FULL BOARD REVIEW

MINIMAL RISK

IN-OFFICE REVIEW
Federal Definition of Minimal Risk

Research involves minimal risk when the probability and magnitude of harm or discomfort anticipated in the research are not greater than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

(45 CFR 46.102(h)(i))
Probability and Magnitude Anticipated
Minimal Risk Procedures

Charles II of Navarre
“Charles the Bad”

1332 - 1387
Probability and magnitude of risks are considered in context.

- Blood draw
- Fasting
- Withholding meds
- Time burden
- Pregnancy test results
- Survey sensitivity
- Age, health, everyday life
Risks can be difficult or impossible to anticipate.

- Additional CSF at LP
- Additional bone marrow at draw
- Vitamins, supplements, diets
- Prophylaxis
- Long-term exposure
- Legal and social effects
- Assays, diagnostic testing
- Genetics testing
- Nanoparticles and other wizardry
Minimal Risk Design Examples

- Single blood draw in healthy subjects
- Non-invasive collection of other samples
- Routine, non-invasive clinical procedures
- Chart review
- Surveys
- Interviews
- Focus groups
- Program evaluation
Primary “Minimal Risk” is often Breach of Confidentiality

Hippocratic Oath c. 450 BCE

“What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account must be spread abroad, I will keep to myself . . . .”
23 employees accessed records
15 employees fired; 8 reprimanded
No leaks
To date, 711 HIPAA breaches affecting >500 Individuals

- Laptop
- Email
- Paper
- Electronic Device
- Thumb Drive

- Improper Disposal
- Loss
- Theft
- Hacking

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Individuals Affected</th>
<th>Date of Breach</th>
<th>Type of Breach</th>
<th>Location of Breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oconee Physician Practices</td>
<td>SC</td>
<td>653</td>
<td>2010-03-09</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Ohio Health Plans</td>
<td>OH</td>
<td>78,042</td>
<td>2011-06-03</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>OhioHealth Corporation dba Grant Medical Center</td>
<td>OH</td>
<td>501</td>
<td>2010-11-05</td>
<td>Theft</td>
<td>Laptop, Computer</td>
</tr>
<tr>
<td>OHP PHSP, Inc.</td>
<td>NY</td>
<td>28,187</td>
<td>08/31/2012 - 09/21/2012</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Okaloosa County Public Safety</td>
<td>FL</td>
<td>715</td>
<td>06/15/2012 - 10/01/2012</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Oklahoma City VA Medical Center</td>
<td>OK</td>
<td>1,950</td>
<td>2010-10-08</td>
<td>Theft, Loss, Improper Disposal</td>
<td>Paper</td>
</tr>
<tr>
<td>Olendorf Medical Services</td>
<td>NY</td>
<td>549</td>
<td>2012-01-17</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Olson &amp; White Orthodontics</td>
<td>MO</td>
<td>10,000</td>
<td>2013-07-22</td>
<td>Theft</td>
<td>Desktop Computer, Network Server</td>
</tr>
<tr>
<td>Omaha Construction Industry Health and Welfare Plan</td>
<td>NE</td>
<td>800</td>
<td>2009-11-11</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
Female, 72
6’1”
140 lbs
Lives alone
No dog
1. Names
2. Address

3. Dates and Age > 89

4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voice
17. Full face photographic images and any comparable images

18. **Any other unique identifying number, characteristic, or code (not including a random linking code)**
   - Code derived from identifiers, combination of data variables or unique single variable.
OHRP “identifiable”

The identity of the subject is or may readily be ascertained by the investigator or associated with the information.
Example of single unique identifier
Risks aren’t always apparent.

- Emotional impact of fully anonymous survey
- Potential for disclosure on subject’s side
  - Recruitment materials and methods
    - Letters
    - Emails
    - Phone Calls
  - Surveys
  - Interviews
    - Safe scheduling
  - Focus groups
    - Participants have a right to describe their experiences with others
Cardiology Department
CHF Study
OHSU
3181 SW Sam Jackson
Portland, OR 97239

Amy Nottellinghusbandaboutheartfailureuntilnext Thursday
221B Baker Street
Portland, OR 97239
<table>
<thead>
<tr>
<th>Title</th>
<th>Policy</th>
<th>Forms</th>
<th>Add'l Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates of Confidentiality (CoC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Use Agreement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Use Agreement: Research</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA Authorization for Obtaining Existing Records Outside of OHSU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prep to Research</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Sharing Agreement (De-Identified)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Sharing Agreement (Identifiable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Representation Form for Research Involving Only Decedents' Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Confidentiality – Protocol Checklist</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Waiver or Alteration of HIPAA Authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

http://www.ohsu.edu/xd/about/services/integrity/policies/irb-policies-privacy-and-conf.cfm
Mark your calendars!

Thursday, December 12
10:00 – 11:00 a.m.
UHS 8B60

“Toward a Better IRB”