

# Incorporating Security Practices to Research Data in Light of HIPAA and ANPRM

October 10, 2012

Research Administrators Forum

Ajay R. Vyas, Esq.  
Office of Compliance

# Today's Discussion

- Review of HIPAA/HITECH and CA Privacy Laws impact on Research
- ANPRM related to Common Rule
- Examples of Sound Security Practices when handling Research Data

# Privacy Laws Overview

- HIPAA Privacy
  - Protects use/release of protected health information (i.e., identifiable health information)
  - “Protected health information” includes any identifiable health information relating to the health of an individual, the care provided or payment for care – in any form
  - Administrative, physical, technical safeguards required to protect PHI
  - Went into effect April 2003

# HIPAA Privacy Rule

- PHI may be used:
  - To treat the patient
  - To get paid for care provided
  - For healthcare operations
- All other uses generally require patient authorization (specific written consent)
- Notice of Privacy Practices

# Use of PHI for Research

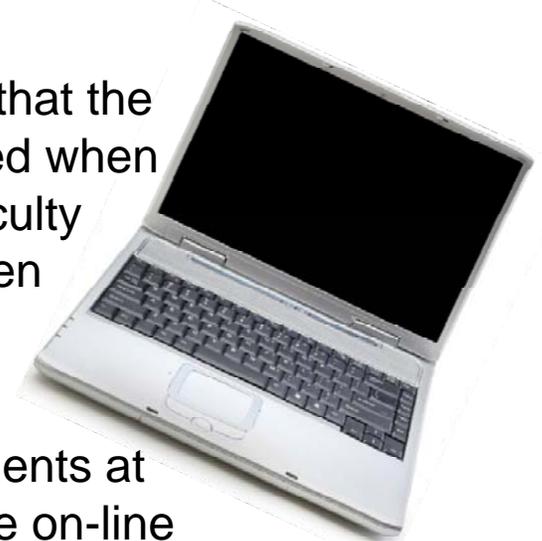
- Patient authorization required to use PHI for research
- Authorization must contain certain elements to be a valid HIPAA authorization
- Exceptions:
  - IRB Waiver
  - Limited Data Set
  - Preparatory to research (limited exception)
  - Decedents research

# California Laws/HITECH

- Similar restrictions on healthcare providers, but more strict than federal law in certain areas (mental health, HIV tests)
- Duty to prevent unlawful use/release of health information – See former UCLA Researcher sent to jail for accessing fellow colleagues PHI.
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Expands HIPAA – creates breach notification requirement
  - 2011-2016: Financial Incentives for meaningful use of an Electronic Health Record
  - Increased Penalties for HIPAA Violations; criminal liability

# Straight from the Headlines

- In November 2011, UCLA Health System announced that the health information of 16,288 patients was compromised when the home of a physician that worked for the UCLA Faculty Practice Group was burglarized and a laptop was stolen containing the patient health information.
- In September 2011, it was discovered that 20,000 patients at Stanford Hospital had their health information viewable on-line for nearly a year when a detailed spreadsheet provided to a billing contractor was posted on a public website. Class action lawsuit has been filed seeking \$20 million in damages.
- DHHS announced a \$1,000,000 Resolution Agreement Massachusetts General that stemmed from the loss of PHI of 192 patients after an employee had left hard-copy records containing PHI that included sensitive records discussing patients' treatments for HIV/AIDS on a subway.



OSTP and HHS releases “*Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay and Ambiguity for Investigators*” in July 2011

- Address concerns about IRBs review of *informational risk*, or those risks related to unauthorized release of research subject data, with the goal of balancing the protection provided by IRBs to human subjects with the progression of research.
- Seeks to extend HIPAA Privacy and Security Standards to all investigators in effect treating investigators as “covered entities” (Individually identifiable health information; Limited Data Set; De-identification of health information)
- **Potential Implications of applying HIPAA Standards to Research could result in increased administrative burden to the Research Administrator (e.g., biorepositories, data use agreements)**

# Best Practices in Handling Research Data

- **USC Research Administrators should always be mindful of security and use discretion and common sense in dealing with research data.**
- **USC Investigators should not sign Data Use Agreements without consulting with OOC to ensure appropriate protections are in place.**
- Use encryption, passwords and other security devices to protect the security of information stored on computers, laptops, flash drives and mobile devices.
- Keep your passwords stored in a secure location, and never share your passwords.
- Log-off or shut down your computer if you will be away from your workstation for an extended period of time.
- Ensure that your workstation uses appropriate screen savers, particularly if you are located in a high traffic area.
- As a general rule, do not remove research data from the premises. If removal is necessary be sure that the information is encrypted or otherwise secured to prevent unauthorized use or access.

# Want to know more?

- USC's HIPAA privacy and security policies and procedures are available on the USC policies website at [www.usc.edu/policies](http://www.usc.edu/policies) or the USC Office of Compliance website at [ooc.usc.edu](http://ooc.usc.edu).
- Review Research 300 series for Policy on Research, Research Authorization, Data Use Agreements

University of Southern California

USC

USC Office of Compliance

USC Compliance Plan PDF  
Help & Hotline  
Compliance Resources PDF

[A resource for navigating university rules, regulations and ethical expectations]

SEARCH GO

RESEARCH COMPLIANCE HEALTHCARE COMPLIANCE PRIVACY & SECURITY CONFLICT OF INTEREST ETHICS AT USC

**RESPECT** A compact with our work, our clients and each other

**HIPAA PRIVACY EDUCATION PROGRAM**  
The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of individually identifiable health information. This program will familiarize you with the law and its mandates.

**GRANTS MANAGEMENT EDUCATION PROGRAM**  
The university offers a grants management education program to help you navigate the complexities associated with sponsored research. Registration and other supplemental materials are available here.

**HEALTHCARE COMPLIANCE EDUCATION PROGRAM**  
USC provides employees with comprehensive healthcare compliance education that enables them to discharge their responsibilities effectively. Learn more about the resources we make available.

**INFORMATION SECURITY EDUCATION PROGRAM**  
This is a quick refresher on how faculty, staff and students can secure the information they create, receive and otherwise maintain as part of their job responsibilities.

CONTACT US | STAFF | GET ADOBE READER | OUTLOOK 2010 WEB ACCESS