


Why has this concern emerged?

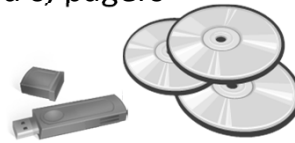
- Growing popularity, availability and lower cost related to enhanced mobile devices.
- Technology advancements that allow greater amounts of data to be stored on a single device.
- Social networking – Facebook, Google Plus and Dropbox all have used exif (exchangeable image file format) data technology.
- Easier connectivity with improved data transfer rates to the Internet.
- Simply put – we have moved from paper to electronic media for many parts of our daily lives.



What

is the definition of a “mobile device”?

- Mobile computers, smartphones and other mobile phones, tablets, iPads, personal digital assistants, calculators, portable media player, digital still/video camera, SD cards, pagers, personal navigation device (GPS), memory stick, jump drive, usb device, cd's, dvd's, pagers
- Anything that can hold data and be easily moved.



Who

offers mobile encryption software?

- Windows 7 and 8 provide Bit locker capabilities.
- Blackberry and iOS Devices including the iPhone have encryption features. Most Android devices require a third party software.
- Third party software vendors include CellCrypt, Navastream, PhoneCrypt and Text Secure.
- Detailed information on encrypting cell phones and software vendors can be found in internet searches.



Where

can I purchase secure devices?

- Staples, Wal-Mart, CDW all have secure devices in stock.
- Kingston Data Traveler 4000 Managed, Kanguru Defender 2000, and CMS CE-Secure Vault FIPS are certified to Level 2 of the government's FIPS 140-2 security standard. Imation Defender F200 is Level 3 certified and Apricorn Aegis Secure Key is being processed for Level 3 certification.
- PC World has a comparison chart available that was published last month at this link:
http://images.pcworld.com/images/article/2012/05/07r_r1_chart-11363275.jpg



How

else can we show compliance?

- A simple policy requiring encryption of all data should be considered; the policy should address owned and non-owned mobile devices and use of customer devices.
- Annual education of staff with competency testing is recommended.
- Antivirus software should be installed on mobile phones.
- Bluetooth connections should be turned off.



When

is the deadline?

- HHS does not address specific mobile device or encryption requirements.
- September 23, 2013 is the effective date for the breach notification changes related to encryption.



Question and Comments

- Please feel free to contact me to discuss any security issue.
- Linda Bower
- SecurityOfficer@mhc.net
- 231-935-7619

