



*Improving Public Health Data
Dissemination through Policy
and Tools*

**Barbara Rudolph, PhD, MSSW
NAHDO Consultant
Senior Scientist, University of
Wisconsin-Madison**

June 23, 2016

Data Stewardship

- What is the role of a data steward?
 - NCVHS updated their definition of stewardship as “the responsibility of ensuring appropriate collection, management, use, disclosure, or safeguarding of information.”
 - NCVHS did this in response to increasing demands from communities who needed data.
 - NCVHC published a report titled, “NCVHS, The Community as a Learning System for Health, December 2011” which discusses data needs and resources and the importance of trust.

Resources for Policies, Processes, Partners

In the next slides, I will quickly share some options for using resources, developing policies based on data release processes, and working with partners to extend data access and use.

In the following presentations, you will get more detail on some of these options --

NAHDO Resources

History of NAHDO Efforts in Privacy of Data

- Testimony at NCVHS; Representation on NCVHS (Denise Love)
- White Papers and Contract Project Reports
- Published articles
- Technical Tools—Inventory for Screening (Data) Release
- Administrative Data Committee leading to PHDSC
- Guidance Documents and Technical Assistance (NY)
- Privacy Workgroups

NAHDO Documents Covering Data Management and Release Policies

- Rudolph, B. Davis, R. Administrative Data and Disease Surveillance: An Integration Toolkit. NAHDO-CDC Cooperative Agreement Project, CDC Assessment Initiative
- Rudolph B., Shah, G., Love D. Small numbers, disclosure risk, security, and reliability issues in web-based data query systems. J Public Health Management Practice, 2006.
- Person-level Data: An Inventory for Screening Release, NAHDO, 2008.
- PHDSC, PRISM--A Privacy Toolkit for Public Health Professionals.; Glossary.
- Guidance Document on Creating and Releasing Hospital and Facility Discharge Data Public Use Files, NAHDO, 2012

Data Release Resources

- Web-based Data Query Systems-- JPHMP
- Web-based Data Tables--JPHMP
- Public Reports with Data Tables
- Public Use Files --PUF Report; Person Level Data Inventory; Privacy Tool
- Research Data Files
- Custom Data Files

Key Release Policy Examples from NAHDO Resources

- Need a defined process for reducing disclosure risk, e.g.,
 - A numerator and event denominator rule—for tables
 - For web-based systems need simultaneous tabulation of both events and underlying population
 - For public reports similar calculations prior to release of report
 - May need a defined duplicate rule
 - CMS PUF requires 11 duplicates for combination of all analytic variables

How to Gain Flexibility Using Data Release Policies focused on Process

- Determine key variables being requested
- Identify variables that can be dropped if populations are too small. Can some variables be further aggregated? (reduces risk of identification) Once the drop or aggregation occurs—the steward could assess file duplicates to assure that risk of identification was low but not zero. One method is to test against the full file.
- Review request with privacy data review board
- Utilize a Data Use Agreement with specifications on use and file destruction.

Use Purpose Specifications— NCVHS

“Another long established fair information practice is purpose specification.” This means that data stewards consider the purpose of data collection (and release) and the future use of data disseminated for a specific project, and they make both initial purpose (use) and anticipated uses explicit in data use agreement.

Data Partnership--Options

Data partnerships can be another way to disseminate data to trusted partners—

- (1) Sensitive data elements can be shared and then stripped off after a linkage done by a trusted third party. For example, address information can be shared with trusted partner who encrypts patient ID and then shares only encrypted patient ID and address to third party for geo-coding. Geo-coding is then added to file and other identifiers stripped off. Files with geo-codes returned to partner and to data steward.

Data Access Options

- A data enclave is an entity that provides analytic access through protected data systems. It allows analysis without releasing sensitive data elements to users.
- Other types of data access can be designed to allow researchers access within data agencies. Again linkages can be made and then identifiers can be stripped off the files.

Where to find resources--

- www.nahdo.org/data_resources/data_dissemination
- www.ncvhs.hhs.gov/recommendations-reports-presentations
- www.cms.gov/Research-Statistics-Data-and-Systems