Human Subjects Protection Workshop: Data Security and Reporting Adverse Events

Emily Anderson, PhD, IHRP

Charles Hoehne, CIP, OPRS

May 17, 2011 10 a.m. to Noon
561 Westside Research Office Bldg.
1747 West Roosevelt Road

Investigator CEs: 2

Housekeeping Notes

Please complete the registration form and return it to me so OPRS can give you investigator Continuing Education Credit for attending this presentation.

Topics

- HITECH Act / Appendix M
- School of Public Health as a Covered Entity
- Email Encryption
- Data Encryption for Portable Devices
- REDCap Overview
- Data Security Cases
- Adverse Event Reporting
- Adverse Event Cases
- Open Discussion / Questions and Answers

HITECH Act and Appendix M: Research Data Security Plan

Reminder- This has always been true:

Researchers are:

- the guardians of the subjects' privacy and confidentiality.

- responsible for the safe keeping of the research subjects' data, whether it is on a desktop, laptop, a disc, thumb drive, or other.

Appendix M – Research Data Security Plan

- In response to the HITECH Act (of October 2009)
- Builds upon HIPAA Privacy and Security
- Note: Most breaches of confidentiality are inadvertent.

Appendix M – Research Data Security Plan

- Goals (2):
  1. Establish a national health care infrastructure for electronic medical records; and
  2. Provide incentives for implementing electronic records.

Appendix M – Research Data Security Plan

HITECH Act applies to:

1. All Protected Health Information; and
2. Sensitive and highly sensitive data

Sensitive Information:

- Information that if disclosed or modified without authorization would have severe or serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.
  - Assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information
  - Covered by federal and state legislation, such as HIPAA, **FERPA**, or the Data Protection Act
  - Payroll, personnel and financial information

Sensitive Information in a research setting- Examples:

Individually identifiable information involving:

- Use or treatment for alcohol or drugs
- Illegal conduct or arrest record
- Sexual attitudes, preferences, or practices
- Psychological or mental health information
- Disclosure of information outside of research that could reasonably cause discrimination or stigmatization, or result in damage to subjects' financial well-being, employability, or reputation.
- AIDS, sexually transmitted diseases, Alcohol/substance abuse, or mental health.

Appendix M – Research Data Security Plan

- A work in progress!
  - Tech Team (basically IT personnel from the health sciences colleges + east side of campus) meeting weekly.
  - Each IRB will have IT representation.
  - FAQs being developed with ACCC and will be posted very soon on OPRS web-site.
- Intent is to help investigators think through their data security process

Appendix M – Research Data Security Plan

Initial Review:

- Application revised to collect additional information on the data security plan.

Continuing Review:

- PI must submit a new appendix, *Appendix M*, focused on data security measures at their next continuing review.

Amendments:

- Include Appendix M if amendment impacts data security.

Appendix M – Sections I and II

- Section I: Research Title
- Section 2: Identifiable Elements
  - Mirrors 18 HIPAA identifiers (PHI)

Section III: Source and Data Collection

Section A: Types of data being collected

- Not just PHI collected via medical records
- Other examples:
  - Interviews/questionnaires
  - School records
  - Internet research data

Section III: Source and Data Collection

Section B: Type of Identifiers

- Spectrum: No IDs – Coded - Direct IDs

Section C. Electronic Data Collection (via Internet or other electronic means)

- Free Version of SurveyMonkey (or similar) is NOT considered to be secure.
- If using encryption software must be “NIST” (National Institute of Standards and Technology) compliant. OPRS/ACCC will develop a list: Consult with ACCC

Section IV: Data Security and Management

Section A: What format (paper, electronic, stored specimens, recording media)

Section B: How will data be stored & secured?

Sections for:

1. Electronic data
2. Hardcopy data, recordings & specimens
3. Portable devices (note: most breaches here)

Section IV: Data Security and Management

Section C: Data Sharing- Who will have access to the data and how?

- Includes HITECH Act specified data transfer methods:
  - Overnight courier
  - US Postal Service
  - Transmitted over a secure network
  - Transmitted over a public network (must be encrypted)
  - Via email (must be encrypted) – More later!
  - Note: Telefaxing of identifiable data is NOT allowed.

Section IV: Data Security and Management

Section D: Plans for data/specimen retention/disposition

- Several specified methods are listed (Goal: lead PIs down the right path)

Final Data Security Remarks

- Data Security Plan is a work in progress at UIC
- Effective October 2009, so we cannot delay
- Many challenges for PIs and IRBs
  - PIs need to communicate at the departmental level
  - IRBs will have “tech support”
- While this is being sorted out- IRBs will be encouraged to use a compassionate common sense approach.

School of Public Health as a Covered Entity

UIC SCHOOL OF PUBLIC HEALTH
UNIVERSITY OF ILLINOIS AT CHICAGO

Six UIC Health Science Colleges:

1. School of Public Health
2. College of Medicine
3. College of Pharmacy
4. College of Applied Health Sciences
5. College of Dentistry
6. College of Nursing

What is a "Covered Entity"?

As per HIPAA, a Covered Entity (CE) is a:

- Health care plan (HCP)
- Health care clearing house- public or private entity such as a billing agency that processes or facilitates processing of health information
- Health care provider that transmits any health information electronically for HIPAA covered transactions

So what?...

Remember: It is the unauthorized release of Protected Health Information outside of the covered entity that will get you in trouble!

The nature of SPH research is evolving…

The line between Biomedical and S-BS Research is blurring, examples:

- Center for Clinical and Translational Science (CCTS) / Community-Based Participatory Research
- Genetic testing
- Data and sample banking

School of Public Health as a Covered Entity

Advantages:

- Promote collaboration between the HSC
- Reduce need to release data outside of the UIC CE.

Disadvantages:

- Some SPH research MAY now be subject to HIPAA and HI-Tech Act
- More Training required (HIPAA Research Training)

Email Encryption

Question: If the IRB required you to encrypt emails, could you?

- No campus-wide solution at this time.
- Tech team is working on it.
- IRB will not require email encryption until campus-wide solution is in place.

Email Encryption

If encryption is not possible, then what?

- PIs must be creative:
  - Send coded data and master list separately.
- Bottom Line: Stay tuned on this one-
  - OPRS Newsletters
  - Emailed announcements from OPRS Director or VCR

Data Encryption for Portable Devices

- Reminder: Most breaches occur via portable devices.

- Encryption software must be “NIST” (National Institute of Standards and Technology) compliant.
  - If buying a commercial product, include a copy of the packet insert with your application.
  - OPRS/ACCC will develop a list of acceptable software.
  - Consult with ACCC:

    ACADEMIC COMPUTING AND COMMUNICATIONS CENTER

    Interim Co-Director

    Cynthia E. Herrera Lindstrom
    2257A SEL MC 135 **T** 312-413-2495
    cynthiar@uic.edu

Research Electronic Data Capture (REDCap) Overview

- Secure, web-based application for building and managing online databases for the collection and entry of research data.

- Fast and flexible with an easy to use design environment to create data capture forms.

REDCap Overview

REDCap is a CCTS-managed product.

- It is offered as a free service to UIC health investigators, faculty, and staff.
- To learn more about REDCap, visit: http://www.redcap.ihrp.uic.edu/.

REDCap Overview

- Capabilities include:
- Building web-based databases quickly and securely
- Data collection, entry and tracking
- Extensive controls for user rights settings
- Exporting data to common data analysis packages such as Excel, R, SAS, SPSS and STATA

REDCap Thoughts

- Great potential to address many data security issues.
- May not be the answer for *all* research:
  - Surveys with complex skip patterns
  - “Non-Health Related” research?
- If used, provides IRB with a sense that data is secure.
  - Fewer questions
  - Faster time to approval

Case Study: What are the data security considerations?

Emily Anderson, PhD

Data Security Considerations: Case 1

An investigator proposes a longitudinal study of several thousand young adults (18-25) who are heavy drug users, “recreational” drug users, and non drug users:

- A lot of contact information will be collected in order to ensure retention, including social security number, Facebook and email addresses, phone numbers of relatives and friends, name of employer or educational institution.
- Names and contact information will be stored separately from study data.

Is password-protection enough or is encryption needed?

Other recommended best practices?

Data Security Considerations: Case 2

An investigator proposes to conduct an online survey of college student physical activity habits, using the Survey Monkey program.

- Participants will be invited to complete the survey from a link posted on the home pages of various universities.
- The survey will be anonymous, and no sensitive information will be collected.

Is password-protection enough or is encryption needed?

Other recommended best practices?

Data Security Considerations: Case 3

An investigator proposes to conduct an experimental study looking at the cognitive effects of smoking tobacco and drinking alcohol in young adults.

- Participants will be recruited using CraigsList; interested individuals will be directed to an online screener that uses the Survey Monkey program.
- The screener will collect names and email addresses so that eligible individuals can be contacted to come to an in-person study, and includes a number of sensitive questions (alcohol and drug abuse and history of mental health diagnoses).

Is password-protection enough or is encryption needed?
Other recommended best practices?

Data Security Considerations: Case 4

An investigator proposes to test an intervention using physician assistants to improve diabetes management among older adults.

- This is a multi-site project, and data collected will include medical records data.
- The investigator would like all data to be entered directly from the institution into a secure database.

Is password-protection enough or is encryption needed?

Other recommended best practices?

Data Security Considerations: Case 5

An investigator proposes to conduct a household survey on health and employment in low-income housing in Chicago.

- The survey will be administered in-person in participants' homes by trained staff who will enter information directly into laptop computers.
- Households will be pre-selected; participant names will not be collected, but addresses will be linked with the survey data.

Is password-protection enough or is encryption needed?

Other recommended best practices?

UIC Prompt Reporting Requirements

Chuck Hoehne, C.I.P.

Prompt Reporting Policy and Procedure: Three Key Goals:

1. To increase the reporting and capturing of **internal** adverse events determined by the investigator to be **unanticipated** and **related** to the research.

2. To enforce a restrictive reporting of external adverse events so that the IRB can concentrate on the most important events.

3. To capture other events that affect patient safety and non-compliance.

Desired Outcome

- In this way, the IRB can have a defined focus and be aware of and act on the most relevant and important problems and events.

Examples of Problems or Events that Require Prompt Reporting

- Adverse Events or Adverse Effects:
  - Internal adverse events determined by the investigator to be unanticipated and related to the research
  - External adverse events determined by the investigator, sponsor, coordinating center or DSMB/DMC to represent an unanticipated problem (i.e., unanticipated, related, and increased risk of harm)
  - Changes to the protocol made without IRB approval to eliminate apparent immediate harm to subjects
  - Unanticipated adverse device effects

Examples of Problems or Events that Require Prompt Reporting

- Non-Compliance
  - Breach in confidentiality
  - Incarceration of a subject in a protocol not approved to enroll prisoners
  - Protocol violations that cause harm to subjects or others, place them at increased risk of harm, impact the scientific integrity, have the potential to recur or represent possible serious or continuing noncompliance.
  - Observed or apparent non-compliance

Examples of Problems or Events that Require Prompt Reporting

- Other Unanticipated Events/Problems
  - Publication, interim analysis, safety monitoring report, or undated investigator's brochure that indicates an unexpected change to the risks or benefits of the research
  - Change in FDA labeling or withdrawal from marketing of a drug, biologic or device used in the research
  - Subject complaints that indicate an unanticipated problem or event which cannot be resolved by the research staff
  - Administrative hold by investigator or sponsor
  - Events requiring prompt reporting by the protocol or sponsor.

What is the time line for reporting?

- Reporting is required within five working days of becoming aware of the event for:

1. Internal adverse events considered serious as defined in previous slides (e.g., death, life threatening injury);

and

2. Changes to the protocol made without IRB approval to eliminate apparent immediate harm to subjects.

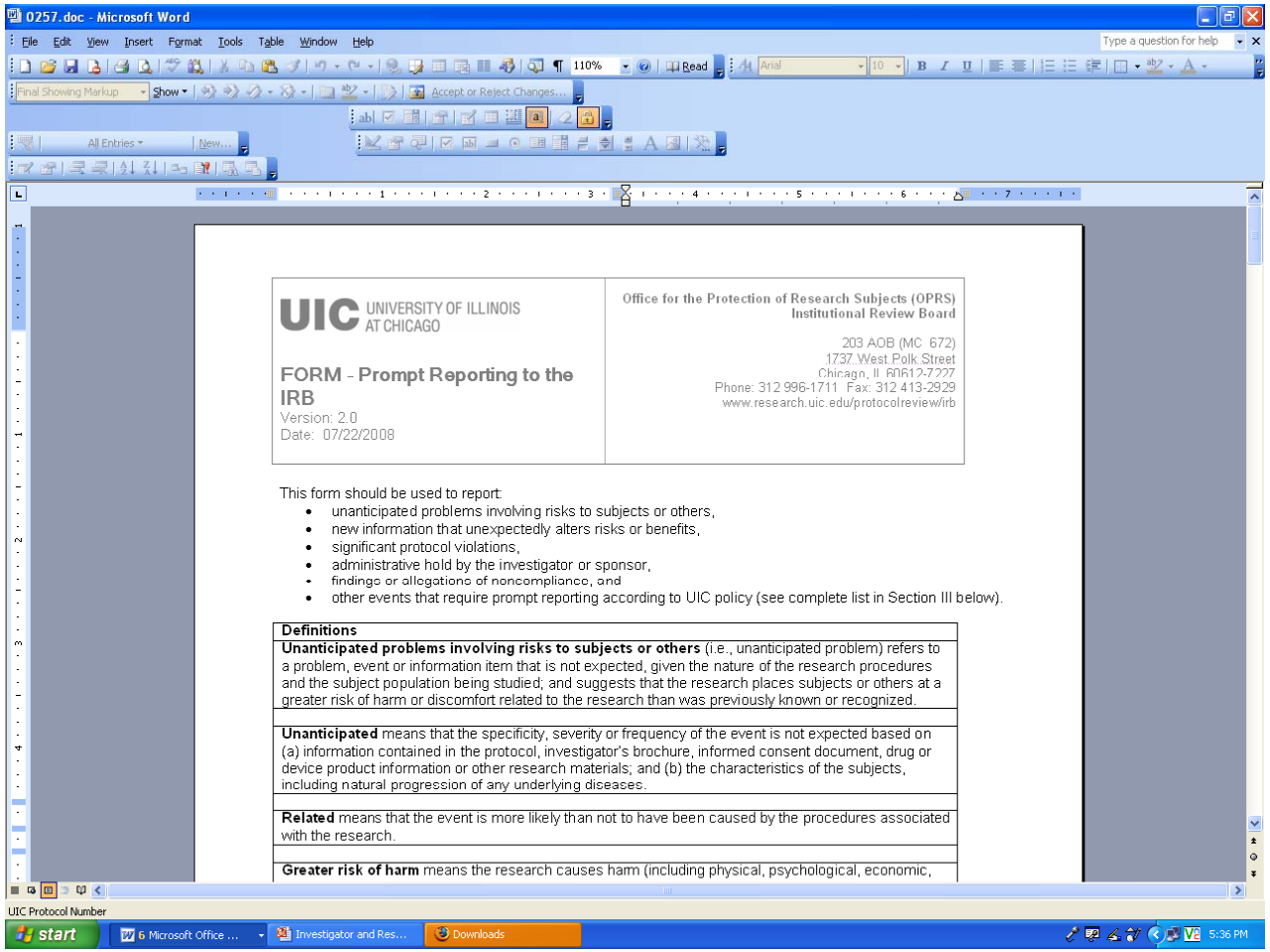
What is the time line for reporting?

- Report within 10 working days of discovering or being notified of the event is required for other incidents.

- PIs also responsible for reporting adverse events and problems to the sponsor and any other agencies as specified in the protocol, data safety monitoring plan or other agreements.

What form should be used?

- *Prompt Reporting to the IRB* form
  - Available on the UIC OPRS website (see next slide)
  - Link: http://tigger.uic.edu/depts/ovcr/research/protocolreview/irb/forms/0257.doc


0257.doc - Microsoft Word
File Edit View Insert Format Tools Table Window Help
UIC UNIVERSITY OF ILLINOIS AT CHICAGO
Office for the Protection of Research Subjects (OPRS)
Institutional Review Board
203 AOB (MC 672)
1737 West Polk Street
Chicago, IL 60612-7227
Phone: 312 996-1711 Fax: 312 413-2929
www.research.uic.edu/protocolreview/irb
FORM - Prompt Reporting to the IRB
Version: 2.0
Date: 07/22/2008
This form should be used to report:
unanticipated problems involving risks to subjects or others,
new information that unexpectedly alters risks or benefits,
significant protocol violations,
administrative hold by the investigator or sponsor,
findings or allegations of noncompliance, and
other events that require prompt reporting according to UIC policy (see complete list in Section III below).
Definitions
Unanticipated problems involving risks to subjects or others (i.e., unanticipated problem) refers to a problem, event or information item that is not expected, given the nature of the research procedures and the subject population being studied; and suggests that the research places subjects or others at a greater risk of harm or discomfort related to the research than was previously known or recognized.
Unanticipated means that the specificity, severity or frequency of the event is not expected based on (a) information contained in the protocol, investigator's brochure, informed consent document, drug or device product information or other research materials; and (b) the characteristics of the subjects, including natural progression of any underlying diseases.
Related means that the event is more likely than not to have been caused by the procedures associated with the research.
Greater risk of harm means the research causes harm (including physical, psychological, economic,
UIC Protocol Number
start
6 Microsoft Office ...
Investigator and Res...
Downloads
5:36 PM

Case Study: UIC Adverse Event Reporting

Emily Anderson, PhD

Prompt Reporting: Case Study 1

A research study aims to measure the short-term mental health effects of a physical activity intervention for older adults.

- During one of the 30-minute sessions, which involves seated activities with very light weights, a 75-year old woman falls off her chair, catches herself, and complains of wrist pain.
- As she appears okay at the time, you advise her to see her regular doctor as soon as possible, and you follow up with her in a few days. It turns out that she has a fairly significant wrist fracture.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 2

You are conducting an in-depth interview study on the effect of sexual assault on intimate relationships.

- All data are collected anonymously; participants are recruited from local survivor networks and told from the first point of contact with the research team to use a pseudonym.
- The IRB protocol states that transcripts will be stored on a secure, password-protected network.
- This is true, but you discover that one of your research assistants has been periodically making copies of the transcript files and emailing them to herself so that she can work on coding the data while at home on her home computer.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 3

You are conducting an online survey of methamphetamine users using a customized online survey programmed by one of your research team members.

- Participants are recruited through CraigsList. For quality control purposes (i.e., to ensure that one individual does not try to complete the survey more than one time), participants are asked to provide an email address. They also provide information about their drug use habits, whether or not they have engaged in illegal activities to support their habit, and sexual practices.
- You learn that due to a programming error, the data (including email addresses, city, state, and zip code, and date of birth) have been stored on a non-secure web site (a Google search on "methamphetamine research" brings up your data on the 2nd page). As far as you know, no one else has found these data online.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 4

Several years ago you completed a longitudinal study of cancer survivors. Your efforts resulted in several very large de-identified databases.

- A colleague with whom you have been working on several papers had their laptop stolen from their car, and the databases were saved on the desktop.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 5

You are conducting a longitudinal study of cancer survivors.

- When you call a participant's house for the fourth wave of data collection, you are told that she died suddenly the week prior.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 6

You are conducting a focus group examining barriers to health care in older adults with chronic health conditions.

- About 30 minutes into the focus group, Stan, one of the men in the group, starts behaving oddly. Initially, he was extremely articulate. Now, he appears confused and his speech is garbled. You ask him to stand up and he loses his balance. You call 911, and he is taken to the emergency room at Stroger. Luckily, Stan has a cell phone, and you have the last dialed number –his daughter.
- When you call her later that day, you learn that Stan had a transient ischemic attack (TIA or "mini-stroke"); this is the third one in the last year.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 7

You are conducting a study that involves digitally video-recording parent-child interactions.

- Someone steals some of the digital recording and computer equipment from an office that is accidentally left unlocked.
- The digital recorder had some footage that had not yet been downloaded on it, and the bag also included another disc.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Prompt Reporting: Case Study 8

You are the PI of a child health study that involves home visits conducted by a trained lay community health worker who both provides child care education and collects data.

- You get a frantic call one evening from one of the health workers. She had been at one of her families' homes earlier. She had been sitting with the mother in the living room, and at one point she got up and walked past the kitchen on her way to use the bathroom. When she entered the kitchen, the woman's husband was sitting at the table with several other men; the couple's 15-month old son was sitting with them in his high chair banging a spoon.
- She saw them quickly shove large amounts of cash, a gun, and a bunch of small Ziploc bags into a paper bag as she walked by.

1. **What needs to be reported to the IRB and how soon?**
2. **How would the event be classified?**
3. **Any other action/solution/ protocol change required?**

Open Discussion / Questions and Answers




Please remember to complete the CE Registration Sheet

- Contact Information:

Charles (Chuck) Hoehne
OPRS Assistant Director, Education and Training
1737 West Polk Street, Room 203
Chicago, IL 60612-7227
312-355-2908 (direct)
312-996-1711 (main)
choehne@uic.edu