



Desktop Security

- Soumitra Sengupta, CUMC Information Security Officer, spoke about a recent incident where patient records were compromised by an employee for profit.
- NYPH responded appropriately and adhered to the Privacy Breach Notification Act, contacting the government and those individuals whose personal information was compromised.
- Some internal applications are not currently encrypted but should be.
- Social Security numbers should not be used unless absolutely necessary; however there are instances when they must be used for billing, patient transfers etc.
- Employee records are often scanned and saved as PDFs without sensitive information being removed, even though it is not needed in that format.
- All System Administrators must make sure that computers in their department are secured.
- Many systems aren't password protected but should be – including those in labs, etc.
- Kiosk systems that are available for public use must be locked down to insure that sensitive information isn't stored on the computer.
- CUMC IT owned public systems in labs and classrooms will be managed by the Bradford tool in the near future to require login via UNI or NetID.
- Employees who change departments or leave must have old accounts deactivated and their computers' hard drives wiped to protect data. It is not secure to allow others in the previous department continue to use the former employee's accounts and computer.
- Unmanaged systems are risky; all computers should have competent IT staff managing them.
- As unmanaged systems are discovered, Network Security may contact those that are financially responsible for the system and advise them about securing the computer.
- Splitting up subnets by department is not feasible since staff in many departments can be spread among a variety of buildings and locations.

Update on CFI Dell Program

- One model is almost ready for purchase, it is pending a quote from Dell.
- D430 and D360 models are still being tested and prepared.
- All three should be available to order in mid May.

iPhones and Wireless

- Morningside has an agreement with AT&T and is able to offer iPhones for staff.
- iPhones are not compatible with the CUMC wireless network; authentication protocols on the phone are currently non-standard.
- iPhone software is not yet compatible with Exchange – this is still in beta testing.
- There is no specific PDA OS or model that is supported at CUMC. Sen reminded all that wireless protocols are relatively new and standards are still being settled, much as Ethernet in the 1980s.