Data Modernization Workshop: Building on Shared Services and Enterprise Technologies

May 19, 2021 – May 21, 2021

An attorney’s perspective on public health data modernization

**Keynote Session | May 21**

**Moderator**
Charlie Ishikawa, Kahuina Consulting, LLC

**Presenter**
Denise Chrysler, Network for Public Health Law

Introductions

Denise Chrysler, JD
Director, Mid-States Region
Network for Public Health Law
An Attorney’s Perspective on Public Health Data Modernization

Denise Chrysler, J.D.
Data Modernization Workshop
May 21, 2021
Goal: Obtain and share useful and useable data

Challenge: Maximize benefits, minimize risks
About the Network for Public Health Law

We believe in the power of public health law and policy to improve lives and make our communities safer, healthier, stronger and more equitable. We know that understanding, navigating and using law and policy can transform our communities so we work to help public health leaders, policymakers, researchers, educators, advocates and healthcare providers do just that.
Law governs every aspect of data

- Collection
- Use
-Disclosure
- Protection

Law friend or foe?

- How does law help us achieve our goals?
- How is law a barrier?
- How do we develop public health data systems to facilitate legal compliance and promote policy priorities?
Find and support pathways to share data

It depends.

Attorneys are necessary to ensure that information sharing complies with laws
Health departments have broad authority to collect data for statistical and public health purposes
(1976 S. Ct opinion, Planned Parenthood v. Danforth)

State law establishes reporting requirements
- Who must report
- Information that must be reported
- Format and manner of reporting
- State law variation mitigated by national standards
HIPAA Privacy Rule should not impede public health data collection functions

- Allows reporting required by law and reporting authorized by law
- Covered entities can rely on government’s representation of authority
- Best practice: Provide memorandum stating authority in the event of pushback

But…may impede data disclosure for HIPAA-covered health departments
Other laws can impede public health data collection functions

- FERPA (education records)
- 42 CFR Part 2 (substance use disorder records)
- Best practices:
  - Design project to satisfy permitted disclosures under law
  - Think “local public health system”
  - Develop partnerships to support data holders’ role in protecting the public’s health
“Health Equity by Design”

States Fail COVID Vaccine Data Reporting Requirements On Race

by Lacy Crawford, Jr | Feb 4, 2021 | Press Releases
Privacy and security fundamentals

Data privacy – the relationship between the collection, use and disclosure of data and the public or legal expectation of privacy surrounding the data.

Data security – protective measures designed to prevent unauthorized access to electronic or paper data.

If you collect it, you must protect it!

(1977 S. Ct opinion, Whalen v Roe)
Analyzing a data sharing issue: multiple datasets, sources, linkages

Establish facts – for each data stream

» What data?
» Who holds it?
» From whom was it obtained (source of data)?
» For what purpose was it obtained?
» To whom is it to be disclosed?
» For what purpose is it to be disclosed?
» How will it be disclosed?
Analyzing a data sharing issue (continued)

Identify laws that apply to each data stream

So much data . . . so many laws

» Data type
» Data source
» Data sharing purpose

May include general and/or specific laws
Data protection and disclosure laws + frequent condition for receiving funds

Federal
- HIPAA
- FERPA
- WIC
- Title X family planning
- Cancer registries
- Substance abuse treatment
- Federally supported research
- Social Security Act

State
- Health information
- Disease surveillance
- Registries
- Vital records
- Screening
- Drug monitoring
- Medicaid
- Clinical services
- Social security number
- Sunshine law
Analyzing a data sharing issue (continued)

Apply law

» What does law allow?
» What prerequisites, conditions or limitations apply?

De-identification

» If personally identifying information in a dataset is removed or obscured
» Then most laws do not prohibit release of de-identified information
Disclosing de-identified data

“Data can be either useful or perfectly anonymous, but never both.” Professor Paul Ohm

**Concern:** Data regarding small geographic size, specific populations, sparsely-populated areas, identifying populations based on multiple characteristics or unique characteristics

**Concern:** Informing the public; aggregate data can be identifiable (is there a reasonable basis to believe data can be used to identify an individual?)

**Concern:** Sufficient identifiers needed to link and combine data across databases and data sources
Release of data: Juggling multiple roles and competing interests

» Protecting the public
» Informing the public
» Protecting individual privacy
» Weighing release of preliminary data or analysis based on limited data
Goal: Obtain and share useful and useable data

Balance: Maximize benefits, minimize risks

» Technology + policy

» Data management and statistical controls to provide the most meaningful data possible while protecting privacy

» Ready to share? Establish and document terms of sharing
Thank you!

Denise Chrysler, J.D.

dchrysler@networkforphl.org
Questions?

• Raise your hand.
• Type your questions into the chat.
• Use reactions to communicate with panelists.
Next steps

• Continue the discussion on the message board (link provided in the chat).

• Fifteen-minute break: 12:15–12:30 PM EST

• Next session: 12:30 – 1:30 PM EST
  • Maker session: Creating a solution and tailoring a value case for leadership
Thank you.