UCSF
University of California
San Francisco

FY15 UCSF Campus Attestation for Device Encryption

IMPORTANT: For Campus workforce, the following attestation language will apply to you in lieu of the attestation language at the end of the 2014 Privacy and Security Briefing. You will still need to click on the attestation language presented at end of the course in order to receive a completion status; however, only the following language will actually apply for Campus workforce.

I understand and acknowledge that it is my responsibility to comply with applicable UCSF data security policies and standards.

- Every device I use for UCSF business (e.g. tablets, smart phones, laptops, and other mobile devices on which information is stored), including personally owned devices, will comply with the UCSF Minimum Security Standards (http://tiny.ucsf.edu/mss), including the use of anti-malware software, using up-to-date and patched software, and physically securing my computers.
- Every laptop I use for UCSF business, including personally owned laptops, will be encrypted with an approved solution unless I have an approved waiver on file.
- Every storage device containing restricted data, including flash drives and portable hard drives, will be encrypted.
- I will report the theft or loss of any computer or storage device used for UCSF business to the UCSF Police Department at 415-476-1414 or on-line at http://police.ucsf.edu.
- I will not share my login or user ID and/or password with any other person. If I believe someone else had used my login or User ID and/or password, I will immediately change my password and report the use to the UCSF IT Service Desk at (415) 514-4100.

I may be personally responsible for any breach of confidentiality resulting from unauthorized access to data on an unencrypted device due to theft, loss or any other compromise or not complying with applicable UCSF data security policies and standards. I will contact the UCSF IT Service Desk at (415) 514-4100 for questions about encrypting my computing device. I understand that if there is any breach of confidentiality resulting from unauthorized access to data on my unencrypted device due to my failure to encrypt the device, I may be subject to disciplinary action up to and including immediate termination from my employment/professional relationship with UCSF, civil fines for which I may be personally responsible, as well as criminal sanctions.

Under federal and state laws and regulations governing a patient's right to privacy, unlawful or unauthorized access to or use or disclosure of patients' confidential information may subject me to disciplinary action up to and including immediate termination from my employment/professional relationship with UCSF, civil fines for which I may be personally responsible, as well as criminal sanctions.

By completing this training, I attest that I am responsible for the security and protection of UCSF data and will adhere to UCSF Campus Administrative Policy 650-16, Information Security and Confidentiality (http://policies.ucsf.edu/policy/650-16), including any and all future policy changes.