Laptop Security

Whenever a data breach occurs, more often than not, a laptop or other portable device was involved. Criminals continue to take advantage of our mistakes which include; storing sensitive information on devices, leaving portable devices unattended in public areas, and not using whole disk encryption.

Did you know that?
- A laptop has about a 1 in 10 chance of being stolen.
- About half of all laptop thefts occur in offices or classrooms.
- A high percentage of stolen laptops are never recovered.

How can you protect your portable devices and the information residing on them?
1. Don’t store sensitive information on a portable device.
   a. If sensitive information, e.g. ePHI, must temporarily be stored on a PMACS managed device, the device must be encrypted using whole disk encryption, e.g. BitLocker, on Windows devices, or FileVault, on Mac devices. It is also recommended that this security control be implemented on personally owned devices, as needed. In general, whole disk encryption is a very good idea since you will most likely, at least occasionally, have some type of sensitive information on your device.
2. Ensure that Absolute Data & Device Security, (formerly Computrace), is installed on the device. This product can be used to trace the device if it is lost or stolen, and wipe the device if necessary.
   a. In the event of a device theft or loss, immediately report the incident to the local or University police, after which you should contact PMACS about the incident.
3. Ensure that virus protection is on the device and being updated in a timely manner.
4. Ensure that security updates are installed in a timely manner.
5. Ensure that the software firewall is enabled.
6. When unattended, secure portable devices in a locked office or cabinet.
7. Traveling?
   a. When flying consider a portable device to be carry-on luggage, and don’t leave it alone even for a few seconds.
   b. Choose an inconspicuous carrying case.
   c. Don’t put the device in the trunk of a cab.
   d. Don’t leave the device in plain view when using a personal or rental vehicle, or when left in your hotel room.
8. If you must have a list of passwords and PINS keep the list separate from the device.

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo: David.Wargo@uphs.upenn.edu
For more security related information, visit the PMACS Information Security web page: http://www.med.upenn.edu/pmacs/