropriately licensed for installation on a SFDPH computer. I will obtain prior authorization from a SFDPH information systems administrator before installing personal software on a SFDPH computer. SFDPH has the right, in its sole discretion, to review and remove personal or unlicensed software and data on any SFDPH computer or information system.

10. **Electronic Signatures:** When my signature or co-signature is required for "a financial, program or medical record" under California or Federal law, California or Federal regulation, or organizational policy or procedure, my user ID and password together shall constitute an electronic signature. For the purposes of authorizing and authenticating electronic health records, my electronic signature has the full force, effect, and responsibility of a signature affixed by hand to a paper document. My electronic signature establishes me as the signer or co-signer of electronic documents. My electronic signature will be valid for the length of time specified in the SFDPH Password Security Policy (or the database administrator, whichever is shorter) from date of issuance, or earlier if it is revoked or terminated per the terms of the user agreement. Prior to the expiration date, I will receive a system alert when my password is due to expire and be given the opportunity to renew it. Setting a new password for my user-ID (electronic signature) renews the terms of this agreement.

11. **Upon Termination**: At the end of my employment, affiliation, or contract with SFDPH, I agree to return to SFDPH all information to which I have had access as a result of my position with SFDPH.

12. **Reporting:** I will report any suspected privacy or data security violations and any other types of misconduct to the Compliance and Privacy Hotline (855-729-6040).

Employees

I understand that looking at patient information without having a permitted business purpose is against the law. I also understand that if I violate any of the requirements set forth in this User Agreement, SFDPH in its sole discretion, may immediately restrict, suspend, or permanently revoke my access to any SFDPH confidential information and/or data systems, terminate my employment, and, if applicable report me to regulatory bodies and/or my professional board.

User Name (Print)		User Department	
User Signature		Date Signed	

Agents, Contractors, Affiliates (e.g., researchers, student interns), Users not employed by the City

I understand that looking at patient information without having a permitted business purpose is against the law. I also understand that if I violate any of the requirements set forth in this User Agreement, SFDPH, in its sole discretion, may immediately restrict, suspend, or permanently revoke, my access to SFDPH confidential information and/or data systems. Further, the City may demand that I be removed or replaced from performing any work on any agreement with the City, terminate my or my employer's contract or agreement with the City, and if applicable, report me to regulatory bodies, and/or my professional board.

I ALSO UNDERSTAND THAT MY ACCESS TO SFDPH CONFIDENTIAL INFORMATION AND DATA SYSTEMS MAY ONLY BE RESTORED BY SFDPH IN ITS SOLE DISCRETION.

User Name (Print)		User Organization	
User Signature		Date Signed	

NOTE: This form must be signed at time of hire, each time authorization to access SFDPH confidential information or a data system is given, and annually thereafter. Signed forms are to be retained a minimum of 7 years post de-provisioning the individual's access to SFDPH confidential information or data system and/or termination of employment.