IT Security Update: Frequently Asked Questions—Encryption, Privacy and Data Protection

The topic of data encryption was discussed at a recent faculty meeting. These FAQs address device encryption and associated topics. Related links are also provided for additional information.

All mobile devices (laptops, phones, tablets, flash drives) used for UCSF work must be encrypted. Devices provided by the department through the IT service come encrypted, those would be laptops and mobile phones. Devices purchased for personal use and also used for work—that is, purchased privately by an individual—do not come encrypted and it is the responsibility of the individual to do this. These devices cannot be used for UCSF work unless encrypted. Question #7, below, discusses encrypted flash drives, which we ask that you use.

1. Is password protection on a laptop or mobile device (phone or tablet) the same as encryption?
   Password protection is not the same as encryption as a password can be breached, encryption cannot.
2. I know my UCSF-provided laptop is encrypted, but what about my UCSF-provided mobile phone or tablet?
   A phone provided by the department is already encrypted by ActivSync when UCSF Exchange mail access is set up. It is the same process for a tablet.
3. Can I get my personal phone encrypted?
   If you would like to encrypt a personal phone or tablet, then you need to contact the IT service desk at 514-4100 to set up ActivSync.
4. What is the process for getting personal laptops encrypted?
   If the user has a premium subscription with ITFS, then an ITFS tech can encrypt a personal device. A ticket should be placed for this request. If the user does not have a premium subscription, they can go to this link and follow the instructions for encrypting a PC laptop or contact me directly for assistance in encrypting an Apple laptop. http://it.ucsf.edu/category/its-categories/security
5. How do these encryption efforts relate to Privacy and HIPAA?
   It is the responsibility of all who work at UCSF to protect the privacy and privileged information of patients and employees. Laptops and other mobile devices can "walk away" and if they are not encrypted, all data is vulnerable.
   The Final Omnibus Rule is here!
   The Final Omnibus Rule of 2013, which amends the HIPAA rules, went into effect Monday, September 23, 2013. It includes important changes that impact multiple areas.
   What you need to know: Final Omnibus Rule Summary:
   http://hipaa.ucsf.edu/documentation/downloads/Final_Omnibus_Rule_Summary.pdf
   UCSF Medical Center has a new Notice of Privacy Practice!
   As a result of the Final Omnibus Rule changes, the UCSF Health System Notice of Privacy Practice (NPP) and Acknowledgement of Receipt Form have been updated and will be available in English, Spanish, Russian, and Chinese. Effective September 23, 2013, the updated NPP must be provided to all new patients, to patients who have recently turned 18 years of age at their next encounter, and to anyone else who requests a copy.
   Click here (http://hims.ucsfmedicalcenter.org/hippa_forms.htm) to view the current versions.
6. Should office desktop computers be encrypted?
   Office desktop computers are being encrypted with new deployments and re-imaging of devices in for service. There is no retroactive program for desktop encryption.
7. Do you have a link to order encrypted flash drives or do we create an IT ticket?

Encrypted flash drives are available through BearBuy/CDW. Encrypted flash drives SHOULD NOT be purchased through Office Max or Office Depot as these devices did not work correctly when someone tried. Follow this link for more information: https://it.ucsf.edu/how_do/buy-recommended-security-products

8. What is the process for disposing of un-encrypted flash drives?
   To dispose of an un-encrypted flash drive, delete everything on the drive and then empty the trash on the computer. Then use for personal transport of non-privileged information or give as gifts to those in need of unencrypted flash drives.
9. What about Anti-virus software? Is that available through UCSF IT Services?
   Yes: Symantec Endpoint Protection (SEP) is provided free of charge to faculty, staff, students, and researchers of UCSF. SEP is designed to detect, remove, and prevent the spread of viruses, spyware, and other security risks.

   The SEP client combines various client security technologies under a single application to help protect your computer without sacrificing performance.

   SEP provides Windows, Macs, and Linux computers with anti-virus (AV) and anti-spyware. SEP scans local hard disks and monitors file access to detect potential threats and blocks any unnecessary access until the threat has been resolved. On Windows computers, for added protection against network-related threats, SEP also provides intrusion prevention (IPS), proactive threat scanning, and personal firewall capabilities.

   In addition, the UCSF SEP clients will automatically keep both the client software and security definitions (AV and IPS) updated for the most complete protection. For more information on SEP Anti-virus software and to download, follow this link: https://it.ucsf.edu/services/symantec-endpoint-protection-sep

Related Links:

- UCSF Privacy and Confidentiality: http://hipaa.ucsf.edu/
- UCSF Information Technology Security Services: https://it.ucsf.edu/services/category/security
- Encryption information: https://it.ucsf.edu/services/encryption
- ITFS Support Team: https://it.ucsf.edu/services/it-field-services-team
- ITFS FAQs: https://it.ucsf.edu/services/faqs-field-services
- Other IT-related information: http://obgyn.ucsf.edu/deptadmin/admin/it_services.aspx/