

## LESSONS LEARNED FROM RECENT INFORMATION SECURITY EVENTS

June 2011

1. Recognize your responsibility to protect confidential information – you are personally accountable for the institutional information entrusted to you.
2. Don't take paper records containing confidential information (including personally identifiable information (PII), protected health information, protected student information, or classified information) off-site.
3. Don't place confidential information on your mobile devices (laptops, thumb drives, or smart phones).
4. If you use a mobile device to work with confidential information:
  - a. Protect the device with a strong password.
  - b. Use VPN access.
  - c. Install approved encryption software (see the IT website for guidance: [http://security.uwmedicine.org/Security\\_Tools/Laptop\\_MobileDevice\\_Encryption/default.asp](http://security.uwmedicine.org/Security_Tools/Laptop_MobileDevice_Encryption/default.asp)).
  - d. Mobile devices should be configured to automatically erase their storage after too many failed login attempts and have remote wipe capabilities enabled. Remote wiping can be accomplished in a variety of ways including integration with Microsoft Exchange and phone-specific tools like Find My iPhone and Windows Live.
5. Safeguard the physical security of paper and devices containing confidential information.
  - a. Lock them in a drawer or cabinet when not in use.
  - b. Use a cable lock for laptops, and CPUs mounted on mobile carts.
  - c. Lock the door to the room where the paper and devices are kept.
  - d. If the device resides on a mobile cart, institute reasonable controls to safeguard the cart when not in use.
6. Consult with the Information Security Program and with the Campus Security Office to learn more about effective strategies for protecting confidential information and university assets.
7. If you experience the theft or loss of confidential information, immediately contact the IT Services Help Desk by phone (206.543.7012) or email [mcsos@u.washington.edu](mailto:mcsos@u.washington.edu).