



University of California
San Francisco

advancing health worldwide™

SOM Encryption Project Overview

*for SFGH Department of Medicine
Division Chiefs*

Department of Medicine

Tim Greer

Manager, SOM SFGH CNS

Erik Wieland

IT Director, DOM

October 6, 2009

Reminder - Reasons to Encrypt

the privacy of our patients, employees and partners is of the highest importance

- **Recent Losses (January - March 2009)**
 1. Timely reported, encrypted, no action needed
 2. Unencrypted, 331 patients notified; **potential penalty \$250K+**
 3. Timely reported, identifying IT owner took 4-6 hours; No reported sensitive data on hard drive, no encryption, **unable to verify or audit data**
- **Compliance with Federal & State laws**
 - **HIPAA** (Health Insurance Portability and Accountability Act)
 - **California Assembly Bill 211** (AB-211)
 - **California Senate Bill 541** (SB-541)
 - **California Senate Bill 1386** (SB-1386)
 - **FERPA** (Family Educational Rights Privacy Act)

Execution Plan

- **Phase 1**
 - Inventory and analysis of devices
 - Encrypt SOM owned laptops
 - Develop USB drive encryption standards
- **Continue to advocate for future phases**
 - Use audit software to locate sensitive data
 - Help users relocate sensitive data to secure servers
 - Encrypt high risk SOM desktops where data cannot be relocated
 - Encrypt personal laptops & desktops (pending policy)

Inventory Status

- **SOM Department Survey results**
 - 2981 laptops - need to confirm how many SOM owned vs. personal
 - 687 laptops to be encrypted by joint IT task force
 - 298 laptops to be encrypted by CNS (90 DOM)
 - 1996 to be self encrypted by departments (525 DOM)
 - 7097 desktops
- **Still gathering data from SOM sites and smaller divisions that have been identified**

Tasks Completed

- **Technical Standard Operating Procedures**
 - Aids departments choosing to do it themselves
 - Ensures consistency throughout SOM
- **Asset Management system**
 - Aids departments in tracking computers/assets
 - Moving forward with a small “proof of concept”
- **Completed Logistics Planning**
 - Verifying for operations and deployment
- **Software license pricing finalized with OAAIS**
 - \$78 for license and support through June 2010 (paid by Dean’s Office)
 - \$38 for annual maintenance and support beginning July 2010 (to be paid by departments)

Successful Encryptions

Department/ Group	Total # Encrypted	# Lockouts/ Resets	# HD Recoveries
MedCenter	600	30	7*
CNS	42	0	1
ISU	14	0	1
Anesthesia	38	0	1
OAAIS	140	10	2*

Current Project Risks – SFGH

- **Some Newly Identified Risks**
 - Resource Challenges
 - Staff may not have staff right skill set or capacity
 - Furloughs impact
 - Faculty might still believe encryption is not needed
- **Previously Identified Risks**
 - Encryption can take up to 10 hours (avg. is 3 hours)
 - CNS Device labor costs higher (~\$225 + \$66.95/hour)
 - Disk crashes (backups taken, spare hard drives)
 - Old systems (need to retire or replace)
 - Repetitive scheduling or unavailability

Inventory Analysis

- **CNS Encrypt**
 - CNS will detail which devices
 - Can be encrypted
 - Need to be upgraded
 - Need to be replaced
 - MSO decides what to do with the devices that do not meet the minimum requirements
 - CNS will prepare an estimate of the total cost of encryption
- **Self Encrypt**
 - ISU will provide CSCs the inventory template
 - MSO decides what to do with the devices that do not meet the minimum requirements

Example of Cost Breakdown

Step	Cost	Total
Encrypt 22 laptops that meet minimum requirements	22 * \$225	\$ 4,950
Replace & encrypt 8 laptops	8 * \$939	\$ 7,512
Upgrade & encrypt 2 laptops	2 * \$ 26	\$ 52
		\$12,464

Execution & Communication

CNS will work with SFGH Dept Managers to identify the best time line for their faculty that will be least disruptive

- **Identify dates, multiple drop off and pick up locations as needed**
- **Help with communications to faculty**
 - **Before encryption** – present at staff meetings explain what to expect
 - **During encryption** – where to pick up laptop
 - **After encryption** – where to get support if needed

Next Steps - SFGH Dept Managers

- **Get the message out to Faculty and Staff**
- **Complete SFGH laptop inventories**
- **Work with ISU or CNS on encryption plan for your department**
- **If self encrypting, ensure your IT staff have capacity and capability to perform encryption**
- **Develop encryption schedule for your department**
- **Work with CNS and ISU on issues that arise on an individual basis**

Next Steps – SFGH CNS IT Team

Step	Date
Complete SFGH laptop inventories	by Oct 31
Inventory analysis and price estimates	Sept 30 - Jan 31
Obtain final version of encryption software from ISU and OAAIS	by Sept 30
Schedule encryption work with your dept.	Sept 30 - Jan 31
Perform encryption execution	Now – June 30
QA activities with ISU	TBD
Test various encrypted USB drives	by Oct 31

Questions for SFGH Managers

- **Will your SFGH department require weekend drop off encryption service? (Friday PM drop-off, Monday AM pickup)**
- **Will your SFGH department require after-hours on-call support (6-10 PM) to assist your staff and faculty with password resets?**
- **What else can CNS and ISU do to ensure the success of this project in your department? (attend faculty meeting, staff meeting, etc.)**

Questions?

**[http://medschool.ucsf.edu/isu/
som-laptop-encryption](http://medschool.ucsf.edu/isu/som-laptop-encryption)**