LEGALITIES OF DATA SHARING

THE VALUE OF DATA SHARING

- To best serve vulnerable individuals within our community, we must communicate across the silos of data created by governmental and community agencies.
- Sharing creates more accurate evaluation of policy options, improved stewardship of taxpayer dollars, reduced paperwork burdens, and more coordinated delivery of public services.

HOW ISC PROTECTS DATA

- All data released from the ISC Community Database are de-identified and aggregated.
- The ISC Data and Research Oversight Committee (DAROC) always includes a member of the agency whose data is requested for research. This member approves data request and data set before release to the researcher.

EXECUTIVE ORDERS ON DATA SHARING

**M-11-02: Sharing Data While Protecting Privacy, 2011**

- Refers to Privacy Act of 1974 § 552a. (b)(5) States no agency shall disclose any record EXCEPT: “to a recipient who has provided agency adequate written assurance that record will be used as statistical research and the record is to be transferred in a form that is not individually identifiable.”
- Notes that laws distinguish between interagency sharing of personally identifiable information that generate only aggregate statistical results and disclosure of personally identifiable information.

**M-13-17: Next Steps in the Evidence and Innovation Agenda, 2013**

- Examples given of harnessing data to improve agency results include linking data across programs and levels of government.
  - A number of Federal agencies have developed protocols to share personally identifiable data to permit linkages (including HUD and DHHS who studied how housing interventions affect health care use of the elderly).
- Notes that linking data can lower costs and improve quality of evaluations and programs.

LEGAL CONSIDERATIONS

- **Privacy**: If all data used is collected for administrative purposes, then data sharing is only a threat to privacy if there is improper disclosure of identifying information.
- **Disclosure**: Unique identifiers, identifying attributes and other attributes are the personal information of concern for improper disclosure. As long as researcher does not have interest in a certain individual and personal information cannot be identifiable when released, safeguards are available and practical.
- **Confidentiality**: Confidentiality can be ensured by anonymity, which is an implicit agreement that no one can identify the individual.