



To Heal. To Teach. To Discover.

HIPAA and Clinical Research

2011 Training

Jennifer Edlind, UH Privacy Officer

Ryan Terry, UH Information Security Officer





Be the Difference.



Agenda

- Research credentialing overview
- HIPAA Privacy and Security Rules
- HITECH Act
- Case studies
- Next steps
- Questions

UH Research Credentialing

- Goal: Provide access to patient records for research
- UH-based title
 - *Research Faculty* – Ph.D. researchers at CWRU
 - *Research Associate* – all others
- UH log-in and email account
- Free access to UH-sponsored research training programs

Credentialing Process Checklist

- ✓ Employment or affiliation with a participating institution (CWRU SOM, VA, Metro, or Ursuline)
- ✓ Participation in valid research project
- ✓ Sponsorship of Department Chair
- ✓ Complete the HIPS modules on the CITI website
- ✓ Completed application & business associate agreement (“BAA”)
- ✓ Criminal background check
- ✓ HIPAA compliance training

HIPAA Privacy Rule & Research

- Key points about HIPAA and research:
 - Applies in addition to Common Rule and FDA regulations
 - Requires approved purpose for use or disclosure of protected health information (PHI)
 - Permits research with IRB/RPB approval
 - Generally requires patient authorization, unless exception or waiver
 - Use or disclosure of data limited to terms of protocol and authorization
 - Does not apply if data is de-identified

HIPAA Privacy Rule & Research

- Key points about research authorizations:
 - Patients must sign authorization before PHI is used or disclosed
 - Exceptions:
 - Waiver or alteration of authorization
 - Activities preparatory to research
 - Research on decedents' information
 - Limited data sets
 - De-identified data sets
 - Minimum necessary standard applies unless authorization is obtained

Key Points About Data Identifiers

- The HIPAA 18

Names	Account numbers
Geographic information smaller than a state (except first 3 of ZIP)	Certificate/License numbers
All elements of dates (except year) relating to individual	Vehicle identifiers, vehicle license numbers, serial numbers
Telephone numbers	Device identifiers, serial numbers
Fax numbers	Web Universal Resource Locators (URL's)
E-mail addresses	Internal Protocol Numbers (IP's)
Social Security numbers	Biometric identifiers
Medical record numbers	Full face or comparable images
Health plan beneficiary numbers	Any other unique identifying numbers, characteristics or code (may assign unique code if key kept separate)

De-Identified vs. Limited Data Sets

- De-identified data: all 18 identifiers removed
 - Safe harbor method
 - HHS creating new guidance on de-identification standard
- Limited data sets: remove all identifiers except
 - City, State, ZIP code
 - All elements of dates (DOB, admission/discharge date)
 - Any other unique identifying number, characteristic or code
- Limited data sets may be disclosed for research purposes with data use agreement

Practical Applications

- Research databases
 - Current HHS interpretation: creating research database/repository and future unknown use of data are separate research activities
 - Challenge for clinical trials that also include creation of biospecimen storage
 - Awaiting new regulations from HHS
- Data mining for potential research projects
 - Requires prior patient authorization or IRB/RPB approval or waiver

Practical Applications

- Pre-screening process
 - Submit form with protocol submission detailing what data is needed
 - Follow protocol enrollment instructions
 - Until subjects enrolled, no use or disclosure of data outside IRB-approved study team
- Contracting with third parties to provide data hosting or analysis
 - May not provide identifiable data without prior written approval from UH and business associate agreement or data use agreement

HITECH Act (2009)

- Significant amendments to HIPAA
- New breach notification rule
 - Report breaches of unsecured PHI to patients within 60 days
 - Report to HHS and (potentially) the media
- Revised enforcement rule
 - Penalty amounts significantly increased
 - Individual criminal liability permitted
 - State Attorneys General may enforce
 - Mandatory HHS audits

Be the Difference.

HITECH Penalties for Entities/Individuals

Type of Offense	Minimum Per Violation Penalty	Aggregate Annual Penalty Cap
No actual or reasonable knowledge of violation	\$100	\$25,000
Reasonable cause of violation	\$1,000	\$100,000
Willful neglect with correction	\$10,000	\$250,000
Willful neglect without correction	\$50,000	\$1,500,000

HIPAA Security Rule & Research

- Key goals of information security are to
 - Assure the confidentiality, availability and integrity of sensitive data, including PHI
 - Assure the environments are free from virus or malicious activity
- Privacy and information security go hand in hand
- Today's focus is on electronic storage and access of PHI for research

Information Security & Research

- UH and CWRU are committed to providing secure access to PHI for research
- Joint project underway to create network architecture to protect patient/research data
- Key components:
 - Encryption for mobile devices
 - Secure access to UH network
 - Secure transfer of PHI for research

Your Role in Information Security

- Need to inventory existing research data repositories at CWRU
 - Databases, spreadsheets, etc.
 - Network/personal servers
 - Personal devices/back-up copies
- Information will be used by UH/CWRU to design new structure and safeguards
- Report to HelpDesk@uhhospitals.org
 - Include location and approximate number of records

Case Studies: UNC (July 2009)

- Breach caused by hacker accessing Carolina Mammography Registry database
 - Contained 163,000+ participants' personal information, including Social Security numbers
- Investigation revealed viruses dating back to 2007
- Consequences for the principal investigator were pay cut and demotion
- UNC found PI negligent for failing to properly secure data and obtaining PHI from UNC Hospitals without appropriate permissions

Case Study: UCLA (April 2010)

- Former researcher received 4-month prison sentence
- Researcher accessed medical records of colleagues and celebrities
- Pleaded guilty to 4 criminal misdemeanor counts of violating HIPAA
- No evidence of improper use or attempt to sell the information
- First example of jail time for HIPAA violations

Case Study: Univ. of Florida (May 2010)

- Breach notification case involving 2,047 patients in IRB-approved study
- Pediatric participants' Social Security number and Medicaid numbers included on mailing labels for study mailing sent by vendor
- Participant information also provided to telephone survey vendor inappropriately
- Notifications to individuals required by federal and state law

What to do?

- Encrypt mobile devices – (handhelds, UH laptops)
- Complete the data use/storage sections of the UH IRB
- Secure network access for non-UH assets:
 - <http://myapps.uhhospitals.org>
- Identify data sources to HelpDesk@uhhospitals.org
- Obtain UH network id (part of credentialing)
- Use UH e-mail only for PHI - @uhhospitals.org
- Contact UH Help Desk for lost/stolen devices or security incidents:
 - (216) 844-3327 or helpdesk@uhhospitals.org
- General questions or need help email InformationSecurity@uhhospitals.org



Be the Difference.

Questions?

Jennifer Edlind

(216) 767-8226

Jennifer.Edlind@uhhospitals.org

Ryan Terry

(216) 767-8512

Ryan.Terry@uhhospitals.org