San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: F.1.0 User Agreement for Confidentiality, Data Security, and Electronic Signature	
Category: Privacy	
Effective Date: March 19, 2015	**Last Reviewed/Revised:** 3/12/2026
DPH Unit of Origin: Office of Compliance and Privacy Affairs	
Policy Contact - Employee Name and Title; and/or DPH Division: Office of Compliance and Privacy Affairs (OCPA)	
Contact Phone Number(s): (855) 729-6040	
Distribution: DPH-wide X	**If not DPH-wide, other distribution:**

All sections in table required.

I. **Purpose and Scope:**

A. **Purpose:** The purpose of this policy is to establish the procedure to ensure that all individuals with access to SFDPH protected health information (PHI), confidential information, and data systems understand that they have a legal and ethical responsibility to protect the security and confidentiality of personal, medical, financial, personnel records, and PHI, and to use that information and those systems only in the performance of their jobs.

B. **Scope:** 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.

II. **Background and Procedure:**

A. **Background:** The San Francisco Department of Public Health maintains electronic client records that support registration, clinical assessments, treatment plans, progress notes, medication management, client referrals, care authorization, provider payment activities, and billing. Federal law defines an electronic signature as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.” Under California law, a digital signature is defined as "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.” “The purpose of a rendering/treating/ordering practitioner’s signature in patients’ medical records, operative reports, orders, test findings, etc., is to demonstrate the services have been accurately and fully documented, reviewed and authenticated. Furthermore, it confirms the provider has certified the medical necessity and reasonableness for the service(s) submitted to the Medicare program for payment consideration.” For the purposes of this policy, an electronically signed record is a financial, program, or medical record.

B. **Procedures:**

1. **User Agreement:** "User" includes DPH civil service, UCSF affiliates, contractors, students, visitors, volunteers, and any other person with access to data as outlined in section I.A above. Every individual user who is provided access to this data will signify (by signing the User Agreement for Confidentiality, Security and Electronic Signature form) that they understand and agree to the terms and conditions outlined on the form. Minimally, this form will be signed by users at time of hire, each time authorization to access a SFDPH 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 a SFDPH data system and/or termination of employment.

2. **Annual Acknowledgement:** All users required to take the annual DPH Compliance and Privacy Training will electronically sign the User Agreement for Confidentiality, Security and Electronic Signature in Part 2 of the Annual Compliance and Privacy Training.

3. **Attestation:** Each user will attest that they understand that looking at patient information without having a business purpose is against the law and that violation of any of the requirements set forth in this User Agreement may result in termination of their employment, reporting to regulatory bodies, and reporting to their professional board.

Last Revised/Revision Date: 1/16/2007; 3/19/2015; 2/5/2025; 3/12/2026