TITLE: REPORTING OF UNLAWFUL OR UNAUTHORIZED ACCESS OF PROTECTED HEALTH INFORMATION

PURPOSE

This document establishes the policy for the reporting and investigation of protected health information (PHI) through the collaborative efforts of DPH departments and through oversight of the Office of Compliance and Privacy Affairs. It is the intent of this policy to define and guide appropriate responses to any unlawful or unauthorized access to, use or disclosure of PHI.

STATEMENT OF POLICY

Pursuant to state and federal laws, DPH strictly prohibits inappropriate viewing of protected patient health information. This policy pertains to all individuals in the DPH who have access to, use, or disclose protected health information, regardless of DPH division or unit. This policy is administered by the Office of Compliance and Privacy Affairs. This policy shall apply to all DPH programs. DPH contractors and affiliates may use this policy as a guide, but should consult with their own counsel to ensure the necessary procedures for their agencies.

BACKGROUND

Effective January 1, 2009, two new laws provide oversight, reporting, stricter requirements and increased penalties for privacy/security breaches in the state of California. Unauthorized access is defined as “the inappropriate review or viewing of patient medical information without a direct need required for diagnosis, treatment or other lawful use” as permitted by the California Medical Information Act. Covered facilities are required to report any unlawful or unauthorized access, use, or disclosure of patient health information to the California Department of Public Health (CDPH), no later than ten days after detection by the facility or face a $100 per day fine. The legislation also authorizes the Office of Health Information Integrity (OHII) to impose fines and refer licensed individuals to appropriate boards. Law AB-211; Law SB-541

DEFINITIONS

- **A breach of PHI:** The unlawful or unauthorized access to, and use or disclosure of, “protected health information” as defined in the DPH Privacy and Data Security Policies/or “Patient’s Medical Information” as defined in the Civil Code Section 56.05(g).
- **Patients, clients, residents:** Any individual who requests or receives health services from a DPH care venue.

PROCEDURE

Date Revised: 09/10/18
I. When, in the course of routine business operations, any DPH employee who knows of, suspects, or has a question regarding a possible violation by another DPH employee or contractor/affiliate is obligated to report this information to their immediate supervisor and/or the local DPH Privacy Officer at the time of discovery. If not already notified, the supervisor is to immediately notify their local DPH Privacy Officer. **Potential breaches can also be reported to the Office of Compliance and Privacy Affairs at 1-855-729-6040 or compliance.privacy@sfdph.org.**

II. When, in the course of routine business operations, the DPH Privacy Officer is notified of a suspected or possible breach of PHI, they are to proceed with an immediate investigation. The Privacy Officer shall:
   a. Request in writing or complete in writing, all details of the violation, including dates and times, as reported and its source, including interviewing of staff.
   b. Contact the violating employee’s supervisor/manager or department director, and notify the Human Resources Department of the employee.
   c. Consult with legal counsel, Risk Management and Information Services regarding the violation.
   d. Maintain documentation of the privacy breach and complete a UO for submission to the Risk Management Department and/or the Summary of Unauthorized Access.
   e. Maintain the confidentiality of the investigation to all except the required department staff identified above.

III. The DPH Privacy Officer, or a designee, on or before the 10th calendar day after their notification of unauthorized access of PHI, shall in writing and by telephone, correspond with the California Department of Public Health (CDPH) and notify the patient(s)/patient representative(s) involved. The Office of Compliance and Privacy Affairs will also notify the Office of Civil Rights (OCR) and the Department of Healthcare Services per regulatory requirements.

IV. All correspondence, data elements and documentation for the breach of privacy shall be maintained and tracked by the Office of Compliance and Privacy Affairs.

V. Any and all occurrences of violations of patient privacy will be reported to the Office of Compliance and Privacy Affairs.

VI. All follow-up pending the CDPH and/or OHII investigation shall be in accordance with current DPH policies with the collaborative effort of the identified departments in this policy.