



University of California  
San Francisco

*advancing health worldwide™*

# SOM Encryption Project Update

*For Department of Medicine Division  
Administrators*

Department of Medicine

**Erik Wieland**  
*IT Director*

November 2, 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) and **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 DOM owned laptops
    1. Supported laptops
    2. Unsupported 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 DOM desktops where data cannot be relocated
  - Encrypt personal laptops & desktops (pending policy)

## Tasks Completed

- **Technical Standard Operating Procedures**
  - Helps groups choosing to do it themselves
  - Ensures consistency throughout SOM
- **Asset Management system**
  - Helps departments in tracking computers/assets
  - Moving forward with a small “proof of concept”
- **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)

# Inventory Analysis

- **Divisions submit their inventories**
  - ~525 laptops in DOM, 140 supported by DOM IT
- **DOM IT details which devices**
  - Can be encrypted
  - Need to be upgraded
  - Need to be replaced
- **Division decides what to do with devices that can't be encrypted**
  - Verifiable retirement
  - Complete waiver form
- **DOM IT prepares estimate of cost of encryption**

# Execution & Communication

**DOM IT will work with you to identify the least disruptive timing for your faculty and staff**

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

## Next Steps – Division Administrators

- Get the message out to faculty and staff
- **Complete laptop inventories**
- Work with DOM IT on encryption plan for your division
- If self encrypting, ensure your IT staff have capacity and capability to perform encryption
- Develop encryption schedule for your division
- Work with DOM IT or your IT service provider on issues that arise on an individual basis

## Questions for Division Administrators

**Will your division require weekend (Friday drop-off, Monday pickup) encryption service?**

**Will your division require after-hours on-call support (6-10 PM) after encryption?**

**What can DOM IT do to ensure the success of this project in your division?**

## More Project Information

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

[http://domsupport.ucsf.edu/  
security/](http://domsupport.ucsf.edu/security/)