

Ethical Use of Administrative Data for Research Purposes

Roger A. Boothroyd, Ph.D. and
Paul G. Stiles, J.D., Ph.D.

Department of Mental Health Law & Policy
University of South Florida

This paper and presentation is produced through support by the John D. and Catherine T. MacArthur Foundation

Charge for Paper

- **Focus:** An overview of the ethical considerations and issues associated with the maintenance, integration, and use of administrative data for research purposes.
- **Primary Audiences:** policy makers and administrators in public agencies
- **Length:** About 30 pages doubled spaced, excluding references.
- **Process:** Outline of proposed paper approved in Fall 2010, peer/expert review in early to mid 2011, conference in November 2011, final version by early 2012.

Approach to Paper

- Provide an overview of ethical issues associated with using administrative data for research purposes
- Readable by multiple stakeholders
 - Comprehensive, but not deep scholarly discussion
- Incorporate the concept of due diligence (how to)
- Structure of paper
 - General Introduction and Concepts
 - Ethical Considerations for Data Owners/Custodians
 - Ethical Considerations for Data Users/Researchers
- Disclosure

Context

- Rapidly increasing capacity to collect, store, integrate, and analyze data
- Shift in use of these data from primarily managing agency programs and performing audits to conducting research and informing policy; purposes are broader in scope and depart from the original intent for which these data were collected
- Ease of access to these data has often out paced our consideration of the legal and ethical issues

Introduction

- Historical Perspective & Core Principles
 - Nuremberg Code
 - voluntary informed consent
 - Belmont Report
 - Respect for Persons
 - Beneficence
 - Justice

Introduction

- Availability of Administrative Data
 - Increased availability
 - Increased use for secondary purposes
 - Issues:
 - People whose information is in the database
 - Data owners/custodians
 - Scientific merit of secondary use
 - Challenges:
 - Poor secondary data quality
 - Statistical significance without meaningfulness
 - Multiple use of statistical tests

Introduction

- Legal Landscape Governing Access to Administrative Data
 - Freedom of Information Act (FOIA)
 - Federal Education Rights and Privacy Act (FERPA)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Other (local, state, foreign)
- Definitions of Key Concepts
 - Data Owners/Custodians
 - Data Users
 - Due Diligence
 - Ethics and Research Ethics

Considerations/Framework

- Development of Considerations
- Framework of Principles
 - Data Security
 - Training (expertise)
 - Policies (processes)
 - Technology (tools)
 - Confidentiality of Information
 - Disclosure Permissions
 - Appropriate Use

Ethical Use of Administrative Data

Data Owner/Custodian

- Recent attempts to ID best ethical practices for data protection & management from data owner perspective
 - Mason (1986)
 - Hotz et al (1998)
 - Kelman et al (2002)
 - AMIA (2007)
 - Karp et al (2008)
 - Stiles et al (2011)

Data User/Researcher

- Similar concerns as data owners, however some important differences in emphasis (many data users are also data owners)
- Need well developed internal and external connections to ensure data integrity/security as well as valid analyses

Principle #1: Data Security

Data Owner/Custodian

- Need to secure and protect data against inappropriate disclosure
- Standards are readily available online, but balance in 3 areas are recommended:
 - Training (expertise)
 - Policies (processes)
 - Technology (tools)

Data User/Researcher

- Provide as good or better security than data owner
- Similar considerations in areas of:
 - Training
 - Policies and processes
 - Technological security
- Need to be careful not to lose vigilance with security concerns

Principle #2: Confidentiality

Data Owner/Custodian

- Conceptual foundations
 - Trust
 - Autonomy and privacy
- Need to clarify processes for deidentification, encryption, etc
- Federal law (e.g., HIPAA)
- Integrating data and creating new information
 - Reidentification

Data User/Researcher

- Document and follow confidentiality processes (e.g., encryption, auto-logouts, deidentification)
- Federal laws
- Special considerations when combining data sets

Principle #3: Disclosure Permissions

Data Owner/Custodian

- Need to secure permissions to provide and allow use of data at 2 levels:
 - Institutional
 - Individual
- Document in agreement:
 - that data were obtained and provided appropriately
 - that adequate permission was secured to use data for the intended research purposes

Data User/Researcher

- Provide formal and detailed data request
- Data agreement should clarify terms of data possession and use
- Third party requests for the data should be referred back to data owner

Principle #4: Appropriate Use

Data Owner/Custodian

- Confirm capacity of data requestor to store/use data
- Be available to provide intelligence about data and interpretation
- Monitor (ask for updates about use) to ensure appropriate use of data

Data User/Researcher

- Critical yet often overlooked area of consideration
- Researcher should ensure:
 - He/she has adequate capacity to use the data
 - That data received are valid and useful for research
 - That the research team has adequate understanding of the data

Conclusions

- Data owners and users have a overarching responsibility for ensuring due diligence.
- We offer this four principle framework for assessing ethical responsibilities of data custodians and the researchers who use these data.

Questions

- Is the level of detail in the paper appropriate for policy makers and administrators in public agencies?
- Are there ethical issues included in the paper that should be removed or any issues that should be added?
- How can we improve the structure and/or format of the paper?