1. POLICY INTENT

This document establishes the policy for defining a PHI information loss, standards for protection against liability and when such a loss requires client notification. It also specifies when, prior to an information loss, the use of encryption technology and other mechanisms which render unusable or to control access to restricted information transmitted or stored by the San Francisco Department of Public Health (SFDPH) facilities and equipment is appropriate. It defines standards and guidelines for when encryption measures to protect SFDPH resources are required and what types of information, storage media and transmission modes require encryption. In addition, it provides a guide to the disclosure circumstances that require client notification and describes the various State and Federal penalties that may be imposed. This policy is intended to comply with those sections of the Code of Federal Regulations that govern HIPAA requirements and enforcement for Information Security. The sections that relate to Access Control, Data Integrity and Transmission Protection are CFR 164.308(a)(4) and 312(a)(1), (b), (c)(1) & (e)(1).

This Policy EXPLICITELY DOES NOT deal with written patient records or paper hard-copies of PHI produced from electronic data.

This policy is an extension and expansion of the Portable Device and Media and the (Interem) Enterprise Encryption policies and includes all of the provisions and requirements of those policies as part of this policy by reference.

DEFINITIONS: For the purposes of this policy –

1. “HIPAA” is the Health Insurance Portability and Accountability Act of 1996 and involves various specific requirements and guidelines regarding the custodial responsibilities of Health Organizations in regard to the confidentially and security of the information which they develop and control.

2. “HITECH” is the Health Information Technology for Economic and Clinical Health, part of American Recovery and Reinvestment Act of 2009 (ARRA) – widely considered to provide the enforcement ‘teeth’ that HIPAA lacked.

3. “Information loss” refers to electronic information that is:
In the custody of SFDPH or for which SFDPH bears fiduciary, legal or regulatory responsibility,

“Restricted Information” as defined in the Data Classification Policy and is

Formatted, transmitted, transported or stored in electronic form.

And then is lost, stolen or otherwise removed from SFDPH control in an unauthorized manner.

4. “Securely Located Drive” – refers to a network-accessed shared physical or virtual drive that is installed in a server device that is located in a physically secured facility (locked room/closet, off-site, badge required to enter etc.) that does not readily permit physical public access or easy illegal physical access (e.g., breaking and entering or burglary) to the device.

5. “At-Risk Facility” – refers to any vehicle, or SFDPH facility/Business Associate facility which both handles/stores PHI and has a history or known significant risk of theft, burglary, breaking and entering or other illegal activity (such as being located in a location designated a ‘High Crime Area’ by local Law Enforcement) potentially resulting in a loss of PHI or computer equipment.

2. POLICY STATEMENTS:

2.1 Basic Principle: Restricted Information is to be either kept on a protected medium – such as a fully encrypted disk-drive OR in a securely located and physically-protected network shared drive – such as a server in a restricted access computer center.

2.2 When an Information loss occurs and the material was not encrypted – It must be reported as required and directed under State and Federal laws and regulations; and the affected patients or clients whose information was lost must be notified of the fact of the loss and the remedial steps taken to correct the loss.

2.3 Critical Information is subject to being encrypted at any time that it meets any of the following criteria:

2.3.1 It is going to be electronically transmitted (refer to 3.1.1 below) to a destination outside of the SFDPH Data Network or it is to be physically transported (refer to 3.1.2 below) to or from physical locations outside of the facilities or control of the SFDPH.

2.3.2 It is stored on any media that is portable enough to be mislaid, lost or stolen. This specifically includes workstation hard drives (refer to 3.1.2 below), regardless of their normal location.
2.3.3 It is concerned with access control or other security measures, regardless of location or transmission (refer to 3.1.3, below).

3. STANDARDS

3.1. Devices containing Restricted Information in clear-text on a memory must be under physical control of the responsible authorized workforce members at all times. All cases where an exception to this policy is required, the exception is to be documented and approved in writing by SFDPH Operational and IT Management - the information involved is fully subject to this policy’s requirements in ALL other circumstances but those that were exempted in the written exception.

3.2. Critical Information must be encrypted under any of the following circumstances:

3.2.1. It is transmitted over any communication infrastructure not controlled by SDFP, including:

3.2.1.1. Information transmitted by any wireless means. (See Wi-Fi Policy).

3.2.1.2. Information transmitted over any public communications infrastructure including the Internet.

3.2.1.3. Information transmitted from facilities or over communications infrastructure that are not controlled by the SFDPH or from facilities in locations that are not on SFDPH property (e.g., via FTP).

3.2.2. It is to be transported - Critical Information is to be encrypted when physically taken off of SFDPH property including:

3.2.2.1. Information stored in the memory of portable computing devices such as laptop computers, Personal Data Assistants (PDA's) and multi-function communication devices such as ‘Smart Phones’ or ‘Tablets’.

3.2.2.2. Information authorized to be stored in the memory of desktop workstations (See 2.1) that are exposed to physical removal from their assigned installation location, either by authorized staff (i.e., mislaid or lost) or by unauthorized persons (i.e., stolen or improperly accessed by staff or acquaintances on shared devices such as offsite workstations, web nodes or home computers).
3.2.2.3. Information transported in removable media form such as tape, hard or floppy disk, CD ROM/DVD, flash chips/wands/cards and so-on

3.2.3. **It is Security-related** – Critical Information to be stored in encrypted form at all times includes:

3.2.3.1. Password files and access control tables.

3.2.3.2. Encryption keys for stored or transmitted data.

### 3.3. Technical Standards for Information encryption under the situations defined in 3.2:

3.3.1. When transmitted by wireless means:

3.3.1.1. For SOHO (Small Or Home Office) and Consortium locations: Non Broadcast SSID and 128-bit static WEP encryption.

3.3.1.2. For Remote Sites and Major Sites: Non-Broadcast SSID, and either

- EAP/TLS = TKIP = 802.11x. OR
- Wireless Protected Access (WPA)

3.3.2. When transmitted over public infrastructure (i.e., Internet):

3.3.2.1. For interactive applications, such as checking individual test results: Secure Socket Layer (SSL) technology.

3.3.2.2. For accessing SFDPH Network Applications: Virtual Private Network (VPN), preferably using Juniper SSL via the Juniper appliance.

3.3.3. When transmitted to/from or via infrastructure not controlled by SFDPH:

3.3.3.1. For accessing SFDPH Network Applications: Virtual Private Network (VPN), preferably using Juniper SSL via the Juniper appliance.

3.3.3.2. For file transfer: Tumbleweed FTP, using SSH, SCP or PGP protocols.

3.3.4. When stored on a portable computer: Symantic Endpoint Encryption® (SEE) full-disk version.

3.3.5. When stored on removable media: Symantic Endpoint Encryption® full-disk version.
3.3.6. When security-related critical data is stored within SFDPH facilities on a workstation Symantic Endpoint Encryption® full-disk version..

4. RESPONSIBILITIES

4.1. **SFDPH Executive Management is responsible for:**

   4.1.1. Developing, reviewing, approving and publishing I.T. policy and its associated standards and guidelines.

   4.1.2. Establishing Standards and Guidelines for the Enterprise-wide application of encryption policy.

   4.1.3. When an Information loss occurs, making a determination whether unencrypted sensitive data has been involved

   4.1.4. When an Information loss occurs and the material was not encrypted – as required under State and Federal laws and regulations; funding and directing the notification of the affected patients or clients whose information was lost of the fact of the loss and the remedial steps taken to correct the loss.

4.2. **DPH Chief Information Officer, Chief Information Security Officer (currently the SFDPH I.T. Director) is responsible for:**

   4.2.1. Reviewing and approving to management all exceptions to I.T. Security policy.

   4.2.2. Directing and overseeing the development of standards and procedures for the secure use of Information technology.

   4.2.3. Directing the development and promulgation of training and orientation materials to enable and encourage employee awareness of the security problems and issues involved in the protection from and reporting of the loss of SFDPH Restricted information.

4.3. **SFDPH Information Technology (DPH-IT) is responsible for:** Implementing Security Policy for all forms and means of processing transmission and storage of electronic information.

   4.3.1. Implementing encryption technologies as specified in this policy.
4.3.2. Providing Enterprise-wide guidelines for and technical assistance in deploying encryption technologies where needed.

4.3.3. Monitoring developments in encryption technologies and recommending changes to standards and guidelines when appropriate.

4.3.4. Recommending new or revised security policies as necessitated by changes in the regulatory or technological landscape.

4.4. **Appointing Authority / Local-Unit Management is responsible for:**

4.4.1. Identifying workforce members whose job roles require them to use encryption on the devices that they use for their assigned tasks.

4.4.2. Facilitating the installation of encryption technology on the devices and media within their area of authority.

4.4.3. Ensuring that workforce members are properly trained to use the provided encryption technology.

4.4.4. Investigating reported data loss incidents and reporting the facts through their own chain of command to Executive Management and the IT Director.

4.5. **Workforce members are responsible for:**

4.5.1. Protection of the information that has been entrusted to their care. All workforce members who come into contact with Restricted information are expected to familiarize themselves with the related Information Security policies and to consistently use it in their SFDPH business activities. Although this policy provides overall guidance, to achieve consistent information protection, workforce members will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

4.5.2. Participating in SFDPH provided Security training and orientation sessions and events, when offered.

4.5.3. Conforming to SFDPH Policies, Standards, Guidelines and Procedures and staying within their defined security roles to minimize risks to the information resources with which they work.
4.5.4. Notifying management of any loss of stored, transmitted or transported SFDPH Restricted information; and vulnerabilities to or risk factors involving the information resources with which they work.

4.6. **Incident Response Team is responsible for:** Reacting to and dealing—with reported losses or interceptions of information that fall under this encryption policy and recommending such remediation actions as seem required to prevent further similar incidents.

5. **SFDPH PENALTIES FOR VIOLATIONS** (Refer to Appendix 6.2 below for the Federal penalties):

5.1. **General Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures are subject to the same progressive discipline processes and sanctions as any other violation of the terms and conditions of employment at SFDPH.

5.2. **Individual Non-Employee and Third Party Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures by persons employed through a third party or otherwise not subject to the progressive discipline processes and sanctions of the terms and conditions of employment at SFDPH are subject to the sanctions provided under the terms and conditions of the agreement(s) whereby their services are provided.

5.3. **Trusted Workforce member Violations:** Managers, System Engineers, System Administrators and other classifications who are given greater than routine access to and control of critical information systems and data may be subject to stricter standards of security behavior and more abrupt and stringent penalties in the case of violations.

5.4. **Contractor and Third Party Entity Violations:** In addition to the individual sanctions noted in 2.1 and 2.2 above, third party organizations, business entities and others who are contractually required to comply with SFDPH Security Policies and standards may be subject to specified monetary fines or penalties or termination of the agreement as required for by the written contract and criminal penalties provided for in the applicable laws and regulations.

6. **APPENDICES:**

6.1. **Federal Disclosure Requirements:**
NOTE: the text sections 6.1 and 6.2 below are paraphrased from Search Security online magazine and are intended for information only. They do not reference the California laws upon which the Federal Statutes were modeled - these have long applied to SFDPH. No copyright infringement is intended nor is any claim of authorship made:

Under rules released August 2010 by HHS, a Covered Organization with a breach involving unsecured protected health information (PHI) must notify the affected individuals. The notifications must be provided no later than 60 days following the discovery of a breach and must include a description of the breach and what the organization is doing to investigate it, among other details. If more than 500 individuals are affected, then the organization must notify major media outlets in affected states and HHS; HHS will list the breaches and the entities involved on its website.

Organizations need to have a process to assess whether there’s been a security breach that requires notification. The security or privacy of protected health information is deemed to be compromised only if the disclosure poses a significant risk of harm to the individual. The process requires a risk assessment that considers the amount of data lost and potential exposure of that data to determine whether notification is required.

EXAMPLE: “If a folder of information is left at a bus stop and someone returns it to the organization, there may not be much risk for that patient information. Whether the organization consider this a breach or not will be based on what the information was. If the information was just a listing of names without other financial/medical identification, it may not be considered a breach because there is little risk to the patient.”

Notification IS NOT required if the PHI is unreadable or indecipherable through encryption according to National Institute of Standards and Technology (NIST) standards. Paper records must be shredded so the PHI can’t be reconstructed, and electronic media purged or destroyed per NIST guidelines.

6.2. Federal Penalties for Failure to Protect PHI:

The new law provides a tiered system of civil monetary penalties based on the level of knowledge of the noncompliant organization (from knowing to willful neglect), and corrective actions taken.

For example, if a violation was due to reasonable cause and not willful neglect, the penalty is $1,000 for each violation. But if the violation was due to willful neglect and not corrected, the penalty is $50,000.
per violation, with a maximum fine of $1.5 million for all such violations in a calendar year. Previously, the civil penalties for HIPAA security and privacy violations set a maximum civil fine of $100 per violation and up to $25,000 for all violations of an identical requirement during a calendar year.

HIPAA also provided for criminal penalties of fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intention of selling it for commercial or personal gain, or for malicious purposes. Previously, the U.S. Department of Justice ruled that a covered entity, not individuals, could be criminally liable for HIPAA violations, but HITECH makes it clear that individuals—hospital employees or others—can be held liable.

In addition, the new law broadens the number of potential HIPAA enforcers. It allows state attorneys general to file a federal civil action on behalf of residents of their states who they believe were adversely affected by a HIPAA violation.