National Committee on Vital and Health Statistics

Advising the Secretary of Health and Human Services on health information policy since 1949.

2015 National Association of Health Data Organizations Annual Meeting: National Committee on Vital and Health Statistics Presentation

Data Stewardship, Privacy, and Confidentiality: Implications for Collection and Dissemination of APCD and Case-Mix Data

Bruce Cohen, NCVHS

October 29, 2015

Overview

- Background on NCVHS
- Concepts
- NCVHS activities
- Update on ONC (Office of National Coordinator) related projects
- Significance for APCD/case-mix data access and use

The National Committee on Vital and Health Statistics

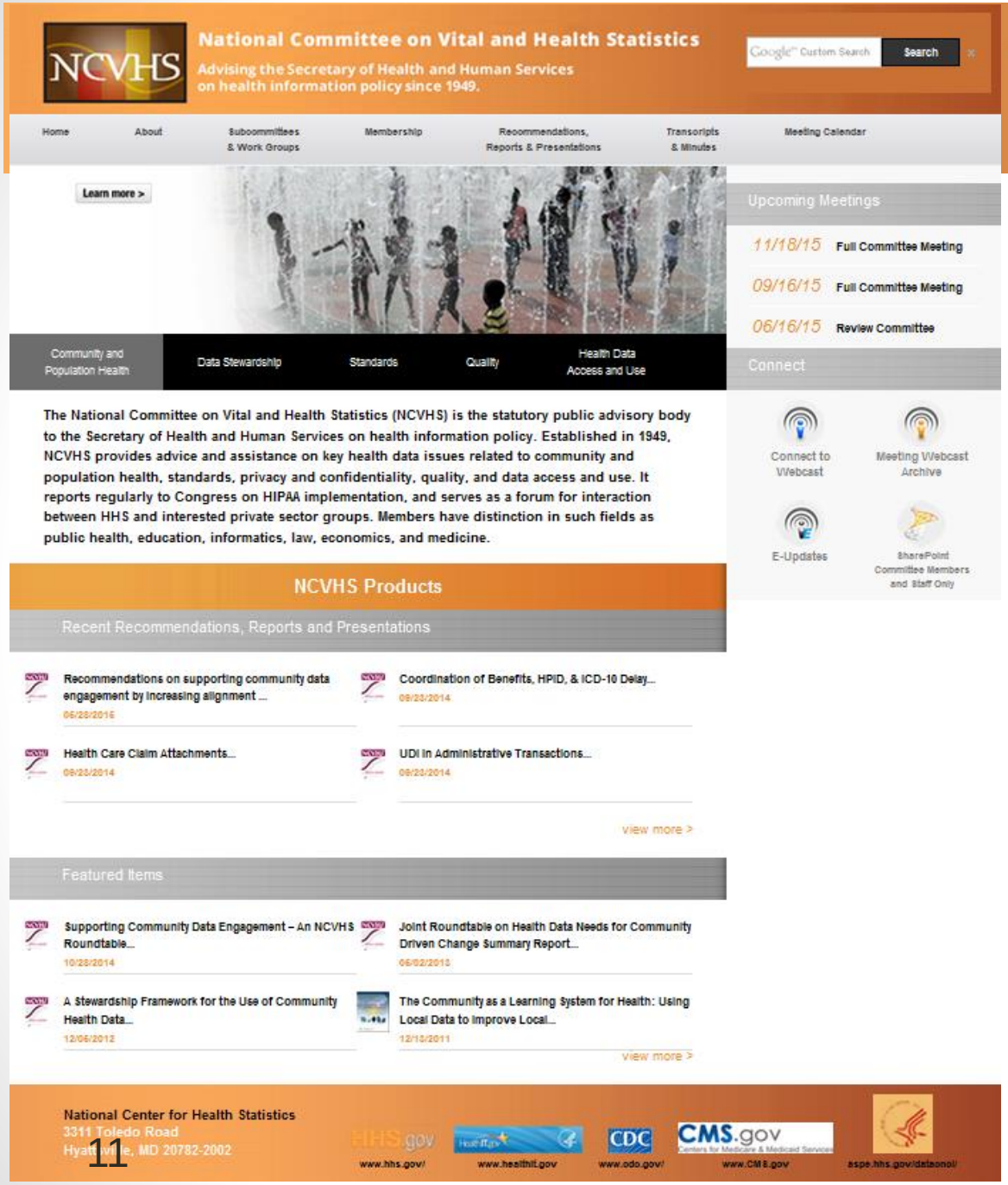
- One of the oldest if not the oldest statutory public federal advisory body to the HHS Secretary
- Focuses on health data and statistics, standards, and health information policy
- Provides advice and assistance to various HHS groups and agencies (HHS Data Council, CMS, CDC, HRSA, AHRQ, others)
- Serves as a forum for interaction with private and public sector groups on a variety of health data and information issues

NCVHS Milestones

1949	Established as federal advisory committee
1974	Public Health Services Act gave NCVHS official status as statutory public advisory committee to the Secretary of HEW (now HHS)
1996	HIPAA charged NCVHS with advising Secretary on health data standards and privacy policy
2003	Medicare Modernization Act charged NCVHS with recommending standards for electronic prescribing
2010	Affordable Care Act charged NCVHS with advising the Secretary on Operating Rules for HIPAA Administrative Simplification
2014	NCVHS designated as the Review Committee (under ACA provisions), to review status of adoption/implementation of standards/operating rules, and advise on changes needed

NCVHS Domains

Areas	Focus
Standards Subcommittee	Standards, code sets, identifiers, operating rules for HIPAA transactions, as required under HIPAA, MMA, and ACA
Population Health Subcommittee	Population-based data and data about specific vulnerable groups
Privacy, Confidentiality and Security Subcommittee	Emerging issues related to health information privacy, confidentiality and security and data stewardship
Data Access and Use Work Group	Principles, best practices, guidelines, gaps on the availability, accessibility, use, utility, usability, and usefulness of HHS data resources



NCVHS Website and Resources

- www.ncvhs.hhs.gov
- All meeting announcements, letters to the Secretary, reports, tools, and other resources available from this site
- Electronic/remote access to meetings and meeting materials

Concepts: General

Privacy deals with the appropriate **use** and **disclosure** of information. Privacy is access to the person.

Confidentiality is about control over use of data and is the term that really is our concern today (the HIPAA privacy rule is really a confidentiality rule).

Security refers to physical, technical, and administrative safeguards to make sure that the data are appropriately protected from destruction or corruption and that they are used only as specified.

Concepts: Federal and State Privacy Laws

FEDERAL

- Federal Privacy Act of 1974 (5 USC Sec. 552a)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Family Educational Rights and Privacy Act (FERPA)

State

- State public records laws, fair information practice regulations and freedom of information statutes. These are state laws that limit how state agencies collect, maintain, use, and share personal data . Generally, they requires agencies to ensure the security of personal data; require agencies to establish procedures that implement state legal requirements; and give people rights with respect to their own personal data held by state agencies
- Other data system-specific laws and regulations
  - Drug and Alcohol Abuse Records, Educational Records, HIV Test Results
  - Vital Records, Hospital discharge/ APCD, State Public Records

Key NCVHS Privacy-Related Activities

- Report to the Secretary of HHS (2007): Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data
- Letter to the Secretary (2010) – Recommendations Regarding Sensitive Health Information
- Letter to the Secretary on the Development of Stewardship Framework for the Use of Community Health Data (2012) and the distribution of The Toolkit for Communities Using Health Data (2014)

A Stewardship Framework for "Secondary Uses" of Electronically Collected Health Data

In making its recommendations, NCVHS observed that currently, the health industry relies upon the HIPAA construct of covered entities and business associates to protect health data. Its recommendations call for a transformation, in which the focus is on appropriate data stewardship for all uses of health data by all users, independent of whether an organization is covered under HIPAA.

Principles:

1. maintain or strengthen individual's health information privacy
2. enable improvements in the health of Americans and the healthcare delivery system of the Nation
3. facilitate uses of electronic health information
4. increase the clarity and uniform understanding of laws and regulations pertaining to privacy and security of health information
5. build upon existing legislation and regulations whenever possible
6. not result in undue administrative burden

A Stewardship Framework for "Secondary Uses" of Electronically Collected Health Data: Recommendations

HHS should issue guidance to covered entities that the HIPAA definition of de-identification is the only permitted method for personal health information

NCVHS believes there are significant concerns surrounding uses of de-identified data that warrant more thorough analysis.

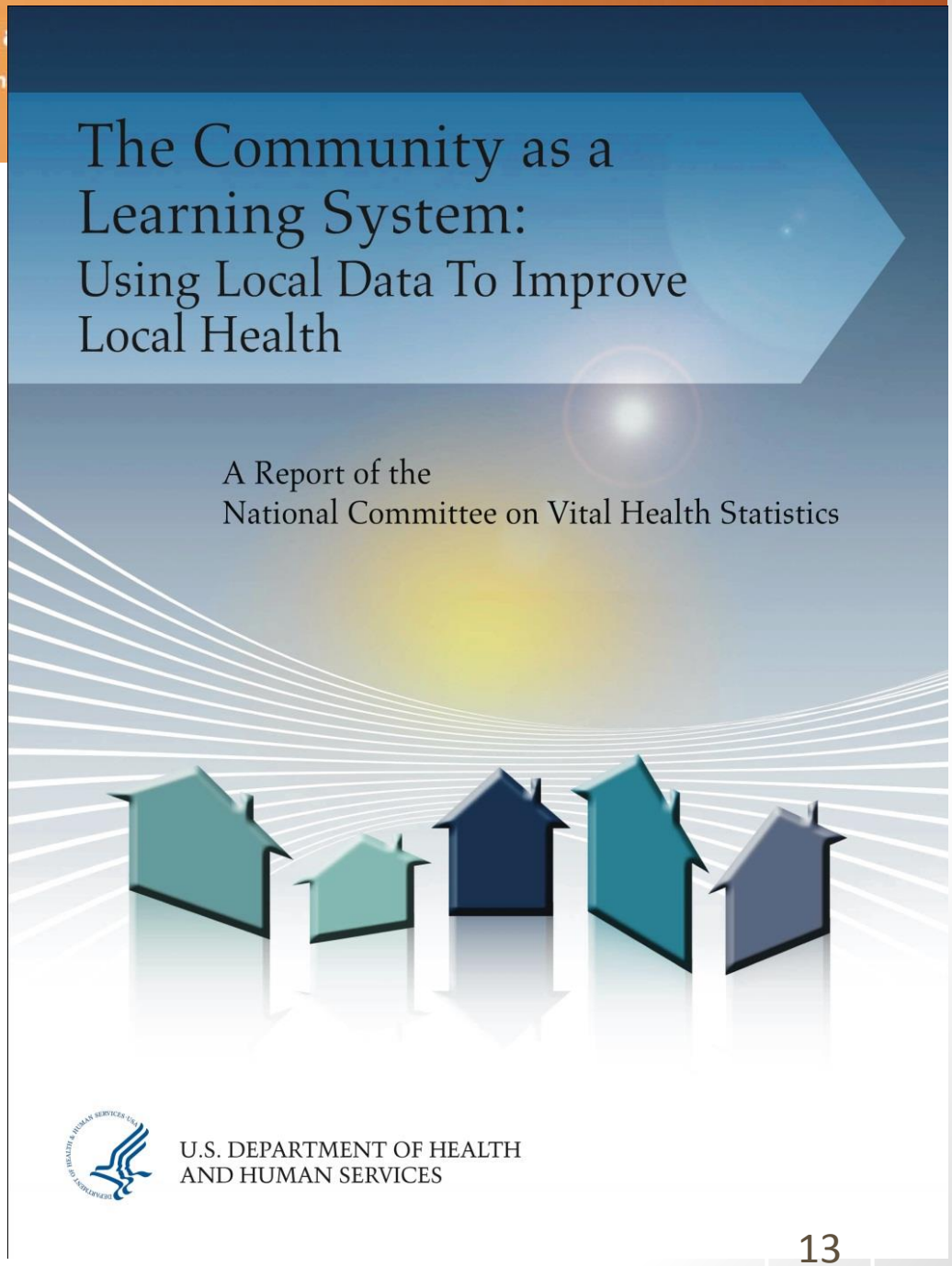
HHS should promote harmonization to ensure consistent privacy and human subject protection for all research efforts.

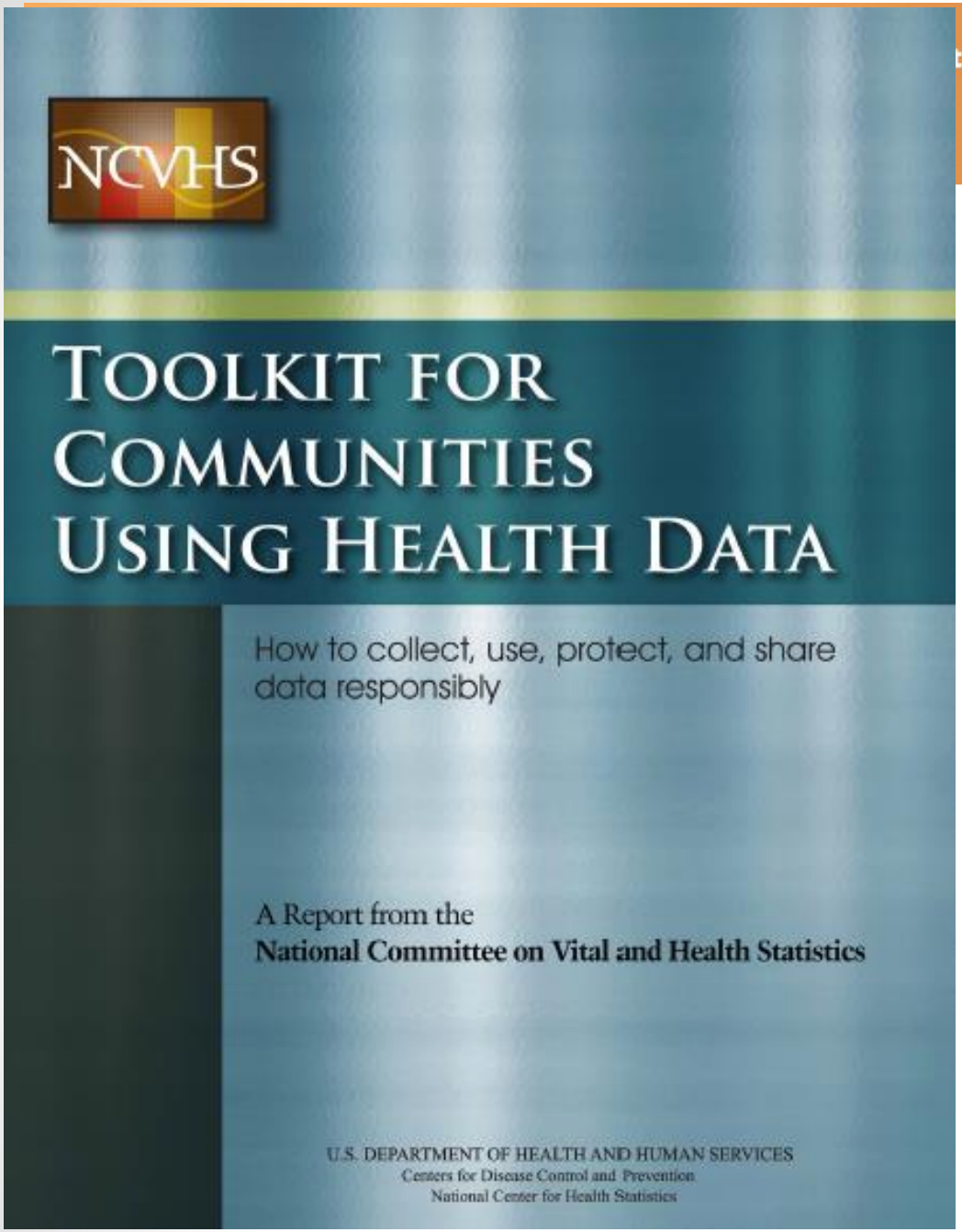
HHS should encourage the Office for Human Research Protections (OHRP) to continue to work collaboratively with the Office for Civil Rights (OCR) and to leverage the tools starting to be used in the industry to aid in distinguishing how requirements apply to uses of health data for quality and research

Letter to the Secretary on Sensitive Information

Seminal suggestions that there should be development of the technical capability to separately manage categories of sensitive information that are subject to special legal requirements. (For example, SAMSHA covered information, genetic information, types of information given special protection under state law).

Published, November 2011
Joint Project of the Population Health and Privacy, Confidentiality and Security Subcommittees





tatistics

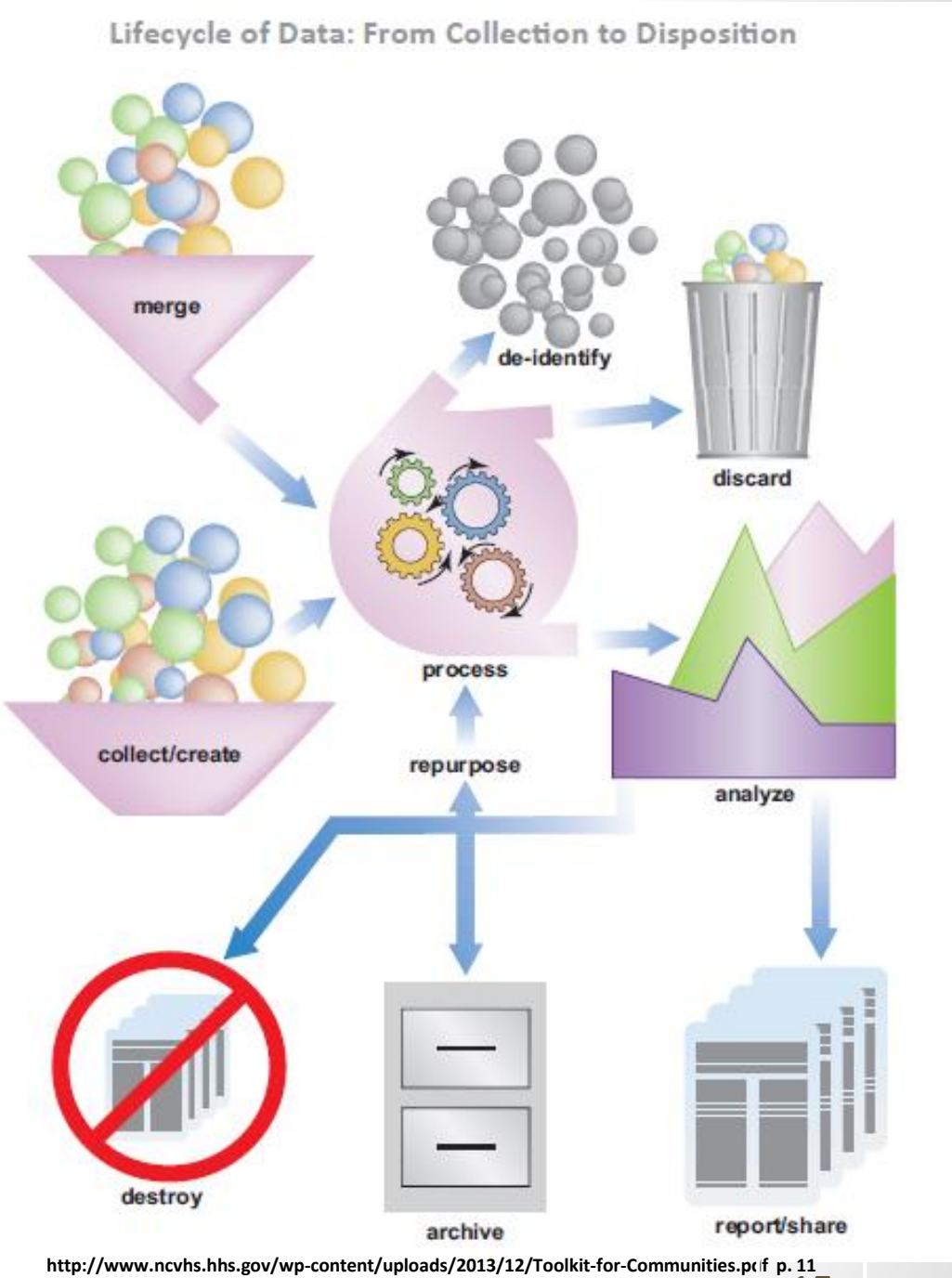
Why a Toolkit and Why Now?

- Communities asked for practical guidance.
- Illustrates principles in NCVHS's letter to the Secretary on *Stewardship Framework for the Use of Community Health Data* (Dec 5, 2012)
- *Stewardship Framework* principles and their application defined, explained and illustrated.
- Applicable laws and regulations cited and explained.
- Practical tips, checklists and cautions highlighted to avoid missteps and potential harm.

National Committee on Vital a
Advising the Secretary of Health and Huma
on health information policy since 1949.

Data Lifecycle

- Effective stewardship extends to all phases of lifecycle
- Community health data can be original data gathered for the purpose or repurposed data
- Use of repurposed data is expanding, driven by technology

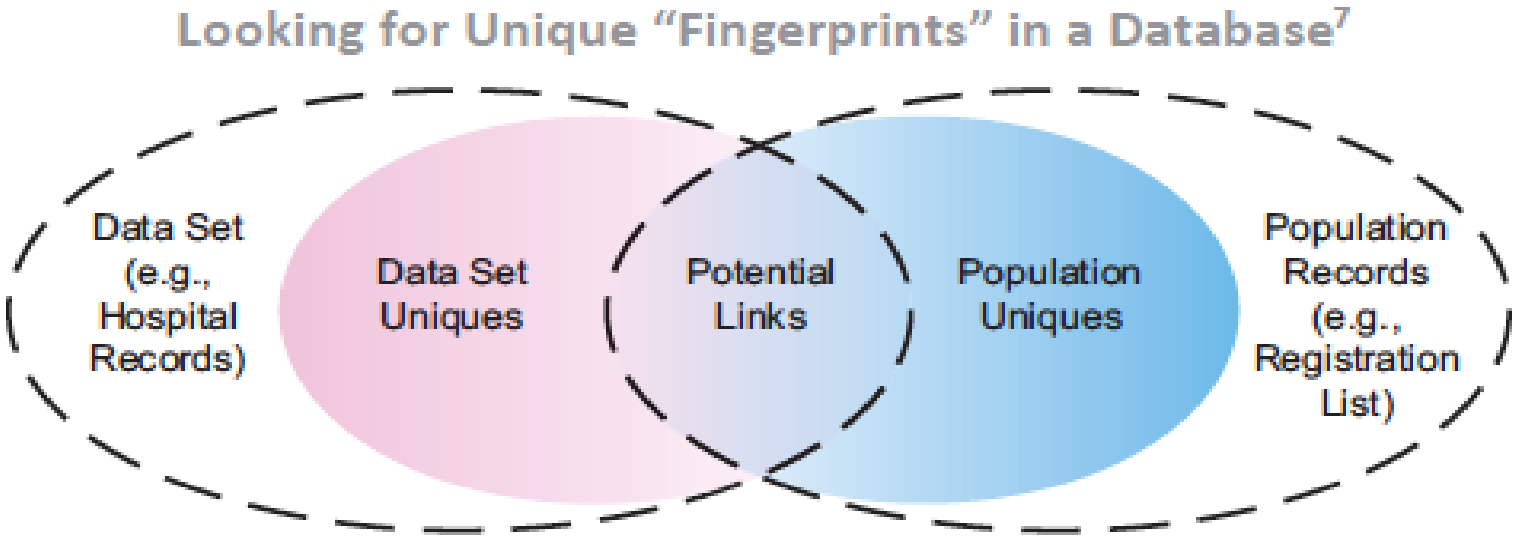


http://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf p. 11

7 Principles of Data Stewardship

http://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf p. 15

De-identified Data



Certain combinations of values may be so rare that they create a "fingerprint" pointing to only one person."

http://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf p. 40

Recent Federal Privacy Activities…

ONC Health IT Policy Committee Big Data Recommendations

Through the proliferation of software applications and mobile technology, the amount of identifiable health information being collected, analyzed, and used is growing exponentially. As the volume, velocity, and variety of such information activities continue to grow, ONC is looking at how to protect that information from potential risks that may arise from unknown and inappropriate use. The report recommends that ONC and other federal stakeholders, including the Office of Civil Rights take several actions to support privacy and security related to health big data. These actions include:

- Address Harm, Including Discrimination Concerns
- Address Uneven Policy Environment
- Protect Health Information by Improving Trust in De-Identification Methodologies and Reducing the Risk of Re-Identification
- Support Secure Use of Data for Learning

Reference: http://dashboard.healthit.gov/strategic-plan/federal-health-it-strategic-plan-2015-2020.php
September 21, 2015

Data Sharing

- ***Data sharing:*** the set of rules and procedures that govern the release of information to other parties for purposes such as research, quality of care assessment, and health care operations
- ***Assumptions:*** the 'right data' (minimum necessary or fuller file?) and are accessed by the right person (approved user with safeguards against re-release?) for a defined purpose (specific project or general use?)

Implications: Mechanisms for Data Sharing, Best Practices

- Authorization applications and forms: establish rules that govern process prior to release; develop application forms/process which is consistently used; make application aware of process, requirements, costs, etc.
- Confidentiality agreements: identify specific legal and regulatory requirements that govern the use of data; release of findings; re-release of shared data; data destruction; and penalties for misuse
- Other: consider the creation of public use 'research file'; consider the creation of use of data enclaves such as data research centers used by Census and NCHS)

Using APCD and Case Mix Data: Considerations for Re-identification and Privacy

- Complexity of files: combination of variables from a variety of sources creates enormous potential for re-identification, particularly for rare conditions or 'outlying' values
- Sensitivity of data: are behavioral health, substance abuse, and other 'sensitive' data available?
- Linked data with publicly available information
- Linkage with public health surveillance, registry, and program data

Using APCD and Case Mix Data: Challenges for Privacy, Confidentiality, and Access

- Trust
- Adherence to principles and practices of stewardship will promote appropriate use of these data
- Creating consistent and reasonable practices for data access and use is required
- Balancing the need for data use with potential fundamental requirements for protection of confidentiality

Additional Slides

NCVHS Configuration

- 18 members appointed for four year terms
- Organized around four core areas:
  - Standards (including HIPAA administrative transactions, code sets, identifiers)
  - Population Health
  - Privacy, Confidentiality and Security
  - Data Access and Use
- Holds quarterly meetings, convenes public hearings, listening session, workshops, roundtables
- Develops and delivers practical, timely, thorough recommendations to the Secretary
- Provides periodic reports to Congress
- Releases reports and resources to the Secretary for use by the public, researchers, and industry

NCVHS Recent Notable Contributions

- Visioning Documents
  - 21st Century Vision for Health Statistics report (2000)
    - Emphasized role of all factors influencing health
  - National Health Information Infrastructure (2002)
    - Led to the creation of Office of the National Coordinator for Health Information Technology
  - Towards Enhanced Information Capabilities for Health (2010)
    - Concept paper highlighting availability, accessibility, standardization and privacy and security of health information
- Population Health
  - Community as a Learning Health System Framework (2011)
  - Supporting Community Data Engagement – NCVHS Roundtable (2014)
  - Electronic Standards for Public Health Information (2014)

NCVHS Recent Notable Contributions (cont.)

- Administrative Simplification
  - Fifteen years of oversight/advice on adoption/implementation of standards, code sets, identifiers, operating rules to fulfill HIPAA and ACA administrative simplification provisions
  - HIPAA Reports to Congress (2011 - 2014)
- Privacy and Security
  - Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data (20070
  - Privacy and Security of Personal Health Records (2009)
  - National Stewardship Framework for Health Information Privacy (2009)
  - Stewardship Framework for the Use of Community Health Data (2012)
- Data Access and Use
  - Steps to improve the Usability, Use and Usefulness of HHS Data Resources (2014)

Concepts: HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA is a federal law that was passed in 1996.
- HIPAA requires safeguards to protect the privacy and security of **protected health information (PHI). Business associates** are entities receiving PHI.
- **Protected health information** is generally defined by HIPAA to be any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.
- **HIPAA** was designed to simplify insurance payments, not as a statute to protect privacy.
- HIPAA only applies to certain types of organizations called **covered entities**, as well as some other organizations that work with them. Broadly, there are three types of covered entities: health care plans (such as health insurance companies); health care providers (such as doctors or hospitals); and health care clearinghouses

NCVHS Major Privacy Related Reports

May 2015 - the distribution of The Toolkit for Communities Using Health Data and 2012 Letter to Secretary on the Development of Stewardship Framework for the Use of Community Health Data

November 10, 2010 – Letter to the Secretary – Reccommendtions Regarding Sensitive Health Information

September 28, 2009 – Letter to the Secretary – Protection of the Privacy and Security of Individual Health Information in Personal Health Records

February 20, 2008 – Letter to the Secretary – Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment

December 21,2007 - Report to the Secretary of HHS: Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data

June 21, 2007 – Letter to the Secretary – Improving the interaction of FERPA and the HIPAA Privacy Rule with regard to school health records

June 21, 2007 – Letter to the Secretary – Update to privacy laws and regulations required to accommodate NHIN data sharing practices

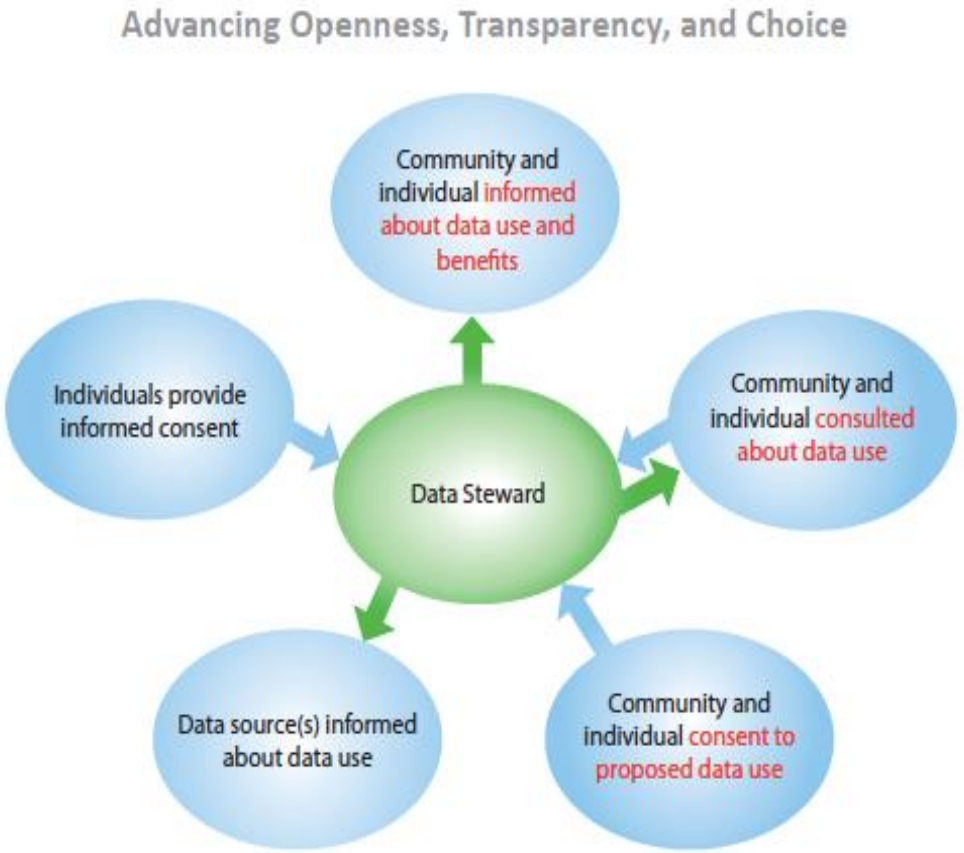
Accountability

- Accountability may lie with an individual or entity.
- Different people may be accountable for different phases of the data lifecycle or different stewardship elements.
- An accountable individual or entity should be named and held responsible for stewardship.
- Data use agreements (DUAs) are one way to establish accountability ground rules among data users.

Advancing Openness, Transparency and Choice

Notice is information provided to the community about data use

Consent is the process of getting permission from a community or individual to use data



http://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf p. 18

Community and Individual Engagement and Participation

- Evaluate opportunities for engaging communities and individuals at every step in the data lifecycle and across all elements of the stewardship framework.
- Be aware of the concerns of subgroups within communities whose interests may be different from those of the larger community.
- Consider the risk of stigmatization of communities or small groups and engage the community or individuals to determine an action plan for addressing the risk.

Purpose Specification

- Define the purpose of data collection or use of repurposed data.
- Consider how to engage the community in purpose specification.
- Anticipate possible adverse impacts of data use or collection.
- Be aware that data may later be repurposed, design collection accordingly.
- When using repurposed data, consider the need for additional notice or consent.
- Address and align goals of collaborating entities regarding goals, funding, use limitations.

Quality and Integrity

- Ensure that data quality and integrity are maintained throughout the data lifecycle
- Before merging data sets, consider how the merger will affect data quality and integrity.
- Example quality questions to ask:
  - Are the populations the same for the different data collection efforts?
  - Do survey questions and response categories match?
  - Might differences in survey administration dates affect survey results?
  - What were the survey sample designs?

Security

Physical

- ✓ Install locks on cabinets or rooms where paper records are stored
- ✓ Keep records away from areas vulnerable to damage in a flood
- ✓ Protect electronic storage facilities against break-ins or destruction
- ✓ Back up data with off-site storage capabilities

Technical

- ✓ Maintain logs of system access and unauthorized extraction of data
- ✓ Add encryption Specific elements in a data set
- ✓ Data set as a whole
- ✓ Devices that allow access to the data set, such as laptop computers
- ✓ Implement monitoring to scan for and identify cyber attacks

Administrative

- ✓ Run a risk analysis
- ✓ Set up policies and procedures for accessing paper records, disposing of data, or adding new equipment on a network
- ✓ Train those with access to sensitive information in data security
- ✓ Require robust passwords
- ✓ Control who has access to view or change the data
- ✓ Conduct due diligence on employees who handle data
- ✓ Implement an incident response program