## 5 Levels Seems Right

Scott Bradner
Ken Carson

1

## HRDSP

- Harvard developed a Harvard Research Data Security Policy (HRDSP) over about 1.5 years
- process driven by chair of Social Science Committee, Provost and Vice Provost for Research
  policy "owned" by VP for Research
- draft reviewed by IRBs, School CIOs, OGC, Social Science Committee, Provost, University Joint Committees on Inspection, ...

2

## HRDSP

- approved October 2010
  http://www.security.harvard.edu/research-data-security-policy
- since revised based on implementation experience
  - Clarified procedures, including facilities certification
  - Clarified responsibilities of Researchers, IRBs, School and HUIT Information Security Officers
  - No change to Security Level definitions

3

## HEISP

- Harvard Enterprise Information Security Policy
  - a set of University-wide policies to protect confidential information
  - annual training, etc
  - annual compliance assessment process
  - checked by Risk Management (Internal Audit) during audits
- been in place for a decade or so

4

## HEISP, contd.

- 3 levels
  - High Risk Confidential Information (HRCI)
    - e.g., SSNs, bank account #s, ...
  - Other Confidential Information
  - non-confidential information

5

## HRDSP, Sections

- Introduction
- Research Information from Non-Harvard Sources
- Research Information from Harvard Sources
- Information Security Categories
- Legal Requests for Research Information

6

## HRDSP, Introduction

- responsibilities: investigators:
  - disclose nature of data
  - prepare data security plans & procedures
  - implement plans & procedure
- responsibilities: IRB
  - ensure adequacy of investigators plans & procedures
- responsibilities: IT
  - assist investigators in determining proper levels
  - assist investigators in implementing security

7

## HRDSP, Non-Harvard Data

- if data has a use agreement (DUA)
  - protection must meet requirements in use agreement
  - IRB can determine that DUA is too weak
    - if so, treat as if data is from a Harvard source
- if research done in non-Harvard facility
  - facility owner may define protection requirements
- otherwise
  - treat as if data is from a Harvard source

8

## HEISP: Data from Harvard Source

- human subjects research
  - research must be reviewed by a IRB
  - information used in research must be protected against inadvertent or inappropriate disclosure
  - IRB will confirm security level categorization
- other sensitive research
  - e.g. research with national security implications
  - researchers should work with school IT groups to determine data categories

9

## HRDSP: Data Categories

- 5 levels of data about individually identifiable people
  - Level 5 - extremely sensitive information
  - Level 4 - very sensitive information (HEISP HRCI)
  - Level 3 - sensitive information about (HEISP other confidential information)
  - Level 2 - benign information
  - Level 1 - de-identified research information and other non-confidential research information

10

## HRDSP: Why 5?

- started with HEISP - 3 levels
  - high risk confidential information (level 4)
  - other confidential information (level 3)
  - non-confidential information (level 1)
- added level 5
  - because non-network connected requirement is in some use agreements and is the right thing for some data
- added level 2
  - to deal with "minimal risk" data

11

## HRDSP: De-Identification Key

- key for coded de-identified research information must be protected at the level that would have been applicable to the non-de-identified data
- what constitutes de-identification is not addressed in policy

12

## HRDSP: Level 5

- description:
  *Disclosure of Level 5 information could cause significant harm to an individual if exposed, including, but not limited to, serious risk of criminal liability, serious psychological harm or other significant injury, loss of insurability or employability, or significant social harm to an individual or group*
- examples
  currently mostly requirement in data use agreements
  e.g., raw census data, some mental health records

13

## HRDSP: Level 5 Protections

- stored in physically secure rooms under university control
  not on janitor's key or building master key
- computers must not be connected to a network that extends outside the room

14

## HRDSP: Level 4

- description
  *Disclosure of Level 4 information could reasonably be expected to present a non-minimal risk of civil liability, moderate psychological harm, or material social harm to individuals or groups*
- examples
  HEISP high risk confidential information (HRCI)
  e.g., subject's SSNs
  medical research records
  information with national security implications

15

## HRDSP: Level 4 Protections

- do not store on user computers or devices
  even if encrypted (too much risk of error)
- servers in physically secure environment
  card based access best - create access log
- local network-based firewalls
- access limited to IRB approved individuals
- media: encrypt or store in a locked safe
- separate networks using private addressing
- regular vulnerability testing

16

## HRDSP: Level 3

- description
  *Disclosure of Level 3 information would could reasonably be expected to be damaging to a person's reputation or to cause embarrassment.*
- examples
  most non-de-identified human research information
  student record information (FERPA)
  some commercial data
  employment records

17

## HRDSP: Level 3 Protections

- encrypt laptops and portable devices
- use automatic patching
- virus protection
- encrypt all transfer over networks and on portable media
- limit access to those doing the research
- host-based firewalls
- lock up all non-electronic records

18

## HRDSP: Level 2

- description
  *Disclosure of Level 2 information would not ordinarily be expected to result in material harm, but as to which a subject has been promised confidentiality.*
- examples
  data from reaction time experiments
  customer satisfaction survey data

19

## HRDSP: Level 2 Protections

- good computer hygiene
  secret complex passwords
  not shared accounts
  regular patching
  avoid dangerous web sites
  don't respond to phishing

20

## HRDSP: Level 1

- description
  de-identified research information about people and other non-confidential research information
- examples
  de-identified research information
    but might be private until publication
  student directory information
    except for FERPA blocks
  research information where no anonymity promised

21

## Legal Requests for Research Info.

- forward any legal request of information (e.g., a subpoena, national security request or court order demanding disclosure of information in researcher possession) to OGC
- researchers not authorized to provide the information
- consider obtaining a Certificate of Confidentiality
  - allow refusal to disclose

22

## HRDSP: Other Information

- policies include specific guidance on how to do data collection in the field for each level data
- web site also includes:
  - requirements when working with vendors
  - process for responding to Freedom of Information Act (FOIA) requests (send to OGC)
  - classified work (can not do)
  - advice for travelers
  - rules about paying subjects (i.e., tax requirements)

23

## Implementation

- specific protection requirements for each level
  - existing HEISP level protection requirements well understood
  - Levels 5 and 2 will take some work
    - special facilities for Level 5
    - researcher cooperation for Level 2
- communications to researchers
  - annually by Deans
  - day-to-day by IRBs
- enforcement is an open question

24

## Facility Certification

- facilities can get certified for particular level use
- IRB can rely on the certification for all research done in facility
  - no need to review security plan for each project
- OK to use higher level facility for lower level research
  - as long as higher level requirements followed

25