



# Office of Human Research Ethics Training Tips

## Subject Privacy & Confidentiality of Data

There should be adequate administrative, procedural and technical provisions to protect the privacy of subjects and to maintain the confidentiality of data. The assessment of adequacy should include consideration of the sensitivity of the data.:

- The ethical principle of “respect for persons” as enunciated in The Belmont Report; and
- **Criteria for IRB Approval of Research: §46.111 & §56.111, (7)** When appropriate, there are adequate **provisions to protect the privacy of subjects and to maintain the confidentiality of data.**

**Note:** Additional guidance is available in the University’s “Information Security Policy and Standards” and the NIH Data Sharing Policy and Implementation Guidance, available [http://grants.nih.gov/grants/policy/data\\_sharing/index.htm](http://grants.nih.gov/grants/policy/data_sharing/index.htm). **The investigator is responsible for maintaining the confidentiality of research subject data for as long as the investigator is in possession of such data.**

### Subject Privacy: Individual Identifiability of Data

Definition of data that is not individually identifiable: This is a table of direct and indirect identifiers that must be stripped from data in order for the data to be considered de-identified.

- |  |   |
|--|---|
| — Names  | — Account numbers   |
| — Telephone numbers  | — Certificate/license numbers   |
| — Any elements of dates (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death. For ages over 89: all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 and older | — Vehicle identifiers and serial numbers (VIN), including license plate numbers   |
| — Any geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code  | — Device identifiers and serial numbers (e.g., implanted medical device)  |
| — Fax numbers  | — Web universal resource locators (URLs)  |
| — Electronic mail addresses  | — Internet protocol (IP) address numbers  |
| — Social security numbers  | — Biometric identifiers, including finger and voice prints  |
| — Medical record numbers   | — Full face photographic images and any comparable images   |
| — Health plan beneficiary numbers  | — Any other unique identifying number, code, or characteristic, other than dummy identifiers that are not derived from actual identifiers and for which the re-identification key is maintained by the health care provider and not disclosed to the researcher |

### Confidentiality of Data

- **HIPAA**
- **FERPA**
- **Certificates of Confidentiality**
- **Limits on Confidentiality: Reporting Requirements**

➤ **Limits of Confidentiality: NIH Data Sharing Policy**

Starting with the October 1, 2003, receipt date, investigators submitting an NIH application seeking \$500,000 or more in direct costs in any single year are expected to include a plan for data sharing or state why data sharing is not possible. In cases where human subjects' privacy precludes or limits data sharing, that explanation will be required in the NIH application. The NIH Data Sharing Policy and Implementation Guidance, is available at [http://grants.nih.gov/grants/policy/data\\_sharing/data\\_sharing\\_guidance.htm](http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm)

➤ **Limits of Confidentiality: Subpoenas**

All subpoenas for research data should be referred immediately to the Office of University Counsel for assistance.

➤ **Limits of Confidentiality: The Shelby Amendment**

The Shelby Amendment (Public Law 105-277 signed October 21, 1998) provides that if federally supported research results are used by the federal government in developing "an agency action that has the force and effect of law" then the federal agency may be required to obtain the research data and make it available if requested under the Freedom of Information Act (FOIA, 5 U.S.C. 552(a)(4)(A)). The extent and format of research data that must be shared is not specified in the Shelby Amendment. In some instances it has been narrowly interpreted to be limited to published data specifically cited in the promulgation of federal regulations. Seek assistance from the Office of University Counsel regarding any request for research data under the Shelby Amendment.