

Department of Radiology

Memo

Re: Departmental Laptop Use

The following is a summary of some of the major new requirements for the secure use of laptop computers within the Department. This summary is being presented to help you understand the scope of and the philosophy behind the new procedures. You should familiarize yourself with the procedures these are based on. The full texts of the procedures are located at: http://radiology.ucsf.edu/staff/hipaa_matters.shtml

- All laptops must require a password at login.
- Strong passwords must be used.
- Password hints, auto login and display of account names must be disabled.
- An auto log-out or password protected screen saver must activate after 15 minutes (or less) of inactivity.
- All sensitive information, including PHI, must be encrypted with a strong password.
- Unattended laptops must be physically secured:
 - Using a lock down cable (e.g. Kensington)
 - Secured in a locked office or locked cabinet
- If your laptop is lost, stolen or compromised (hacked or infected with a virus) report the incident to the Computer Support Help Desk at (415) 502-5838.

The Department of Radiology Computer Support Group will provide security configuration assistance and software including anti-virus software and encryption solutions. All laptops will be required to have:

- A properly configured personal firewall.
- An approved virus and/or spy ware detection system(s) with current anti-virus definitions and auto-updates enabled.
- All unused or unnecessary services must be disabled (e.g. Bluetooth, file sharing).
- The operating system auto update feature must be activated.
- Current operating system patches and security updates must be installed.