The Basics of Protecting Electronic Personal Health Information

Greg Nance - CISSP, CRISC, CISA, ITIL
Information Security Governance, Risk & Compliance
Why do we need to protect PHI?

• Protected Health Information (PHI) is regulated by the Office for Civil Rights and we are required by law to protect it (HIPAA regulations)

• Inappropriate disclosures of PHI may cause harm to our patients, lead to fines/sanctions, and damage the reputation of the university
What are the requirements for protecting PHI?

- Information Security Policy requirements align with regulatory requirements: [http://regulations.utah.edu/it/4-004.php](http://regulations.utah.edu/it/4-004.php)

- Specific requirements for the handling of PHI are found in the Data Classification and Encryption Rule [http://regulations.utah.edu/it/rules/Rule4-004C.php](http://regulations.utah.edu/it/rules/Rule4-004C.php)

  - Encryption of PHI is required in a manner that supports the burden of proof in accordance with applicable state or federal safe harbor guidance
What do you need to do to protect PHI?

• Do not store PHI on your personal laptop or other personal electronic devices

• Store and transmit PHI using only approved means
  • Ubox
  • Email with “PHI” in subject line

• Do not send PHI to your personal email account
  • Auto-forwarding email to a personal account is not allowed

• Do not take photographs of patients using your personal device
Things to keep in mind...

- It is easier than you may realize for malicious actors to compromise your personal computer
  - Sometimes malware can infect a computer visiting reputable websites, so keep your computer patched
- Exercise caution with any suspicious email you receive
  - Send suspicious emails as an attachment to phish@utah.edu
  - Contact the information security office with any questions at iso@utah.edu
- You can also call the ITS helpdesk with questions at (801) 587-6000