

HOW TO PROTECT THE PRIVACY AND SECURITY OF PHI AND PII UNIVERSITY OF CALIFORNIA SAN FRANCISCO

Some steps you should take to protect our patients, yourself, and UCSF:

ENCRYPTION



Do you leave your house without locking the front door? Probably not. Think of **encryption** as the lock on your front door, preventing thieves from entering your house.

- Before using your personal computer or electronic device for any UCSF business and/or communications (including UCSF email), it must be **encrypted!**
- By having your device **encrypted**, you can rest assured that the information it contains is secure and inaccessible to thieves.

Wondering how to encrypt your personal device? See below:



- **Desktop/Laptop:** If you plan to use your personal desktop or laptop for UCSF business, click here to access self-guided encryption installation instructions: <http://tiny.ucsf.edu/9bTkaB>
 - Document your personal device encryption with UCSF by submitting a [ServiceNow](#) ticket and specifying “**Encryption Documentation Request for Individuals**” in the ticket
- **Smartphone:** If you plan to access UCSF email via smartphone, you must use ActiveSync, which will automatically configure the required security settings (including encryption). Click here for guidance: <http://tiny.ucsf.edu/QweBYV>
- Contact the IT Service Desk at (415) 514-4100 for encryption assistance

PHYSICAL SECURITY



You are responsible for protecting UCSF information, including PHI and PII* stored on laptops, smartphones, iPads, memory sticks, cameras, paper documents, printed photographs, films, etc. Keep PHI in your direct possession **AT ALL TIMES**.

Locking your laptop and documents in your vehicle’s trunk or glove compartment is **NOT** secure and is a target for thieves.

REMEMBER: If your **unencrypted** personal device containing UCSF data is lost or stolen, **YOU MAY BE HELD PERSONALLY RESPONSIBLE**, with consequences up to and including termination of employment, and liability for civil fines and/or criminal sanctions.

GOT QUESTIONS?

- Review UCSF’s Encryption Frequently Asked Questions (FAQs) at <http://tiny.ucsf.edu/ZAayfD>
- Email, encryption or other security-related issues: contact the IT Service Desk at (415) 514-4100
- Privacy-related issues: contact the Privacy Office at (415) 353-2750 or privacy@ucsf.edu

***PHI:** Protected Health Information is individually identifiable health information which is created in the process of caring for the patient; **PII:** [Personally Identifiable Information](#) is an individual’s first name or first initial and last name in combination with any one or more of the following: social security number; driver license number or California identification card number; financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; medical information; health insurance information.