Information security and research

Kevin Hardcastle
Washington University School of Medicine in St. Louis
Information Security and Research

Kevin Hardcastle
Information Security Officer
Washington University School of Medicine
June 6, 2012
How does regulations impact YOU?

• Understand exposure to PHI
• Appropriate Access is granted
• Protect PHI
• “Transport” of PHI
• Understand how you can share PHI
• Report any suspected problems where you are working
HIPAA & Research – What’s New?

• More HITECH
  • Consents for research
  • Data Breaches

• Encryption Policy
HITECH: Accounting for Disclosures

- **HIPAA Privacy Rule Accounting for Disclosures**
  
  *Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule*, published May 31, 2011 contains provisions that, if enacted, will:

  - Eliminate accountings for research disclosures
  - Require access reports for electronic designated record sets, including access for research purposes, which would:
    - Go back 3 years
    - Include the following information:
      - Date and time of access
      - Name of person or entity making access
      - Description of information access, if available
      - Description of action by user, if available
FISMA Applicability to Research

- All information systems, electronic or hard copy which contain federal data need to be protected from unauthorized access. This applies to information associated with NIH grants and contracts.

- FISMA applies to grantees only when they collect, store, process, transmit, or use information on behalf of HHS or any of its component organizations.

- If grantees retain the original data and intellectual property of the research we do not need to be compliant with FISMA.
Common Rule: ANPRM Potential Privacy Changes

  - Jointly issued by the Office of the Secretary, HHS, and FDA
  - Only a proposal at this time
  - If changes accepted, implementation still a year or more away
ANPRM Potential Privacy Changes

- Aligning standards on what constitutes individually identifiable information, limited data sets, and de-identified data with HIPAA
- Biospecimens may be determined to be individually identifiable information due to advances in genomics
- Establishing data security, information protection, and data breach notification standards similar to HIPAA
- Eliminating IRB responsibility to determine adequate provisions to protect privacy of subjects and confidentiality of data.
Local Issues

• Unsecured and/or Loss of ePHI
  • Misplaced Flash Drives
  • Lost and/or Stolen Devices
  • Unmarked box of PHI for shredding thrown away by housekeeping

• Unauthorized Access of ePHI
  • Using clinical systems for personal use versus business need
  • PHI mistakenly posted on Facebook

• Unauthorized Disclosure of PHI
  • Discussion of patient’s history in public area in front of other patients
Services offered by Information Security

- Security Risk Assessments for IRB
- Contract review for Government requirements
- Incident Management
- Provide training and encrypted USB drives
- Track all the regulatory changes and determine impact
Contact Information

Mike Caputo  314 747 4343

Kevin Hardcastle  314 362 0735

Sondra Hornsey  314 747 4975

Security Incidents and Questions to infosec@wusm.wustl.edu

Privacy Questions to hipaa@wusm.wustl.edu
Questions?