Privacy and Confidentiality in Human Subjects Research

March 29, 2008
Emory University IRB
Sarah Putney
Key Concepts: Privacy v. Confidentiality

- **Privacy** is a sphere of protection surrounding a person and his/her property or information, in which s/he can be let alone, without unwarranted interference or intrusion.

- **Confidentiality** is the limited scope in which a person’s private information is shared with others.

- **Breach of confidentiality** happens when a person’s private information is taken outside the scope of confidentiality by someone else (intentionally or not, with resulting harm or not).
Privacy, Confidentiality and the Belmont Report’s Big 3

- Respect for persons (autonomy)
  - Researchers actively protect subject’s privacy
    - Comply with all applicable rules and laws, including HIPAA
  - Researchers don’t breach confidentiality of subject’s private info
    - Use appropriate data security measures
Privacy, Confidentiality and the Belmont Report’s Big 3

- **Beneficence**
  - Researchers maximize the benefits of the research to the subject, group, community or society
    - Use of subject’s private info should be justified by benefit of research
  - Researchers minimize harm from research, including breach of confidentiality and intrusions on privacy
    - Data security
    - Certificates of Confidentiality
    - HIPAA compliance by covered entities and researchers working with them to use individually identifiable information
Privacy, Confidentiality and the Belmont Report’s Big 3

- Justice
  - Do the benefits of the research accrue to the persons whose individually identifiable, private information was used?
    - Answer doesn’t have to be “yes” but IRB must find appropriate balance of risk and benefit, ensure integrity of voluntary, comprehending, informed consent, and that the importance of the knowledge reasonably expected to be gained justifies “no”
  - Is the informed consent process appropriate and IRB approved?
  - Are necessary HIPAA authorizations in place or a waiver approved by a privacy board/IRB?
How to Describe Risks of Breach of Confidentiality

- Honestly
  - E.g., “no known risk,” “remote” or “slight” risk
  - Avoid “no risk”
  - Give statistical risk if available

- Specify data security measures
  - E.g., locked file, stripped of identifiers (name, address, SSN, date of birth) at what point, electronic technical protections, who will have access to personal identifiers
Other Consent Form Issues

- “But what if the description sounds scary or might unduly alarm prospective subjects?”
  - Balance description of risks with the measures you will take to prevent breach
  - Cite your track record for no breaches
  - Analogize to the daily risks of breach in other situations
  - Emphasize the partnership aspect of research and your commitment to doing your part in return for use of the subject’s private or confidential information
Other Consent Form Issues

“What if a breach occurs? What do I do?”
- Take immediate measures to prevent further breach and any damage resulting from it
- Report it to your IRB as an adverse event
  - Include a corrective action plan, if appropriate, that would prevent more incidences of breach
  - Review data security procedures with research staff
- Cooperate with IRB on follow-up with subject
Certificate of Confidentiality

- **What is it?**
  - A legally effective form of protection permitting a PI and/or institution under subpoena **not** to release confidential study data

- **Whom does it “cover”?**
  - The PI and/or institution, not the subject
  - But the subject benefits from preservation of confidentiality
Certificate of Confidentiality

Who issues it?

- U.S. Dept. of Health and Human Services
- NIH has authority on behalf of DHHS
- Highly disseminated system, currently with a poor tracking ability
- Turnaround time: 3 to 8 weeks
CoC: Statutory Authority

- Section 301(d) of the Public Health Service Act, 42 U.S.C. 241(d)
- Secretary of DHHS may authorize persons engaged in biomedical, behavioral, clinical and other research
  - To protect the privacy of individuals who are the subjects of that research
- Authority has been delegated to the NIH
Certificate of Confidentiality

- **Subpoena**
  - A legally enforceable written command to appear at a certain time and place to give testimony upon a certain matter. A subpoena is served on a person (e.g., a PI).

- **Subpoena duces tecum (“bring with you”)**
  - A court process, initiated by a party in litigation, compelling production of certain specific documents and other items, material and relevant to facts in issue in a pending judicial proceeding, which documents and items are in custody and control of person or body served with process. *Black’s Law Dictionary, 6th edition*
Certificate of Confidentiality

- Boundaries of its protection:
  - Date of issuance to date of expiration
  - Does not protect against PI’s voluntary disclosure
  - Does not protect against request for disclosure without a subpoena
    - PI can say “yes” or “no” voluntarily, unless IRB bars disclosure
Certificate of Confidentiality

- Does not prevent subject from voluntarily disclosing private information
- Does not prevent mandatory reporting by PI in accordance with law
  - Child abuse
  - Threat of harm to self or others
  - Reportable communicable diseases
Certificate of Confidentiality

- Does not prevent seeker from getting same private info from other, unprotected sources
- NIH, FDA, IRB may audit files and view research information
CoC: Requirements

PI/Institution obtaining CoC must:

- Disclose its existence to subjects
  - In consent form or information sheet
  - PI may need to recontact subjects and reconsent with new information
- Include a clear explanation of COC
  - What it does, its power v. a subpoena
  - What it doesn’t do, its limits
CoC: Requirements

- Document IRB approval and IRB qualifications
- Provide a copy of the informed consent forms approved by the IRB
- PI and Institutional Official must sign application
CoC: assurances undertaken by PI/institution

- Agree to protect against compelled disclosure and to support and defend the authority of the Certificate against legal challenges
- Agree to comply with Federal regulations that protect human subjects
- Agree not to represent Certificate as endorsement of project by DHHS or NIH or use to coerce participation
- Agree to inform subjects about Certificate, its protections and limitations
What kind of information is eligible for its protection?

- Only “sensitive” information, i.e., if disclosure could have adverse consequences for subjects or damage their:
  - financial standing
  - employability
  - insurability, or
  - reputation
Certificate of Confidentiality

- Allows the investigator and others who have access to research records to refuse to disclose identifying information in any
  - civil
  - criminal
  - administrative
  - legislative, or other proceeding, whether at the federal, state, or local level
Certificate of Confidentiality

- For IRB-approved research collecting identifying information
- NIH or PHS funding not required
Certificate of Confidentiality

- "Identifying Information" is broadly defined
- Not just name, address, social security number, etc.
- Includes any item or combination of items that could lead directly or indirectly to the identification of a research participant
CoC: examples of eligible studies

- Collecting genetic information
- Collecting information on psychological well-being of subjects
- Collecting information on sexual attitudes, preferences or practices
- Collecting data on substance abuse or other illegal risk behaviors
- Studies where participants may be involved in litigation related to exposures under study (e.g., breast implants, environmental or occupational exposures)
COC: examples of non-eligible work

- Not research
- Not collecting personally identifiable information
- Not reviewed and approved by the IRB as required by NIH guidelines
- Collecting information, that if disclosed, would not significantly harm or damage the subject
CoC: consequences of not defending against a subpoena

- NIH would take this very seriously and probably would open an inquiry with the institution and PI, look for a corrective action plan, possibly impose disallowances, demand refunds, restrict individual PI/dept/school/institution
- NIH cannot monitor all individual PIs
- NIH enforces regulations through institutions, which are responsible for the compliance of their PIs
Certificate of Confidentiality

- Only once has a CoC been challenged in court and it was upheld
- IRB’s confidentiality-protecting steps can make a big difference in court; even lines from a consent form can provide the basis for a decision
Certificate of Confidentiality

- Privileges protecting against subpoena are rare:
  - Attorney-client
  - Doctor-patient
  - Marital
  - Clergy
  - CoC – provides high degree of protection and privilege to the PI
Certificate of Confidentiality

- Caveat: CoC does not obviate need for data security
- Data security is key to protecting subjects’ private information
  - Unauthorized persons must not be granted access to research data or learn the identities of human subjects
  - CoC does not protect a subject from a negligent researcher
CoC: for more information

Go to the Certificates of Confidentiality Kiosk at http://grants1.nih.gov/grants/policy/coc/index.htm

Kiosk includes:

- background information and Instructions
- application information for extramural investigators
- application information of intramural investigators
- FAQs
- contact list
- reportable communicable diseases policy
CoC v. HIPAA Privacy Rule

- A CoC can stop a subpoena; HIPAA can’t
- HIPAA requires tracking of uses/disclosures of PHI; a CoC does not require tracking of attempts at forced disclosure
- HIPAA provides a floor of protection for all individuals; a CoC provides a strong but narrow protection for research subjects sharing sensitive information with researchers
Thank you

Acknowledgments:

Tina Sheldon, Diane Lopez, the Harvard University IRB Operations Group and HIPAA Working Group, Mary Mitchell, Pearl O’Rourke and colleagues at Partners Healthcare Systems, Wendy Baldwin and Lora Kutkat of NIH, privacy consultants Bob Gellman and Peter Swire, and PRIM&R.