The Network for Public Health Law

Ideas. Experience. Practical answers.

The *Legal* Landscape of Interjurisdictional Exchange

Denise Chrysler, JD
Director, Mid-States Region
Network for Public Health Law

AIRA National Meeting, August 15, 2018

The Network for Public Health Law

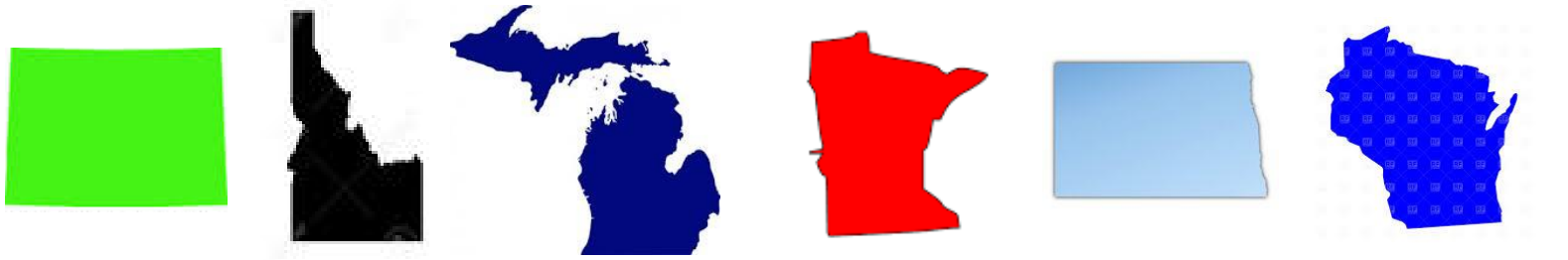
Navigating law to share IIS data among jurisdictions

- Where we have been
- Where we are
- Where we are going (or might go)

The Network for Public Health Law

Six State Pilot

- Goal: common agreement for IIS exchange
- Developed in consultation with state attorneys, IIS staff, ASTHO, AIRA
- MOU instead of data sharing agreement
- Signed by all six states as of April 10, 2017
- Technology inclusive
- Addressing unique needs of each state
- Used by ONC for HUB participants



Colorado Idaho Michigan Minnesota North Dakota Wisconsin

The Network for Public Health Law

MOU provisions

- **Parties – original and additional**
- **Purpose**
- **Communications outside MOU; emergency powers**
- **Definitions**
- **Data to be provided (elements, frequency, method of exchange)**
- **Incorporation, use and disclosure of data**
- **Privacy and security safeguards**
- **HIPAA – exchange among "public health authorities"**
- **Period of MOU**
- **Termination**
- **Warranties – best efforts, no guarantees**
- **Contract boilerplate** (e.g. authority, entire agreement, severability, limitation on liability, no third party beneficiaries, governing law, etc.)

The Network for Public Health Law

"Ownership" / control of data

11. Incorporation of data. A party that receives IIS data from another party may incorporate the data into its IIS.

12. Control, use and disclosure of data. Absent exception, upon receipt, data are subject to the control of the receiving state. As such, the receiving party is responsible for maintenance, use and disclosure of data that it has received under this MOU, consistent with its laws and policies, as applicable.

"Ownership" / control of data continued

EXCEPTION: A sending party must specify in Appendix C any limits on the receiving party's assumption and exercise of control over data that it receives from the sending party under this MOU.

13. Privacy and security. By signing this MOU, a party affirms that it has established and uses appropriate administrative, technical, and physical safeguards to protect the privacy and security of data received under this MOU and to prevent unauthorized use of or access to it. Each sending party, with regard to the data that it provides, is subject to the privacy and security provisions established within its own jurisdiction, and is not required to adhere to the law or policies of the receiving jurisdiction.

MOU provisions, continued

- **Appendix A:** Identifies IIS core data elements and any additional data elements that each party is able to provide and receive from other parties
- **Appendix B:** Each party identifies frequency and methods of exchange and transport
- **Appendix C:** Each sending party identifies any limitations on maintenance, use or disclosure of data based on the sending party's law or policies

The Network for Public Health Law

Status

- **Community of practice feedback**
- **Defined use cases**
- **Network review:**
  - Identify what worked well
  - Identify what needs addressed
  - Provide recommendations

Goals: Improve exchange among current states; Expand interjurisdictional exchange to include more states.

The Network for Public Health Law

What Worked Well

- **Came to agreement**
- **Agreement adopted for HUB project**
- **Some states exchanging data**
- **States exploring options for moving data** (e.g. via statewide HIEs)
- **Addressed concern about impact of MOU on other agreements**
- **Served well as pilot**

The Network for Public Health Law

Identified Concerns

- **Lack of administrative oversight and facilitation**
- **Lengthy timeframe for execution by all states** (August 2015 - April 2017)
- **Logistics of amending MOU**
- **Variation in terms of agreement due to state laws** (defeats “one agreement” goal; logistical challenges, might limit exchange benefits)
- **Point to point data transfer** (each participant must address with all other participants)

The Network for Public Health Law

Infrastructure Considerations

- Administration and oversight of system
- Participation
- Governance/ decision-making
- Data standards
- "Moving" data
- Expenses
- Privacy and security
- Use and disclosure
- Variation in state law and policy
- Public display of agreements/terms

The Network for Public Health Law

Variation of State Law: Impact on Data Use & Disclosure

- **Extent of problem:** How many states are able to sign with no restrictions?
- **Significance of problem:** Are restrictions actually barriers?
- **Source of problem:**
  - Law vs. nonlaw
  - Plain language vs. interpretation
  - Statute vs. regulation

What Next? Might Address:

- Administrator
- Execution of agreement
- Adding parties
- Governance and decision-making – DURSA & TEFCA
- Moving data / technology
- Public display of agreements, terms, restrictions

The Network for Public Health Law

Addressing Variation State Law

- **What provisions are necessary to satisfy use cases?**
- **What provisions might be included in MOU to minimize sending state's concerns?**

e.g. strengthen "purpose;" expand permissible uses and disclosures; specify prohibitions; expand privacy and security provisions

The Network for Public Health Law

Addressing Variation State Law

continued

» **Implement multiple approaches?**

- Execution of common agreement by jurisdictions that can do so with no reservations
- Technical assistance to states with concerns to identify potential legal solutions
- States with restrictive laws – execute separate tailor-made agreements or other solutions with priority states, such as border states

The Network for Public Health Law

Thank you!

Denise Chrysler, J.D.
dchrysler@networkforphl.org