
University of Kansas
Medical Center

**HIPAA Security
&
Human Subjects Research**



Office of Compliance

November 16, 2006

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- A little background...
 - Privacy Rule
 - Effective April 14, 2003
 - Security Rule
 - Effective April 20, 2005
 - Assessment & interviews leading up to the compliance deadline

Information Protected Under HIPAA

- Protected Health Information (PHI) and electronic PHI (ePHI)
 - Information about an individual's past, present or future health, healthcare or payment for healthcare
 - Combined with at least one of 18 identifiers
 - ePHI is PHI in an electronic format

Security Rule Basics

- Implement administrative, physical and technical safeguards
- Protect ePHI created, received, stored and transmitted by KUMC
- Ensure the confidentiality, integrity and availability of ePHI

HIPAA Security and the Researcher

- At KUMC, compliance with the HIPAA Security Rule rests jointly with the institution and the principal investigator (PI)
- Consider HIPAA security when:
 - Creating, using and receiving ePHI
 - Accessing ePHI
 - Storing ePHI
 - Transmitting ePHI
 - Disposing of ePHI

Creating, Using and Receiving ePHI

- Requires *prior* approval from the Human Subjects Committee (HSC)
- Submit collaborative research involving ePHI from another institution to the KUMC HSC
- Special procedures exist for collaborative research between KUMC and KU-Lawrence
- ePHI may be received under a Data Use Agreement (DUA) or a Business Associate Agreement (BAA)

Examples

- Touch-screen health assessments
- Identifiable data set received electronically under a DUA
- Data entered into a spreadsheet

Using Existing Data for Research

- Retrospective chart review of electronic medical records
 - Qualifies as research and requires prior HSC approval
 - Requires appropriate access
- Creating research databases from clinical records
 - Used by several departments/campuses
 - Requires HSC approval and consent
 - Future use can be fairly broad within the description
- Receiving coded or de-identified data
 - Register with HSC, but no consent

Accessing ePHI

- Ensure ePHI is accessed only by authorized research personnel for approved projects
- PI is responsible for administering and managing role-based access to ePHI
 - *Information Resources (IR) can help with this*
- PI is responsible for ensuring ePHI is password protected and for password management
 - *IR can help with this*

Examples

- Changes in study personnel
- Office Space (i.e. shared drives)

Storing ePHI

- Store ePHI with only the individual identifiers minimally necessary to support the research
- Store ePHI on network drives (G:, K:, Q:, etc.)
 - Authentication, intrusion detection, patch management, virus protection, disaster recovery
- Mobile devices
 - Temporary storage; require security protections
- Stand-alone computers and sponsor-provided laptops must be approved by IR

Examples

- Laptops and kids
- PDA and Jimmy's Jigger
- "I love you"

(Sure I do, but I'm talking about the virus.)

Transmitting ePHI

- ePHI transmitted into or out of KUMC must be encrypted
 - Dedicated line, virtual private network (VPN), encrypted Web site, secure file transfer protocol (secure FTP)
 - Electronic storage media (e.g. disk, CD, DVD) must be password protected
- Email communications containing ePHI
 - Within KUMC and between KUMC-KC and KUSM-Wichita are secure using Groupwise
 - Between KUMC and KU-Lawrence or others requires encryption; Groupwise can do this; ask IR

Examples

- Research personnel in KC and Lawrence
- It's in the mail

Disposal of ePHI

- Sanitize equipment prior to disposal or re-use
 - Coordinate disposal and/or re-use through the KUMC Environmental Health and Safety Office
- Remember to follow requirements of study grants or contracts
- Follow the KUMC records retention policy

Example

- Here's your “new” computer

Reporting Breaches in Security

- Inform the Human Subjects Committee office
 - HSC will coordinate review of the breach by HIPAA and IR personnel
- Sanctions may be applied

Upcoming Security Week Events

- **Have You Seen My Laptop? How to Protect Yourself in a Mobile World**
 - 11:30 a.m. – 12 p.m.; Friday, Nov. 17; B018 SON
- **Identity Theft: When Bad Things Happen to Your Good Name**
 - 12:10 – 1 p.m.; Friday, Nov. 17; B018 SON

Questions and Contacts

QUESTIONS?

■ Contacts

- Karen Blackwell, Director-Human Research Protection Program & Privacy Official 8-0942
- Tom Field, Manager-HIPAA Compliance, Compliance Education & Outreach 8-0940
- Sherry Callahan, Director-Information Security & Security Official 8-0966
- HSC Office 8-1240